RAPPORT D'ACTIVITÉS 2013
ACTIVITEITENVERSLAG 2013

Quis custodiet ipsos custodes?

Quis custodiet ipsos custodes ? est une série de publications qui a pour objectif de stimuler une discussion approfondie quant au fonctionnement, aux compétences et au contrôle des services de renseignement et de sécurité et du travail de renseignement. Cette série reprend notamment des études scientifiques, les rapports d'activités du Comité permanent R et des rapports de colloques.

Rédaction

Comité permanent de contrôle des services de renseignements et de sécurité, rue de Louvain 48, boîte 4 à 1000 Bruxelles (02 286 29 88).

Déjà parus dans cette série

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Comité permanent R, *Rapport d'activités 2006,* 2007, 147 p.
3) Comité permanent R, *Rapport d'activités 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.
5) Comité permanent R, *Rapport d'activités 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Comité permanent R, *Rapport d'activités 2009,* 2010, 127 p.
8) Comité permanent R, *Rapport d'activités 2010,* 2011, 119 p.
9) Comité permanent R, *Rapport d'activités 2011,* 2012, 134 p.
10) W. Van Laethem et J. Vanderborght, *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, 2013, 565 p.
11) Comité permanent R, *Rapport d'activités 2012*, 2013, 127 p.
12) Comité permanent R, *Rapport d'activités 2013*, 2014, 212 p.

RAPPORT D'ACTIVITÉS 2013

Comité permanent de contrôle des services de renseignements et de sécurité

Comité permanent de contrôle des services
de renseignements et de sécurité

intersentia
Antwerpen – Cambridge

Le présent *Rapport d'activités 2013* a été approuvé par le Comité permanent de contrôle des services de renseignements et de sécurité lors de la réunion du 24 juillet 2014.

(*soussignés*)
Guy Rapaille, président
Gérald Vande Walle, conseiller
Pieter-Alexander De Brock, conseiller
Wouter De Ridder, greffier

Rapport d'activités 2013
Comité permanent de contrôle des services de renseignements et de sécurité

ISBN 978-94-000-0551-8
D/2014/7849/156
NUR 823

TABLE DES MATIÈRES

LISTE DES ABRÉVIATIONS

ACOS-IS	*Assistant Chief of Staff intelligence and Security*
ACOS Ops & Trg	Département d'état-major *Operations and Training*
A.M.	Arrêté ministériel
ANS	Autorité nationale de sécurité
A.R.	Arrêté royal
Ann. parl.	Annales parlementaires
AR C&HS	Arrêté royal du 24 mars 2000 portant exécution de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
AR OCAM	Arrêté royal du 28 novembre 2006 portant exécution de la Loi du 10 juillet 2006 relative à l'analyse de la menace
BELINT	*Belgian intelligence*
BENIC	*Belgian National Intelligence Cell*
BIA	*Belgian Intelligence Academy*
BIC	*Battle Group Intelligence Cell*
BISC	*Belgian Intelligence Studies Centre*
CANPAN	Commission d'avis pour la non-prolifération des armes nucléaires
CCB	Centre pour la cybersécurité Belgique
CEDH	Convention européenne des droits de l'homme
CIC	Code d'instruction criminelle
CMRS	Comité ministériel du renseignement et de la sécurité
Comité permanent P	Comité permanent de contrôle des services de police
Comité permanent R	Comité permanent de contrôle des services de renseignement et de sécurité
Commission BIM	Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité
CHOD	*Chief of Defense*
CIA	*Central Intelligence Agency*
CP	Code pénal
CPOE	*Comprehensive Preparation of the Operational Environment*
CPVP	Commission de la protection de la vie privée
CRIV	Compte Rendu Intégral – Integraal Verslag
CTIF	Cellule de Traitement des Informations Financières
Doc. parl.	Documents parlementaires

FragO	*Fragmentary Orders*
GCHQ	*Government Communications Headquarters*
HUMINT	*Human intelligence*
IMINT	*Image intelligence*
ISAF	*International Security Assistance Force*
ISTAR	*Intelligence Surveillance, Target Acquisition and Reconnaissance*
JIB	*Joint Information Box*
L.Contrôle	Loi organique du 18 juillet 1991 du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace
L.C&HS	Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité
L.OCAM	Loi du 10 juillet 2006 relative à l'analyse de la menace
Loi MRD	Loi du 4 février 2010 relative aux méthodes de recueil des données par les services de renseignement et de sécurité
L.Org.recours	Loi du 11 décembre 1998 portant création d'un organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité
LPA	Loi du 11 avril 1994 relative à la publicité de l'administration
L.R&S	Loi organique du 30 novembre 1998 des services de renseignement et de sécurité
MAT	*Military Assistance Team*
M.B.	Moniteur belge
MRD	Méthodes de recueil des données
MPR	Méthodes particulières de recherche
NSA	*National Security Agency*
OCAM	Organe de coordination pour l'analyse de la menace
OEF	*Operation Enduring Freedom*
ONU	Organisation des Nations Unies
OSINT	*Open sources intelligence*
OTAN	Organisation du Traité de l'Atlantique Nord
PRT	*Provincial Reconstruction Team*
PSE	Potentiel scientifique et économique
Q. et R.	Questions et réponses écrites (Chambre ou Sénat)
RFI	*Request for information*
SGRS	Service général du renseignement et de la sécurité des Forces armées
SIGINT	*Signal intelligence*
s.l.	*sine loco*
SOP	*Standing Operating Procedure*
SPF	Service public fédéral
TIC	Technologies de l'information et de la communication
VSSE	Sûreté de l'État

PRÉFACE

Pour le Comité permanent R, l'année 2013 a été marquée par deux événements tout à fait différents, mais chacun à leur manière importants pour l'organisation.

Le premier événement fut son vingtième anniversaire. C'est en effet le 24 mai 1993 que le Comité permanent de contrôle des services de renseignement et de sécurité a vu le jour. Cet anniversaire ne pouvait pas passer inaperçu. C'est ainsi que nous avons rédigé un ouvrage de plus de 500 pages intitulé « Regards sur le contrôle ». Cet ouvrage aborde pour ainsi dire tous les aspects du contrôle démocratique des services de renseignement. Tous les acteurs d'hier et d'aujourd'hui ont également apporté leur pierre à l'édifice en donnant leur vision du contrôle. Ce livre a été présenté comme il se doit au Sénat, sous les auspices de sa présidente.

S'il ne fallait retenir qu'un seul élément, ce serait qu'en vingt années d'existence, le Comité permanent R a acquis ses lettres de noblesse dans notre système démocratique. Le Comité est devenu une organisation qui veille au fonctionnement concret des services de renseignement et qui, avec ses rapports et ses recommandations, fournit une contribution essentielle au débat sur les tâches et les compétences de ces services. Tout ceci n'a été possible que grâce à l'engagement et à l'expertise de tous ceux qui travaillent ou ont travaillé pour le Comité permanent R, quelle que soit leur fonction au sein de l'organisation.

Le Comité permanent R d'aujourd'hui ne ressemble certes plus à l'organe de contrôle de 1993, et ce en raison des nombreuses modifications de la législation et d'une meilleure compréhension de la pratique. S'il s'agissait parfois de « retouches » techniques, certains changements ont considérablement modifié l'aspect du Comité et ses processus de travail. Et cette évolution n'est pas terminée, comme le démontre la loi du 6 janvier 2014. En effet, avec la réforme du Sénat qui fait suite à la sixième réforme de l'État, l'interlocuteur du Comité au Parlement est devenu, depuis les élections du 25 mai 2014, la « Commission chargée de l'accompagnement du Comité permanent P et du Comité permanent R » à la Chambre des Représentants, qui contrôlera à la fois les services de police et de renseignement. Et ce n'est pas tout : dans la nouvelle composition de cette commission, les présidents de tous les groupes politiques se voient dorénavant attribuer un siège et pourraient également prendre connaissance d'informations classifiées. L'avenir nous dira quelle influence ces modifications auront sur le contrôle parlementaire.

L'autre événement marquant de 2013, qui a surtout animé le second semestre, est qu'Edward Snowden, ancien collaborateur d'un service de renseignement américain, est parvenu à copier des dizaines de milliers de documents extrêmement sensibles de la *National Security Agency* et à les communiquer à des journalistes. C'est ainsi que sont parus à plusieurs reprises des articles de presse interpellants, relatant l'interception massive de données à l'échelle mondiale ainsi que l'espionnage économique et politique par les services de renseignement américains et britanniques. Il est évident que la communauté internationale du renseignement a été sérieusement ébranlée par ces révélations. Celles-ci ont également donné lieu à des enquêtes parlementaires, judiciaires et de renseignement dans le monde entier, y compris en Belgique. Dans ce cadre, le Comité permanent R a ouvert pas moins de quatre enquêtes.

Que des grandes puissances disposent de moyens et de programmes sophistiqués pour intercepter massivement des données n'était pas une révélation en soi. Ce qui l'était en revanche, c'était le caractère universel et massif de ce recueil électronique d'informations, pour lequel les logiciels et le matériel les plus en pointe ont été utilisés et pour lequel des moyens humains et financiers sans précédent ont été déployés. Le second élément nouveau était qu'il est apparu de plus en plus clairement que des grandes puissances n'ont pas hésité à mener des activités d'espionnage de nature politique et économique à l'égard de « pays amis », en interceptant des données de manière massive ou ciblée. Les dirigeants, les services de renseignement, mais aussi les dépositaires du contrôle, devront en tirer les leçons qui s'imposent.

Guy Rapaille,
Président du Comité permanent de contrôle
des services de renseignement et de sécurité

Le 1er juin 2014

CHAPITRE I
LE SUIVI DES RECOMMANDATIONS DU COMITÉ PERMANENT R

Une des tâches principales du Comité permanent R consiste à formuler, pour les pouvoirs législatif et exécutif, des recommandations qui portent en particulier sur la légitimité, la coordination et l'efficacité de l'intervention des deux services de renseignement belges, de l'OCAM et, dans une moindre mesure, de leurs services d'appui.[1] Les recommandations que le Comité a formulées en 2013 figurent au dernier chapitre du présent rapport d'activités. Ce chapitre introductif énumère les principales initiatives que les différents acteurs ont prises dans la lignée des recommandations du Comité permanent R. Ensuite, une attention particulière est accordée aux recommandations que le Comité estime essentielles, mais qui n'ont pas encore été mises en œuvre.

I.1. INITIATIVES ET RÉALISATIONS DANS LA LIGNÉE DES DIFFÉRENTES RECOMMANDATIONS

I.1.1. UNE STRATÉGIE FÉDÉRALE EN MATIÈRE DE PROTECTION DES SYSTÈMES D'INFORMATION ET DE COMMUNICATION

Dans la société actuelle, la protection des systèmes d'information et de communication est essentielle. Dans ce cadre, le Comité avait déjà formulé des recommandations visant à œuvrer à une politique de sécurité intégrée en matière de cyberattaques. Il avait plaidé pour un élargissement des compétences du SGRS et de la VSSE et pour le recrutement de collaborateurs qualifiés. Il avait recommandé la plus grande prudence lors du choix des équipements techniques sécurisés utilisés pour le traitement des informations classifiées. Enfin, il avait

[1] Les enquêtes relatives à l'OCAM et aux services d'appui sont menées conjointement avec le Comité permanent P (art. 53, 6° L.Contrôle).

souligné le manque de moyens techniques de certification et d'homologation en matière de sécurité de l'information.[2]

En référence à ces recommandations, le Sénat et la Chambre des Représentants ont déposé plusieurs propositions de résolution. En 2011, les membres de la Commission parlementaire de suivi du Comité permanent R de l'époque avaient déjà introduit une « *proposition de résolution relative à la mise en œuvre rapide d'une stratégie fédérale de sécurité des systèmes d'information et de communication* »[3], suivie, à la fin novembre 2012, par une « *proposition de résolution visant à sécuriser les informations électroniques et à lutter contre les cyberattaques* ».[4] Une proposition de résolution « *visant à instaurer un Centre pour la cybersécurité en Belgique* »[5] a été déposée dans le même sens à la Chambre en juin 2013. Le Conseil des ministres du 19 décembre 2013 a approuvé le projet d'Arrêté royal portant création du Centre pour la cybersécurité Belgique (CCB) qui, sous l'autorité du Premier ministre, doit se charger de la mise en œuvre de la stratégie de cybersécurité belge.[6]

I.1.2. DESTRUCTION D'ANCIENS DOSSIERS

L'article 21 L.R&S stipule que les données à caractère personnel traitées par des services de renseignement peuvent uniquement être conservées « *pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées, à l'exception de celles présentant un caractère historique, reconnu par les archives de l'État* » et qu'elles ne peuvent être « *détruites qu'après un certain délai qui suit le dernier traitement dont elles ont fait l'objet* ». Les délais de conservation et la procédure relative à leur destruction doivent – déjà depuis la Loi du 30 novembre 1998 ! – être définis par Arrêté royal, après avis de la Commission de la protection de la vie privée. Cet arrêté n'a pas encore été pris. Le Comité a pourtant insisté[7] sur ce point, non seulement afin de se conformer à une obligation légale, mais également parce que la conservation de données anciennes par les services de renseignement peut constituer une infraction à l'article 8 CEDH.

---

2 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 108-110 (IX.2.3. Recommandations relatives à la sécurité de l'information).

3 *Doc. parl.* Sénat, 2011-12, n° 5-1246/1.

4 *Doc. parl.* Sénat, 2012-13, n° 5-1855/1.

5 *Doc. parl.* Chambre 2012-13, n° 53-2918/001. Voir dans le même sens : « Résolution du Parlement européen du 12 juin 2012 sur la protection des infrastructures d'information critiques – Réalisations et prochaines étapes : vers une cybersécurité mondiale », *Journal officiel de l'Union européenne*, C 332 E/22, 15 novembre 2013.

6 http://www.presscenter.org/fr/pressrelease/20131219/creation-du-centre-pour-la-cybersecurite-belgique.

7 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 19-31, particulièrement la page 30 (II.2. « Dossiers réservés » au sein de la VSSE).

En 2012, la ministre de la Justice a rédigé un projet d'arrêté qui a été soumis à l'avis de la Commission de la protection de la vie privée. Cette dernière a rendu son avis le 20 février 2013.[8] Depuis lors, le Comité est sans nouvelle de ce projet d'arrêté.

I.1.3. UNE NOUVELLE NOTE DE SERVICE DE LA VSSE SUR LE SUIVI DE PARLEMENTAIRES

Trois enquêtes de 2013 (II.2, II.3 et II.4) ont démontré que le devoir d'informer le ministre de la Justice chaque fois qu'un parlementaire se trouve dans le collimateur de la VSSE n'est généralement pas respecté. Le Comité permanent R avait pourtant déjà souligné l'importance de ce devoir d'information. Il a recommandé aux ministres compétents de traduire leurs besoins en matière d'informations et les éventuelles restrictions à l'égard du recueil d'informations concernant des mandataires et des partis politiques dans des directives claires (IX.1.3). En outre, le Comité a suggéré que les deux services de renseignement prennent une initiative commune à l'égard du Comité ministériel du renseignement et de la sécurité en vue de l'adoption d'une telle directive.

Peu après la clôture des enquêtes de contrôle visées, la Sûreté de l'État – et donc pas la ministre de la Justice et pas non plus en concertation avec le SGRS – diffusait une note de service «*concernant les liens de parlementaires et mandataires politiques dans les documents de la VSSE*». Dans cette note, il est entre autres stipulé que le ministre de la Justice ne doit plus être automatiquement informé lorsqu'un parlementaire ou un ministre apparaît dans un rapport des services extérieurs. Il doit seulement l'être lorsque ces mandataires politiques sont cités nommément dans des documents d'analyse, ce qui réduit le flux d'informations à destination du ministre compétent.

I.1.4. LA FONCTION « ANALYSTE OPÉRATIONNEL » AU SEIN DU SERVICE GÉNÉRAL DU RENSEIGNEMENT ET DE LA SÉCURITÉ

Lors de l'audit réalisé au sein du SGRS[9], le Comité a indiqué qu'il convenait «*de déterminer quelle est la collaboration opportune et requise entre et au sein des divisions*».[10] Le SGRS a pris cette recommandation à cœur et a créé la fonction

---

8 Commission de la protection de la vie privée, Avis n° 07/2013 du 20 février 2013 relatif à l'avant-projet d'Arrêté royal portant exécution de l'article 21 de la Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (CO-A-2012-044).

9 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 (II.1. Un audit au sein du service de renseignement militaire).

10 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 105.

d'« analyste opérationnel » au sein de la Division C(ounter) I(ntelligence).[11] Celui-ci joue un rôle d'intermédiaire entre les analystes et les personnes sur le terrain (collecte), et ce afin de veiller à une meilleure harmonisation des besoins mutuels.

I.2. RETOUR SUR DES RECOMMANDATIONS ANTÉRIEURES

L'article 35, alinéa 3 L.Contrôle confère au Comité permanent R la mission de faire rapport au Parlement « *lorsqu'au terme d'un délai qu'il estime raisonnable, il constate qu'aucune suite n'a été réservée à ses conclusions, ou que les mesures prises sont inappropriées ou insuffisantes* ». Dans ce cadre, le Comité reprend chaque année une ou plusieurs recommandations qu'il estime essentielles à la lumière de sa double finalité : le fonctionnement efficace des services et la garantie des droits fondamentaux.

Dans ce cadre, le Comité permanent R n'a de cesse d'insister sur l'urgente nécessité d'exécuter les obligations définies dans les articles 19 et 20 L.R&S. Ces articles visent en effet à réglementer l'échange d'informations et la collaboration des services de renseignement belges avec d'autres autorités, y compris étrangères.[12] Dans son « Aperçu des principales recommandations du Comité permanent R (1994-2005) »[13], le Comité avait déjà insisté sur une réflexion à ce propos.[14] Le projet de loi décrivant les méthodes de recueil des données (l'actuelle Loi MRD) offrait une excellente opportunité pour remédier à cette lacune. Le législateur n'a toutefois pas saisi cette occasion. En 2007, le Comité a réitéré sa recommandation.[15] Lors de l'enquête de contrôle sur lesdits « dossiers réservés », le Comité a une nouvelle fois demandé, en 2008, l'élaboration d'une réglementation claire pour la transmission de données à caractère personnel à des services (de renseignement) étrangers et a particulièrement fait référence à la réglementation néerlandaise, allemande et norvégienne en la matière.[16] En 2009,

---

11 Dans l'intervalle, la Division C(ounter)I(ntelligence) a fusionné avec la Division S(ecurity) pour former la Division CIS.

12 Les Commissions de suivi ont elles aussi toujours souscrit à cette recommandation.

13 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 4 et 132.

14 « *Bien que le Comité permanent R soit conscient que les services de renseignement (étrangers) considèrent comme «intouchable» la «règle du service tiers», il a maintes fois insisté sur la nécessité de réfléchir à l'application de cette règle et à son contrôle. En effet l'application de la règle du service tiers peut donner lieu à une interprétation erronée (due à une certaine culture du secret) ou, dans des cas extrêmes, à une utilisation incorrecte. Par ailleurs, le Comité permanent R a toujours estimé que la collaboration avec les services de renseignement étrangers, en particulier européens, devait être renforcée, non sans prévoir un contrôle adéquat.* » dans COMITÉ PERMANENT R, *Rapport d'activités 2006*, 4.

15 COMITÉ PERMANENT R, *Rapport d'activités 2007*, 73-74.

16 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 6, 105-106.

le Comité a affirmé que l'absence de telles directives « *rend légalement discutable cette communication d'informations* ».[17] Les deux années qui ont suivi (2010 et 2011), plusieurs dossiers MRD ont montré que les services de renseignement belges opèrent parfois sur indication de services étrangers et peuvent alors être amenés à communiquer des données à caractère personnel. Le Comité tient à attirer l'attention sur cette question délicate, d'autant plus que le Comité ministériel n'a pas encore élaboré de directive en la matière.[18] Les recommandations du *Rapport d'activités 2012* abordent une nouvelle fois cette question[19], tout comme le présent rapport d'activités. Deux enquêtes importantes (II.1. « Le rôle du Service général du Renseignement et de la Sécurité dans le suivi du conflit en Afghanistan », II.10. « Rapports intermédiaires dans les enquêtes faisant suite aux révélations d'Edward Snowden ») démontrent une fois encore toute l'urgence d'une telle réglementation.

17 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 4, 106-107.
18 COMITÉ PERMANENT R, *Rapport d'activités 2010*, 3-4 et *Rapport d'activités 2011*, 5-6.
19 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 2 et 97.

CHAPITRE II
LES ENQUÊTES DE CONTRÔLE

En 2013, neuf enquêtes ont été clôturées. Dans le même temps, le Comité permanent R a également bouclé un rapport intermédiaire relatif à l'une des enquêtes menées dans la foulée des révélations d'Edward Snowden (voir II.10). Six des dix enquêtes ont été ouvertes à la demande de la Commission de suivi du Sénat (dont une résulte en partie d'une initiative de la ministre de la Justice). Quatre enquêtes de contrôle ont été menées à la suite d'une plainte ou d'une dénonciation. Les sections qui suivent traitent des neuf rapports finaux (de II.1 à II.9) et du rapport intermédiaire (II.10). Ensuite sont énumérées et brièvement décrites les enquêtes toujours en cours (II.11).

Dans cette dernière rubrique, il est également fait mention des dix enquêtes de contrôle ouvertes en 2013. Trois de ces enquêtes sont menées conjointement avec le Comité permanent P. Quatre des dix nouvelles enquêtes ont été ouvertes à la demande du Sénat, cinq à la suite d'une plainte et une à l'initiative commune des Comités R et P.

Au total, le Comité a reçu 28 plaintes et dénonciations en 2013. Après vérification de plusieurs données objectives, le Comité a rejeté 22 de ces plaintes ou dénonciations, soit parce qu'elles étaient manifestement non fondées (art. 34 L.Contrôle), soit parce que le Comité n'était pas compétent pour en traiter les motifs. Dans ces derniers cas, les plaignants ont été renvoyés, si possible, à l'instance compétente. Dans quelques cas, les autorités policières ou judiciaires ont aussi été informées en raison d'un risque potentiel. Comme cela a été dit, cinq plaintes introduites en 2013 ont donné lieu à l'ouverture d'une enquête de contrôle. Une plainte, qui a été introduite à la fin de l'année, n'a donné lieu à l'ouverture d'une enquête que début 2014. C'est la raison pour laquelle elle n'est pas mentionnée dans ce chapitre.

II.1. LE RÔLE DU SERVICE GÉNÉRAL DU RENSEIGNEMENT ET DE LA SÉCURITE DANS LE SUIVI DE LA SITUATION EN AFGHANISTAN

En décembre 2001, la Belgique décidait d'intégrer l'International Security Assistance Force (ISAF), une force internationale de maintien de la paix en

Afghanistan, qui a été créée au sein des Nations unies. Outre l'OTAN (et ses États membres), une vingtaine d'autres contingents y collaborent.

La majeure partie du contingent belge était stationnée à Kaboul et devait assurer la protection de l'aéroport international. Dans la province de Kunduz, au nord du pays, la Belgique appuyait les équipes provinciales de reconstruction et rendait des avis techniques à l'armée afghane. Enfin, plusieurs avions belges de combat opéraient depuis 2008 à partir de Kandahar.

Afin de se faire une idée globale de la manière dont le service de renseignement militaire était impliqué dans cette opération, le Comité a décidé, en janvier 2010, d'ouvrir une enquête de contrôle *« concernant le rôle du SGRS dans le suivi de la situation en Afghanistan »*.[20] Avec cette enquête de contrôle, le Comité permanent R poursuivait un objectif clair : cartographier de la manière la plus exhaustive possible[21] l'une des missions les plus importantes menées par le SGRS à l'étranger, en vue de tracer un cadre de référence pour les missions futures ainsi que pour les enquêtes de contrôle susceptibles d'être ouvertes à ce sujet.

Les conclusions de la commission d'enquête parlementaire concernant les événements au Rwanda[22], créée en 1997 à la suite de la mort tragique de dix para-commandos belges, ne pouvaient évidemment pas être ignorées. Cette commission a notamment retenu les points suivants en matière de recueil et d'analyse de renseignements :

- Le contingent belge doit toujours disposer d'un réseau de renseignement solide qui lui soit propre, composé d'officiers de renseignement suffisamment formés et maîtrisant, dans la mesure du possible, la langue du pays. À défaut, il doit disposer d'interprètes dignes de confiance.
- Pour l'analyse des renseignements, le service de renseignement militaire doit disposer de suffisamment d'analystes capables d'évaluer le contenu de chaque information. En outre, il doit y avoir un retour systématique d'informations à l'adresse des unités sur le terrain.
- Il est essentiel de réformer le SGRS, notamment en tenant compte de la nouvelle loi (Loi du 30 novembre 1998) sur les services de renseignement et

---

20 Dans le cadre de cette enquête, dont un rapport final classifié « SECRET – Loi 11.12.1998 » très détaillé a été transmis au ministre de la Défense en septembre 2013, le Comité permanent R a pu compter sur le grand esprit d'ouverture dont ont fait preuve le chef et les membres concernés du SGRS. L'organisation irréprochable des visites sur le terrain en Afghanistan mérite également d'être mentionnée.
Le rapport a été discuté dans sa version 'DIFFUSION RESTREINTE' lors de la réunion de la Commission de suivi du Sénat le 12 mars 2014. Lors de cette réunion et par la suite (courrier du 16 juin 2014), le SGRS et le ministre de la Défense ont souhaité ajouter quelques précisions et nuances au rapport. Ces remarques sont prises en considération dans le présent rapport.

21 Seul le recueil de SIGINT en Afghanistan n'a pas été développé. Cet aspect a été repris dans une enquête de contrôle ultérieure (voir II.10.12. Quatre enquêtes de contrôle dans le cadre des révélations d'Edward Snowden).

22 *Doc. parl.* Sénat 1997-1998, 1-611/7.

de sécurité. Le service doit avant tout devenir un instrument efficace et cohérent de soutien pour les responsables des opérations. Il est nécessaire de mettre les capacités d'analyse à la disposition des responsables pour leur permettre de définir des options politiques. Il faut veiller à assurer la diversité des sources d'informations et le caractère contradictoire des analyses. En outre, il importe d'organiser un retour d'informations permanent entre, d'une part, le service et les responsables sur le terrain d'autre part.

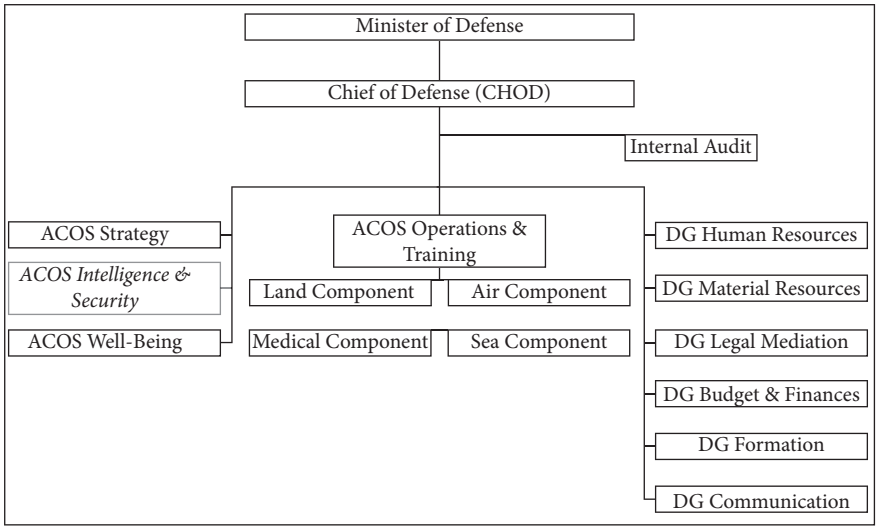
– Le service de renseignement militaire doit renforcer ses unités déployées sur le terrain dans le domaine du renseignement, en particulier en déployant du personnel spécialisé ou des moyens techniques.

II.1.1. LA PLACE, LA STRUCTURE ET LES COMPÉTENCES DU SGRS

II.1.1.1. La place et la structure du SGRS

Pour une bonne compréhension, il importe de savoir comment est structuré le SGRS et où le service se situe au sein des Forces armées (où d'ailleurs d'autres composantes sont chargées de recueillir des renseignements).

Structure des Forces armées belges



Le Service général du renseignement et de la sécurité aussi dénommé *Assistant Chief of Staff Intelligence and Security* (ACOS-IS)[23] est un des départements d'état-major des Forces armées.[24] Au moment où l'enquête a été menée, le service était constitué de quatre divisions.[25]

La Division S(ecurity) réalise les enquêtes de sécurité sur des personnes ou des sociétés déterminées et veille au respect des directives relatives à la sécurité militaire de domaines, de personnes, de systèmes informatiques…

La Division A(ppui) est notamment chargée de la gestion du personnel, la gestion budgétaire, l'ICT et les aspects logistiques qui sont gérés au sein même du SGRS.

La Division C(ounter)I(ntelligence) suit sur le territoire belge ce qui constitue une menace pour les intérêts militaires ou pour d'autres intérêts devant être défendus par le SGRS. Toutefois, cette division a aussi un rôle à jouer dans la « *force protection* » d'unités belges à l'étranger : elle apporte son soutien à ces unités afin de contrer des menaces spécifiques (par exemple, l'infiltration par des groupements locaux).

La Division I(ntelligence), enfin, est l'unité la plus grande du SGRS. Elle se concentre sur des phénomènes qui se produisent à l'étranger et est donc active là où sont engagées les troupes belges. Les services d'analyse de la Division I sont en grande partie organisés par région du monde, mais il existe aussi des bureaux pour les *Naval intelligence* et *Land intelligence* ainsi que pour les questions transnationales. En matière de collecte (recueil de données), différents services sont actifs au sein de la Division : les services *Human Intelligence* (HUMINT), *Image Intelligence* (IMINT), *Signals Intelligence* (SIGINT ou COMINT) et *Open Sources Intelligence* (OSINT). La mission de recueil de renseignements sur place incombe à la Division I/Ops. Les unités d'I/Ops déployées à l'étranger sont désignées sous le label BENIC (*Belgian National Intelligence Cell*) ou BELINT (*Belgian Intelligence*).

II.1.1.2. Les missions du SGRS

Les quatre missions du SGRS sont décrites à l'article 11 L.R&S : remplir la mission de renseignement classique, veiller au maintien de la sécurité militaire, protéger des secrets militaires et effectuer des enquêtes de sécurité. Chacune de ces tâches peut avoir un lien avec des opérations à l'étranger. Ainsi, par exemple,

---

23 Étant donné que la plupart des instructions et ordres permanents de ce service sont rédigés en anglais, le Comité a repris la terminologie militaire employée.

24 La L.Contrôle et la L.R&S utilisent l'appellation « Service général du renseignement et de la sécurité des Forces armées » (SGRS), là où l'Arrêté royal du 21 décembre 2001 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités (AR Défense) parle de Département d'état-Major Renseignement et Sécurité ou *Assistant Chief of Staff Intelligence and Security* (ACOS-IS). Il s'agit d'un seul et même service.

25 En 2013, les Divisions S(ecurity) et C(ounter) I(ntelligence) ont fusionné.

le SGRS a pour mission de recueillir, d'analyser et de traiter des renseignements (en d'autres termes, sa mission de renseignement) relatifs à toute activité qui menace ou pourrait menacer l'accomplissement des « *missions, actions ou opérations dans le cadre national, dans le cadre d'une alliance ou d'une collaboration internationale ou supranationale* » des « *Forces armées belges, des Forces armées alliées ou des organismes de défense interalliés* ». Des informations peuvent aussi être recueillies sur des menaces collectives portant atteinte à « *la vie ou à l'intégrité physique de ressortissants belges à l'étranger et des membres de leur famille* ». La deuxième mission – veiller au maintien de la sécurité militaire[26], par exemple du « *personnel relevant du Ministre de la Défense nationale* » et « *des installations militaires, armes, munitions, équipements, plans, écrits, documents, systèmes informatiques et de communications ou autres objets militaires* » – est également importante dans le cadre d'opérations à l'étranger.

II.1.1.3. Les compétences du SGRS et le principe de territorialité

L'article 11 L.R&S ne laisse planer aucun doute sur le fait que le SGRS peut recueillir des informations *sur* l'étranger. Mais le service peut-il aussi recueillir des informations *à* l'étranger ? Il n'est indiqué nulle part explicitement que le SGRS peut intervenir à l'étranger. Cependant, la possibilité d'intervenir à l'étranger découle logiquement de la description de plusieurs missions (par exemple la sécurité des opérations dans le cadre d'une alliance et la sécurité de ressortissants belges à l'étranger), qu'il est impossible d'accomplir uniquement depuis la Belgique. Il en va de même pour les autres missions. Ainsi, par exemple, en ce qui concerne la « mission de protection », aucune différence n'est faite selon que du personnel ou du matériel se trouve en Belgique ou à l'étranger.

Pour autant, la possibilité pour le SGRS d'intervenir à l'étranger ne signifie pas encore que toutes les méthodes de recueil de renseignements peuvent être utilisées. Ainsi, l'utilisation des méthodes spécifiques ou exceptionnelles n'est autorisée que sur le territoire belge par l'article 18/1, 2° L.R&S. La mise en œuvre de ces méthodes dans le cadre d'une enquête sur une éventuelle menace pesant sur une mission à l'étranger n'est donc possible que sur le territoire belge.

Le SGRS estime que les méthodes MRD peuvent bien être mises en œuvre à l'étranger. Le Comité est d'avis qu'une telle interprétation va à l'encontre de la loi. Il est néanmoins possible d'intercepter des communications émises à l'étranger, par exemple pour des raisons de sécurité et de protection de nos troupes et de celles de nos alliés lors de missions à l'étranger. Le SGRS dispose en effet d'un mandat légal spécifique à cet égard défini par les articles 259*bis* § 5 CP *juncto* et 11 § 2, 3° L.R&S. Avec entre autres objectifs le respect des droits de l'homme et la définition des besoins opérationnels sur le terrain, le ministre de la

[26] Cette mission se limite à l'élaboration de directives et à la garantie du respect de celles-ci, par exemple par la mise en place de contrôles sur place.

Défense a souscrit à l'idée d'accorder une attention spécifique à cette problématique dans le cadre de l'évaluation de la Loi MRD.

II.1.1.4. La communication de renseignements à des pays tiers

La communication de renseignements à des pays tiers et l'utilisation qui peut en être faite constitue un problème spécifique. Conformément aux articles 19 et 20 L.R&S, le SGRS peut/doit collaborer et échanger des informations avec des services étrangers. En outre, la question est de savoir si une telle situation peut engager la responsabilité juridique du service.[27] La *High Court of Justice* britannique a déjà dû se prononcer sur la requête d'un ressortissant pakistanais. Ce Pakistanais prétendait que les membres du GCHQ britannique s'étaient rendus coupables de crimes (complicité de meurtre) en fournissant des renseignements (SIGINT) que la NSA et la CIA auraient ensuite utilisés lors d'attaques de drones ayant entraîné le décès de son père. La *High Court of Justice* a rejeté la requête parce que le membre du service de renseignement n'était pas, dans ce cas-ci, en mesure de déterminer quels renseignements il pouvait ou non transmettre aux responsables sur le terrain.[28]

II.1.1.5. Quelques autres acteurs dans le domaine du recueil de renseignements

Le SGRS est loin d'être la seule entité au sein des Forces armées belges à recueillir des renseignements et à être active à l'étranger.

Ainsi, il y a, au sein des états-majors des Composantes terre, mer et air[29] du Département d'état-major *Operations and Training* (ACOS-Ops & Trg), des services qui, lors de la préparation d'opérations, recueillent et traitent des renseignements par de biais de toutes sortes de sources (par exemple via le SGRS ou via les commandants sur le terrain). La manière dont ces services doivent collaborer entre eux était décrite, au moment de l'enquête, dans une *Standing Operating Procedure* (SOP) *Joint Intelligence, Counter-Intelligence and Security Structure* de 2008[30] qui émanait d'ACOS-Ops & Trg. Cette SOP décrit notamment la position du SGRS dans l'ensemble de la « structure de renseignements » de la Défense. Il était ainsi stipulé que le SGRS recevait les directives du ministre de la Défense et du Chef de la Défense (CHOD), qu'il devait se concentrer sur les renseignements politico-stratégiques et opérationnels et qu'il pouvait, si nécessaire, déployer une cellule de renseignements à l'étranger.

---

27 Voir à cet égard la note de bas de page n°35 relative à l'exposé du SRGS au Sénat.

28 High Court of Justice, Queens Bench division, Administrative Court, *R – Noor Khan v Foreign Secretary* – 2012.

29 Ainsi, par exemple, une division d'Air-Intel était active en Afghanistan. Cette division est spécialisée dans l'analyse des menaces aériennes opérationnelles.

30 Cette *Standing Operating Procedure* a été remplacée par la SOP '*The Belgian Joint Intelligence and Security Structure*' de novembre 2013 (également d'ACOS-Ops & Trg).

Par ailleurs, il existe, au sein de chaque unité opérationnelle des Forces armées, une « fonction S2 » assurée par un officier chargé d'assister le *Commanding Officer* pour communiquer des renseignements relatifs à la situation sur le terrain. Il transmet surtout des informations tactiques.[31]

Pendant les opérations, le *Commanding Officer* est assisté par un *Battle Group Intelligence Cell* (BIC). En outre, un bataillon de reconnaissance *'Intelligence, Surveillance, Target Acquisition and Reconnaissance'* (ISTAR) a été créé en 2011. Ce bataillon est chargé des missions de préparation d'actions sur le terrain et, dans ce cadre, doit recueillir surtout des informations tactiques.[32]

Enfin, il y a encore l' « *Information Operations Group* » de la Force terrestre duquel dépendent « *Psyops* » et « *Human Factor Analysis* ». « *Psyops* » se concentre sur la communication avec la population et les autorités locales là où les troupes belges sont déployées. Le service doit aussi réagir à une éventuelle propagande anti-belge. « *Human Factor Analysis* » étudie divers facteurs humains susceptibles d'influencer une mission, tels que l' « *antropology* » et la « *human geography* ».

II.1.2. LA PLACE ET LES COMPÉTENCES DU SGRS AU SEIN DE L'ISAF

II.1.2.1. L'opération ISAF

Trois jours après les attentats du 11 septembre 2001, le Congrès américain adoptait une résolution autorisant l'usage de la violence armée contre les responsables et éventuels commanditaires de l'attentat. Le 15 septembre 2001, le Conseil nord atlantique de l'OTAN se réunissait et déclarait, à la demande des États-Unis, que l'article 5 du Traité de l'Atlantique nord était d'application : il s'agit du devoir d'assistance des États membres de l'OTAN à un État membre qui a été victime d'une attaque armée.[33]

Le 20 septembre 2011, les États-Unis désignaient Oussama Ben Laden et son organisation Al Qaida comme responsables des attentats du 11 septembre. Ben Laden séjournait à ce moment-là en Afghanistan, où le régime des Taliban le protégeait et refusait de l'extrader.

À partir du début du mois d'octobre 2001, des troupes américaines, britanniques, françaises et australiennes sont entrées en action en Afghanistan, aux côtés de groupes locaux de résistance, et y ont constitué ce que l'on a appelé

---

31 Lors des travaux parlementaires préparatoires de la L.R&S une distinction avait déjà été établie entre d'une part les renseignements stratégiques ou géopolitiques, et d'autre part les renseignements tactiques relatifs à la réalité concrète du terrain et avec le déploiement d'une unité (*Doc. parl.* Chambre, 1996-1997, n° 49-638 /14, 22-24 et 38).

32 Voir également Chapitre V.2.

33 Depuis la création de l'OTAN, c'est la seule fois que cet article a été appliqué.

« l'Alliance du nord ». Cette opération a été baptisée *Operation Enduring Freedom* (OEF).

La Belgique – et donc le SGRS aussi – n'opère pas dans ce cadre.[34] Les activités des Forces armées belges se situent dans le cadre d'un mandat de l'ONU. Ce mandat trouve son origine dans « l'Accord de Bonn » du 5 novembre 2001, prévoyant la création d'une « *International Security Force* » (ISAF). Les signataires afghans de l'accord priaient le Conseil de sécurité des Nations unies « *to consider authorizing the early deployment to Afghanistan of a United Nations mandated force. This force will assist in the maintenance of security for Kabul and its surroundings. Such a force could, as appropriate, be progressively expanded to other urban centres and other areas* ».

Donnant suite à cette demande, le Conseil de sécurité a adopté, le 20 décembre 2001, la résolution 1386 (2001). Cette résolution donnait mandat à l'ISAF pour se déployer « *to assist the Afghan Interim Authority in the maintenance of security for Kabul and its surrounding areas, so that the Afghan Interim Authority as well as the personnel of the United Nations can operate in a secure environment* ».

Dès le 21 décembre 2001, le Gouvernement belge décidait de prendre part à cette mission. À la fin janvier 2002, un premier avion de transport était engagé, tandis que le déploiement de troupes sur le terrain a eu lieu environ un an plus tard.

Au départ, la mission ISAF se trouvait sous un commandement qui changeait tous les six mois. Depuis mars 2003, c'est l'OTAN qui assure le commandement de l'ISAF. Cette force est composée, outre des États membres de l'OTAN, d'une vingtaine d'autres armées.

Il est important de souligner que les troupes de l'ISAF visent à assurer la sécurité de la population et à soutenir les autorités afghanes légitimes de telle sorte que, de concert avec les autorités onusiennes, elles puissent mener à bien leurs missions civiles. D'un point de vue militaire, cela signifie que les troupes de l'ISAF doivent sécuriser le terrain en contrant et en affaiblissant les capacités militaires des adversaires pour que ceux-ci ne soient plus en mesure de déstabiliser le pays. Néanmoins, cette tâche militaire ne constitue pas l'essence de la mission de l'ISAF. Cette mission est principalement orientée vers ce que l'on appelle la « *counter insurgency* » dont le but est de tenter de diminuer, et à terme de faire disparaître, le soutien (passif ou non) dont les insurgés bénéficient dans la population. C'est en effet ce « terreau » qui permet aux insurgés de poursuivre leur résistance. L'opération est finalement une lutte pour gagner les « *minds and hearts* » de la population. Le déploiement militaire

[34] La Belgique n'a pris part à l'*Operation Enduring Freedom* que sous la forme d'opérations de soutien, et ce en dehors du territoire afghan (e.a. l'engagement d'avions de transport C-130 pour l'aide humanitaire, le stationnement d'une frégate en Méditerranée et la mise à disposition d'un équipage pour les appareils AWACS survolant les États-Unis).

peut donc seulement faciliter cette tâche, en créant un cadre sécuritaire dans lequel les autorités civiles peuvent mener à bien leurs missions.

Si l'ISAF n'est pas une pure opération militaire, elle n'a pas non plus pour objectif, contrairement à l'*Operation Enduring Freedom*, de lutter contre le terrorisme. Dans cet ordre d'idées, il convient de mentionner le *CHOD OPORDER for Bel contribution to ISAF* (voir ci-après II.1.3.3.4), qui établit que les troupes belges ne participeront pas aux opérations « *Counter Terrorist* ». Au niveau des flux de renseignements, il n'est toutefois pas exclu que des renseignements qui sont partagés dans le cadre de l'opération ISAF avec des membres de cette coalition, parviennent à l'OEF par le biais des alliés faisant également partie de la *US-led coalition*, même si tel n'est pas le but.[35] L'interdépendance étroite entre les deux missions sur le terrain tient aussi au fait que le commando de l'ISAF et celui des *US forces* en Afghanistan (USFOR-A) se confondent.

II.1.2.2. La présence belge en Afghanistan avec une attention pour le SGRS

Jusqu'au 30 septembre 2012, la majeure partie des hommes composant le contingent belge (320 personnes) assurait la protection du Kabul International Airport (KAIA). La Belgique jouait également un rôle dans l'état-major de l'ISAF à Kaboul, et une unité nationale d'appui stationnait au Kabul International Airport. En ce qui concerne Kunduz, La Belgique a envoyé quelque 25 militaires pour soutenir les équipes provinciales de reconstruction (*provincial reconstruction teams*, PRT), dont la mission était de veiller à l'instauration d'un environnement sécurisant, de coordonner des projets de reconstruction et d'apporter un soutien dans des domaines tels que la santé, l'éducation et les ONG.

D'autre part, la Belgique a fourni, dans le nord de l'Afghanistan, un *Military Assistance Team* (MAT) d'environ 60 militaires, avec pour mission de rendre des avis techniques à l'état-major d'une brigade et d'un bataillon de l'armée nationale afghane.

Par ailleurs, des avions F-16 belges étaient basés à Kandahar. À partir de 2008, la Belgique a participé à l'Operation Guardian Falcon et elle a formé des pilotes afghans et du personnel médical à Kandahar.

Enfin, des militaires étaient aussi déployés à Mazar-E-Sharif.

En ce qui concerne le SGRS, tant la Division I, CI que S ont pris part aux missions en Afghanistan. La composition et les effectifs du SGRS variaient

---

35 Devant la Commission parlementaire Opérations à l'étranger du 19 avril 2012, le SGRS a déclaré ce qui suit : « *En conclusion, nous sommes en mesure de certifier qu'en aucun cas, les informations collectées, ni les analyses fournies aux unités ou aux partenaires ont un objectif de targeting. Tous nos produits servent uniquement à des fins de protection, de prévention et de contextualisation du processus de décision. Mais nous ne pouvons pas nier que dans la communauté dite des Four Eyes (UK/US) ou des Five Eyes (US/UK/CAN/NZ/AUS) d'autres pratiques sont d'application* ».

évidemment en fonction des besoins et des disponibilités. Le suivi de la situation stratégique était assuré par des personnes affectées à ce que l'on appelle la *Belgian National Intelligence Cell* (BENIC). De plus, le SGRS a aussi déployé des membres de son personnel, par exemple chargés de l'échange de renseignements entre les unités belges sur le terrain et les militaires étrangers des troupes alliées. Ils transmettaient ces informations à la *Battle Group Intelligence Cell* (BIC), au S2 et à d'autres partenaires éventuels. En outre, des analystes de la Division I étaient envoyés ponctuellement en Afghanistan. Le Comité a constaté que leurs missions n'étaient pas toujours décrites de manière claire. La Division CI était présente notamment pour détecter d'éventuels problèmes de sécurité pour les unités belges, pour assurer le suivi du personnel local[36] travaillant pour les unités belges et pour évaluer le degré d'appréciation dont bénéficiaient les Belges auprès notamment des Afghans collaborant avec l'ISAF. Enfin, le SGRS-S envoyait une équipe si un audit de sécurité était demandé. Cette équipe contrôlait, le cas échéant, l'application des règles de sécurité relatives au personnel, au matériel et à l'infrastructure.

La situation en Afghanistan n'a pas été suivie que sur le terrain. À Bruxelles, des analystes étaient affectés à un « bureau Afghanistan ». Ils répondaient à des *Requests for Information* (RFI) d'ACOS-IS, de l'OTAN, de l'UE et des « États amis » et procédaient à l'analyse des informations émanant des différents organes de collecte (HUMINT, IMINT, SIGINT…). Le bureau assurait également les briefings pour le staff général, les unités appelées à être déployées sur le terrain, le BENIC ainsi que les partenaires externes (des ambassadeurs par exemple).

La grande majorité des RFI que recevaient les analystes portaient sur des questions d'ordre opérationnel ou tactique (la plupart du temps émanant d'ACO-Ops & Trg) ; les questions stratégiques ne représentaient qu'une minorité des RFI.

Le Comité a dû constater que les analystes du « bureau Afghanistan » ne savaient pas toujours précisément quel type de renseignement les partenaires extérieurs au monde du renseignement et militaire attendaient d'eux. Inversement, les questions posées par ces derniers étaient souvent peu ciblées, dans la mesure où ils ne savaient pas exactement ce que le SGRS pouvait leur communiquer. La présence d'analystes sur le terrain s'est avérée importante pour mieux harmoniser l'offre et la demande.

[36] Le screening de ce personnel LEP (« *Local Employed Personnel* ») est effectué par un bureau « *vetting* » de l'OTAN.

II.1.3. LE CADRE NORMATIF APPLICABLE AU SGRS EN AFGHANISTAN

II.1.3.1. Le cadre national

Il convient évidemment de mentionner en premier lieu l'article 11 L.R&S, qui décrit en termes généraux les quatre missions du SGRS (voir ci-dessus II.1.1.2). En ce qui concerne la mission de renseignement classique, il faut souligner que la loi n'établit aucune distinction entre les renseignements (politico-)stratégiques, opérationnels ou tactiques.[37] Bien qu'il ressorte des travaux préparatoires de la loi que le recueil d'informations purement tactiques n'était pas vraiment considéré comme une mission du SGRS (voir ci-dessus II.1.1.5), le service est cependant actif sur les trois terrains. En matière de repérage d'activités susceptibles de menacer l'accomplissement des missions des forces armées, toutes les formes de renseignements peuvent en effet avoir leur importance.

En outre, l'article 23 de l'Arrêté royal du 21 décembre 2001 déterminant la structure générale du Ministère de la Défense et fixant les attributions de certaines autorités, stipule que le sous-chef d'état-major renseignement et sécurité (ACOS-IS) est notamment chargé de *« l'organisation de l'appui renseignement et sécurité aux opérations »*.

En exécution de la L.R&S, le Comité ministériel du renseignement et de la sécurité (CMRS) pourrait édicter des directives complémentaires sur le fonctionnement du service de renseignement militaire en cas d'opérations à l'étranger, mais il ne l'a pas encore fait. À ce jour, le Comité ministériel n'a pas non plus élaboré de directive concernant l'échange de renseignements avec des services étrangers. Le Comité permanent R a déjà signalé cette lacune à plusieurs reprises.[38]

Les priorités du SGRS sont décrites dans le Plan directeur de renseignement (de la Division I) et dans le Plan directeur de renseignement de sécurité (de la Division CI). Depuis 2001, selon les Plans directeurs de renseignement, l'Afghanistan mérite une analyse permanente et intensive, basée sur une recherche continue et soutenue d'informations par les organes de collecte. Ce n'était pas le cas auparavant. Les Plans directeurs de renseignement de sécurité présentent la même évolution.

---

37 Les renseignements stratégiques sont destinés à aider les décideurs politico-militaires. En revanche, les renseignements opérationnels sont utiles pour la préparation et l'exécution de campagnes sur le terrain (par exemple : quelle est la force militaire de l'adversaire dans une région et quelle est la situation sur le terrain ?). Enfin, les renseignements tactiques sont des renseignements très concrets et concernent des situations très spécifiques. Ces renseignements sont utilisables immédiatement par les personnes présentes sur le terrain.

38 Voir COMITÉ PERMANENT R, *Rapport d'activités 2006*, 128 ; *Rapport d'activités 2007*, 71, *Rapport d'activités 2008*, 6 et 105-106 ; *Rapport d'activités 2009*, 4 et 105-107 ; *Rapport d'activités 2010*, 3-4 et *Rapport d'activités 2012*, 97.

En outre, le *CHOD Operations Order for Bel contribution to ISAF* (2012) a toute son importance. Cette directive décrit en termes généraux la contribution du SGRS dans le cadre de l'intervention militaire en Afghanistan : le service intervient sous l'angle du renseignement lors de la préparation et de l'exécution de l'opération à l'étranger. Cette directive stipule également que la capacité de renseignement belge (BELINT) demeure sous commandement national. Les tâches du BELINT s'étendent au recueil et/ou à la diffusion de renseignements tant stratégiques qu'opérationnels et tactiques.

Par ailleurs, le SGRS a lui-même édicté des directives comprenant davantage de détails pratiques sur tous les aspects organisationnels et opérationnels qui sont importants en cas de déploiement de personnel à l'étranger et précisant davantage la mission en matière de « *force protection* ».

Enfin, il y a encore plusieurs *Fragmentary Orders* (FragO) qui portent sur des missions ponctuelles, par exemple d'une équipe donnée pendant une période déterminée. Un FragO est en fait une spécificité d'un *Operations Order* général pour une mission spécifique.

II.1.3.2. Le cadre international

Au niveau international, il convient surtout de tenir compte du *SACEUR Operational Plan for ISAF* qui offre un cadre pour les services de renseignement des nations qui collaborent aux opérations de l'ISAF.[39] Le principe qui prévaut ici est que les composantes du SGRS sur place ne se trouvent pas sous le commandement d'ISAF/NATO, et ce contrairement aux unités opérationnelles belges. Le BELINT ne peut donc en recevoir aucune instruction spécifique pour mener certaines opérations. Il va de soi que cela n'empêche pas le BELINT de collaborer avec les instances de l'ISAF (par exemple sous la forme d'un échange d'informations). Bien au contraire. Ainsi, le *SACEUR Operational Plan for ISAF* part du principe que les pays participant à l'opération sont disposés à recevoir des *Requests for Information* de l'ISAF et d'y répondre. En outre, le BELINT s'inscrira autant que possible dans la définition des priorités de l'ISAF, de telle

[39] Plusieurs règles internes à l'OTAN sont également d'application, d'une part parce que la Belgique est membre de l'OTAN, et d'autre part parce que l'ISAF opère sous le commandement de l'OTAN. Ainsi, il y a, par exemple, la *NATO Human Intelligence (HUMINT) Policy IMSTAM(INT)-0157-2011(SD1)*, qui reprend la politique générale de l'OTAN en matière de HUMINT. Dans ce document, qui ne concerne pas spécifiquement l'opération ISAF, sont notamment abordés l'échange d'informations nécessaire par les différents États membres et l' « *interoperability* » des systèmes qui sont utilisés à cette fin. Par ailleurs, une référence peut être faite à la *NATO STANAG 2578 – Allied Intelligence Publication – AIntP-5 – Doctrine for Human Intelligence Procedures*. Cette directive définit entre autres les conditions auxquelles un opérateur HUMINT doit satisfaire et indique comment les données sont récoltées au mieux et comment un rapport est rédigé. On y retrouve également l'organisation et la structure HUMINT. Cette instruction vise à adopter une approche uniforme entre les différents États membres et à garantir un certain niveau de qualité.

sorte que son recueil de renseignements contribue aux objectifs en matière de renseignements définis par l'*Operation Plan*.

II.1.3.3. Quelques points à améliorer[40]

II.1.3.3.1. Des normes intégrées, des notions de base communes et des objectifs précis en matière de renseignement

Le Comité permanent R estime qu'une plus grande attention pouvait être accordée à l'harmonisation des documents susmentionnés, même s'ils ne se contredisaient pas. Ainsi, il n'y a que peu – voire pas – d'intégration entre les normes belges et internationales. Il s'agit, il est vrai, de niveaux de compétences différents, indépendants les uns des autres, mais pour les personnes sur le terrain, cette situation n'offre aucun point de repère.

Le Comité est aussi d'avis qu'au niveau des normes belges, il doit être possible d'utiliser des notions de base communes, dans le cadre desquelles toutes les missions et les tâches internationales du service de renseignement militaire pourraient se situer. Ces notions de base communes devraient découler des menaces décrites dans la L.R&S, à partir desquelles l'objectif serait d'en élaborer une description plus précise pour le SGRS, les bureaux et chaque membre du personnel. En d'autres termes, l'on doit s'efforcer de traduire l'assignation de tâches en besoins d'informations et en moyens à engager, de sorte que tous les collaborateurs connaissent précisément leurs objectifs en matière de renseignements.[41] Cette constatation vaut tant pour la préparation d'une opération que pour son exécution.

Ainsi, le rôle précis du SGRS dans la préparation d'une mission internationale n'était, jusque récemment, que peu – voire pas du tout – défini. Cela s'est traduit, par exemple, dans le fait que même après la décision du Gouvernement en 2002 de participer à l'intervention internationale en Afghanistan, « l'effort de renseignement » concernant la situation en Afghanistan est resté très limité.

II.1.3.3.2. Une méthodologie documentée dans le cadre de la préparation d'une mission

Le Comité a dû constater que dans le cadre de la préparation d'une mission, aucune méthodologie documentée n'était utilisée, ce qui n'est plus le cas aujourd'hui. Depuis environ deux ans, ACOS-Ops & Trg utilise la méthode *Comprehensive Preparation of the Operational Environnement* (CPOE) pour la

---

40 Au cours de l'enquête, le SGRS a anticipé plusieurs remarques qui ont été formulées et a procédé à une série de changements.

41 Lors de l'audit du SGRS en 2011, l'absence d'une telle approche structurée a été pointée du doigt (COMITÉ PERMANENT R, *Rapport d'activités 2011*, 7-14 et 104-107).

préparation des missions. En ce qui concerne la fonction de renseignement, il apparaît qu'un rôle important, mais pas exclusif, revient au SGRS. Par ailleurs, le Comité encourage à (continuer à) élaborer et suivre une telle doctrine ou méthodologie.

II.1.3.3.3. Une méthodologie documentée dans le cadre de l'exécution d'une mission

Lors de l'exécution de l'opération en Afghanistan aussi, les objectifs du SGRS en termes d'informations et de renseignements n'étaient pas toujours bien précisés. Idéalement, les besoins en matière d'informations et de renseignements et les moyens à mettre en œuvre devraient être définis, en partant des objectifs et des menaces énumérés dans la L.R&S.

II.1.3.3.4. Une approche intégrée pour toutes les divisions

L'enquête a montré que jusqu'à la fin de l'année 2012, il n'existait aucun document où les Divisions I, CI et S étaient reprises ensemble et de manière intégrée. Certes, le *CHOD OPORDER for Bel contribution to ISAF* comprenait plusieurs dispositions relatives à la mission de renseignement, mais il n'indiquait rien sur les contributions respectives des Divisions CI et S. Cette lacune a été comblée en janvier 2013 en ce qui concerne la Division CI.[42]

II.1.3.3.5. Un manque de clarté sur la nature des renseignements à recueillir

Le Comité permanent R a constaté un manque de clarté concernant la nature des renseignements sur lesquels le SGRS doit se concentrer en priorité : stratégiques, opérationnels et/ou tactiques. Selon le *SOP OPS – Joint Intelligence, Counter-Intelligence and Security Structure* d'ACOS-Ops & Trg (voir II.1.1.5), le SGRS devait fournir avant tout des renseignements politico-stratégiques et opérationnels. Dans le CHOD OPORDER relatif à l'Afghanistan (voir II.1.3.3.4), le SGRS se voyait toutefois aussi attribuer une tâche en matière de *« tactical intelligence »*.

Dans la pratique, il apparaît que les services d'analyse du SGRS sont plutôt orientés vers les renseignements stratégiques, alors que les gens de terrain ont surtout besoin de renseignements opérationnels/tactiques.

Le Comité permanent R constate que ce flou existe depuis un certain temps déjà. Cette question n'est pas sans conséquence sur la manière dont le SGRS organise sa collecte et son traitement des renseignements. La confusion des différents types de renseignements peut nuire à l'efficacité. De plus, l'impact sur les domaines de connaissances nécessaires pour la collecte et l'analyse se traduit

[42] Depuis lors, l'engagement conjoint des divisions est une réalité sur le terrain.

par une approche plus « politico-civile » pour les renseignements stratégiques, opposée aux « *facts and figures* militaires » pour les renseignements tactiques et opérationnels.

II.1.4. L'ÉVALUATION PAR LES CLIENTS DU SGRS

Le Comité permanent R a interrogé les principaux clients du SGRS, c'est-à-dire le SPF Affaires étrangères (surtout son « centre de crise » pour ce qui est de la protection des ressortissants belges à l'étranger, et le « service de sécurité » pour ce qui concerne la sécurité des postes diplomatiques à l'étranger), ACOS-Ops & Trg qui, au sein de la Défense, est chargé du commandement opérationnel des forces d'interventions, et le Cabinet du ministre de la Défense.

Dans l'ensemble, il ressort que ces « clients » sont assez satisfaits de la collaboration avec SGRS : d'une part, le service réagit avec célérité aux questions qui lui sont posées et fait preuve de flexibilité, et d'autre part, la pertinence et l'acuité de ses produits sont reconnues. En outre, le SGRS jouit d'une excellente réputation quant à la fiabilité de ses productions.

Le SGRS entretient avec ses partenaires à la fois des contacts formels et structurels et une multitude de contacts informels qui favorisent la flexibilité et la souplesse.

Les produits du SGRS couvrent essentiellement les thématiques sécuritaires au niveau opérationnel, tactique et stratégique et, dans une moindre mesure, les thématiques politiques. Néanmoins, le SGRS a aussi pour mission de couvrir les domaines économiques, sociaux, médiatiques, comme le prévoit le « *Comprehensive Preparation of the Operational Environnement* » (CPOE). Selon le SGRS, ces domaines ne sont que partiellement couverts par manque de personnel. Aussi a-t-il été récemment convenu que la Défense se concentrerait sur les problématiques sécuritaires, tandis que les Affaires étrangères se focaliseraient sur le domaine CPOE.

ACOS-Ops & Trg a pourtant fait savoir qu'il attendait une plus grande implication du SGRS, en particulier dans la mise en œuvre du CPOE. Étant donné l'importance de cette mission, tant pour les autorités militaires que pour le Cabinet du ministre, il y aurait lieu pour le SGRS de réfléchir à sa capacité à répondre à cette demande.

Enfin, le Comité a dû constater que les clients ne savaient pas suffisamment ce que peut produire le SGRS – même s'ils sont satisfaits de la contribution du SGRS – et donc ne lui posaient pas toutes les questions qui pouvaient l'être. De son côté, le service Analyse du SGRS regrette l'absence de feedback sur ses produits.

II.1.5. CONCLUSIONS

II.1.5.1. Le contrôle de légalité et d'autres aspects réglementaires

Le Comité estime que le SGRS remplissait ses missions en Afghanistan conformément à la législation belge et internationale, nonobstant la multitude de normes et leur manque d'intégration.

Le Comité regrette toutefois que le SGRS ne se soit pas penché sur sa responsabilité éventuelle lorsqu'il fournit des informations ou des renseignements à un service de renseignement étranger ou à une instance étrangère, et ce malgré l'absence de directive (à ce stade) du Comité ministériel du renseignement et de la sécurité.

Enfin, le Comité attire l'attention sur la nécessité de redéfinir les concepts de renseignements « opérationnels », « tactiques » et « stratégiques ». La plupart des normes nationales et internationales utilisent ces notions pour délimiter les différents domaines de compétences des différents acteurs (BENIC, officier renseignement S2, BIC…). Pour autant, la Loi du 30 novembre 1998 n'utilise pas cette terminologie. Cette loi détermine en effet la compétence du SGRS en fonction des menaces à suivre. Pour mener à bien cette mission, le SGRS doit collecter l'ensemble des informations disponibles. Le Comité constate également que, dans la pratique, ces notions ne sont pas déterminantes pour la collecte ni pour la diffusion des informations. Le Comité estime dès lors nécessaire de réfléchir au lien entre ces notions et les missions légales du SGRS. L'existence du bataillon ISTAR rend cette réflexion d'autant plus nécessaire (cf. *supra*).

II.1.5.2. La nécessité d'évaluer les risques pour le personnel dans des zones de conflit

Le Comité a pu constater à plusieurs reprises que le personnel du SGRS courait des risques dans certaines situations. Aussi le Comité insiste-t-il sur la qualité de la formation préalable à un déploiement et sur la nécessité de disposer de moyens matériels et logistiques adéquats.

Le Comité a constaté plus particulièrement que le SGRS n'avait pas encore procédé à une évaluation globale des risques inhérents à l'engagement de personnel militaire et civil en zones de conflit. Une telle évaluation devrait par exemple permettre de juger si un déploiement de personnel civil (analystes) est envisageable, et si c'est le cas, de définir les besoins en formation et en matériel. De plus, une telle réflexion devrait permettre de préciser le rôle des analystes dans l'environnement où se passe la collecte d'informations, ceci en vue de garantir l'objectivité de la fonction d'analyse et d'éviter toute influence. Le personnel militaire du SGRS devrait évidemment être aussi intégré dans cette réflexion sur les risques, ce qui, selon le Comité, n'est pas encore suffisamment le cas.

II.1.5.3. La nécessité d'avoir une approche systématique de l'engagement du SGRS en zone de conflit

Le Comité estime que le déploiement du SGRS en Afghanistan s'est effectué de manière pragmatique. Une telle manière d'agir n'est pas mauvaise en soi, mais elle comporte le risque de négliger certains aspects conceptuels. Une approche intégrée partant des menaces à suivre permet d'établir des liens cohérents entre la L.R&S, le « *mission statement* » du SGRS, le plan stratégique intégré de I, CI et S, les Plans directeurs de renseignement et les Plans directeurs de renseignement de sécurité, le plan de collecte et surtout les moyens humains et matériels à mettre en œuvre pour atteindre ces objectifs (en matière de renseignement). De manière générale, seule une approche intégrée permettrait d'évaluer en toute objectivité si le SGRS dispose d'effectifs suffisants et de matériel adéquat pour remplir sa mission légale.

II.1.5.4. La nécessité de disposer du matériel adéquat

Le Comité a dû constater que l'intégrité physique des membres du personnel du SGRS pouvait être mise en danger. Il est dès lors indispensable qu'ils disposent de moyens matériels adéquats. De manière générale, c'est certainement le cas. Toutefois, les moyens de communication mis à disposition du BENIC pourraient être améliorés.

II.1.5.5. Les recommandations de la commission Rwanda

II.1.5.5.1. Des règles d'engagement claires traduites en directives compréhensibles

Le Comité a attiré l'attention sur la diversité des normes nationales et internationales qui s'appliquaient au déploiement des forces armées belges en Afghanistan. En outre, ces réglementations sont particulièrement complexes, d'une part en raison d'un manque d'intégration (en l'absence de code), et d'autre part d'un défaut de « traduction » de ces règles en directives compréhensibles. Une telle complexité peut avoir pour conséquence la méconnaissance ou la mauvaise interprétation de ces normes. Aussi le Comité plaide-t-il en faveur d'une présentation intégrée des normes en vigueur.

Par ailleurs, en ce qui concerne les règles nationales, le Comité estime qu'une meilleure intégration de celles-ci s'impose, par exemple en partant des missions légales du SGRS.

II.1.5.5.2. Une préparation adéquate de la mission

Le Comité a pu constater que les membres du SGRS avaient bénéficié d'une préparation spécifique avant leur départ en mission. Celle-ci abordait différents aspects tels que les comportements à adopter sur place, la situation dans le pays ainsi qu'un exposé pratique sur les règles d'engagement. À l'exception de ce dernier aspect, le Comité a pu récemment constater des améliorations significatives.

II.1.5.5.3. Un réseau de renseignement solide

La commission Rwanda a insisté pour que le SGRS dispose à l'avenir d'un réseau de renseignement propre ainsi que d'officiers de renseignement formés, entraînés et maîtrisant la langue ou pouvant faire appel à des interprètes. Le Comité a pu constater que cet objectif avait été atteint, tout en relevant deux points d'amélioration possibles.

D'une part, la formation du personnel du SGRS déployé pourrait encore être améliorée. Le SGRS doit fournir un effort important et constant en la matière. Les récentes adaptations ont apporté une valeur ajoutée indéniable, mais elles restent insuffisantes aux yeux du Comité. La formation doit être pratique et flexible sans dépendre de la disponibilité des formateurs.

D'autre part, le rôle du SGRS dans la préparation d'une mission internationale doit être renforcé. À cet égard, le SGRS doit s'inscrire dans la méthodologie du « *Comprehensive Preparation of the Operational Environnement* » (CPOE), et s'adapter aux besoins exprimés par les partenaires au sein de l'armée en faisant preuve de proactivité. Cela implique notamment que le SGRS effectue des analyses dans des domaines qui relèvent de sa responsabilité.

II.1.5.5.4. Disposer de suffisamment d'analystes compétents

La commission Rwanda a préconisé une réforme du SGRS, afin que ce service devienne un instrument efficace et cohérent pour les responsables d'une opération. La commission a proposé également d'améliorer les capacités d'analyse en vue d'élaborer des options politiques pour les responsables.

Le Comité a constaté que ces objectifs étaient en grande partie atteints. En effet, le SGRS est devenu un partenaire incontournable et important pour le recueil et l'exploitation d'informations au profit des troupes sur le terrain, en particulier dans le cadre de la « *force protection* ». De même, son rôle de conseiller des instances hiérarchiques et politiques s'est confirmé, tout comme ses interventions dans le cadre de la préparation des opérations ou lors de leur exécution.

Le Comité estime cependant que le SGRS ne peut encore jouer pleinement son rôle de conseiller des instances hiérarchiques et politiques, et ce peut-être en partie à cause d'un manque d'analystes. Le service pourrait toutefois pallier ce

manque en recrutant des analystes davantage en fonction d'objectifs clairs en matière de renseignements.

Les clients du SGRS ont confirmé leur satisfaction sur les produits du SGRS, tout en reconnaissant ne pas connaître suffisamment ce qui pouvait leur être livré. Les analystes quant à eux estiment ne pas obtenir suffisamment de feedback de la part de leurs clients quant aux produits qu'ils leur livrent. Ces constatations plaident en faveur d'une relation plus proactive entre le SGRS et ses clients. Concrètement, le SGRS devrait s'enquérir plus activement des besoins et des souhaits des clients internes et externes de la Défense afin d'optimaliser l'efficience de ses produits. Le Comité est bien conscient que les clients eux-mêmes doivent contribuer à cette optimalisation.

II.1.5.5.5. La nécessité de déployer des équipes spécialisées

Lors de sa mission en Afghanistan, le Comité a pu constater que les équipes déployées par le SGRS effectuaient un travail très professionnel, et ce à la satisfaction des autorités belges et étrangères. Les commandants des détachements belges sur place reconnaissent qu'il existe un retour systématique des informations vers les unités de terrain.

II.2. NOTES SECRÈTES SUR L'ÉGLISE DE SCIENTOLOGIE DANS LA PRESSE

Le 17 janvier 2013, la presse citait des passages de la note de la VSSE intitulée « *Église de Scientologie – Infiltration de la communauté congolaise ou d'origine congolaise de Belgique – Implantation en République démocratique du Congo* ».[43] Peu avant, le service avait transmis cette note du 11 décembre 2012, classifiée secrète, à certaines autorités. Il ressortait de ces articles que l'Église de scientologie tentait d'élargir ses activités en Afrique et, dans ce cadre, cherchait des relais dans la communauté belgo-congolaise. En outre, plusieurs responsables politiques étaient cités nommément[44] : Bertin Mampaka, alors vice-président du Parlement de Bruxelles-Capitale et conseiller communal à Bruxelles[45] ; Justine Kasa-Vubu, ancienne ministre du premier gouvernement de Laurent-Désiré Kabila, puis ambassadeur à Bruxelles ; Gisèle Mandaila, pendant cette période, députée bruxelloise et en 2004, secrétaire d'État aux Familles et Personnes handicapées et conseillère communale à Etterbeek ; et enfin Pierre Migisha, qui, à l'époque de la fuite, était député bruxellois et conseiller communal à Anderlecht.

43 A. CLEVERS, *La Dernière Heure*, 17 janvier 2013 (La scientologie infiltre les milieux belgo-congolais) ; K. VAN EYCKEN et H. ADRIAEN, *Het Laatste Nieuws*, 17 janvier 2013 (Scientology infiltreert in Congolese gemeenschap in Brussel).

44 Les noms de ces responsables politiques ont été largement cités dans les médias.

45 Ensuite, l'intéressé a été nommé sénateur par le Parlement de la Communauté française.

À la demande de la Commission de suivi, le Comité a ouvert une enquête de contrôle visant à examiner tant la réalisation que la diffusion de la note.

À peine quinze jours plus tard, la presse a fait état d'une autre note de la VSSE[46], qui portait cette fois sur l'« *Analyse de phénomène – Activités non étatiques d'ingérence* ». De nombreux responsables politiques auraient également été cités dans ce rapport secret pour leurs relations avec, entre autres, l'Église de scientologie. La ministre de la Justice a dès lors chargé le Comité d'ouvrir une enquête de contrôle afin d'examiner si la directive ministérielle du 25 mai 2009 (en vertu de laquelle le ministre de la Justice doit être informé chaque fois que le nom d'un parlementaire fédéral est mentionné dans un rapport) a été correctement appliquée, et s'il était indiqué ou non de citer nommément des parlementaires dans une analyse de phénomène. Le lendemain, la Commission de suivi a donné pour mission au Comité d'élargir la première enquête à la réalisation et la divulgation de cette analyse de phénomène, ainsi qu'à la question de savoir si les services de renseignement belges ont correctement appliqué le principe du « *need to know* ».[47]

Étant donné que les missions que la Commission de suivi et la ministre de la Justice ont confiées au Comité portaient en grande partie sur la même problématique, le Comité a décidé de réunir tous ces aspects dans une seule et même enquête intitulée « *Enquête de contrôle sur la manière dont la VSSE a réalisé et diffusé la note concernant l'infiltration par le mouvement-Scientologie de la communauté congolaise à Bruxelles et le rapport 'Analyse de phénomènes – Activités non étatiques d'ingérence', en examinant également la problématique de la mention de noms de mandataires politiques et des listes de destinataires ainsi que leur 'need-to-know'* ».[48]

---

46 M. BUXANT et S. SAMYN, *De Morgen*, 2 février 2013 (Staatsveiligheid houdt Wetstraat in de gaten).

47 Le Comité a également été chargé d'effectuer une « analyse transversale » sur la manière dont les services de renseignement recueillent des informations sur des mandataires politiques (II.4).

48 Le Comité permanent R n'a pas été le seul à ouvrir une enquête. En raison des différentes fuites, la VSSE a déposé plainte contre X avec constitution de partie civile, début février 2013, pour violation de l'article 11 de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS). Le Comité n'a pas pu consulter l'enquête judiciaire. L'Autorité nationale de sécurité (ANS) a elle aussi ouvert une enquête de sécurité auprès des destinataires tant de la première note que de l'analyse de phénomène. Le Comité permanent R ignore aussi les résultats de cette enquête. Enfin, le 20 mars 2013, une plainte a été déposée au nom de l'ASBL Église de scientologie de Belgique auprès du Comité permanent R. L'enquête qui en a résulté s'est clôturée début 2014 (II.11.8). Une « Proposition visant à instituer une commission d'enquête parlementaire chargée d'examiner les cas dans lesquels le Service de la Sûreté de l'État surveille des hommes ou femmes politiques élus » a également été déposée au Parlement (*Doc. parl.* Chambre 2012-2013, n° 53-2652/001 et *Doc. parl.* Sénat 2012-13, n° 5-2034/1).

II.2.1. LA NOTE SECRÈTE DU 12 DÉCEMBRE 2012 SUR L'ÉGLISE DE SCIENTOLOGIE

II.2.1.1. Le contenu de la note

La VSSE doit suivre les activités qui constituent ou peuvent constituer une menace pour la sûreté de l'État et la pérennité de l'ordre démocratique et constitutionnel. Dans l'exercice de cette mission, la VSSE a découvert des noms de mandataires politiques qui pouvaient être mis en relation avec l'Église de scientologie. Plusieurs notes ont été rédigées, dont celle du 11 décembre 2012, qui a fait l'objet d'une fuite et qui traitait de la relation des quatre responsables politiques susmentionnés avec l'Église de scientologie. Cette note peut se résumer comme suit :

- un des quatre intéressés est approché par l'Église de scientologie ;
- un second entretient des relations avec l'Église de scientologie ;
- quant aux deux autres, la VSSE avance, sur la base de faits relatés par les services extérieurs, qu'ils sont très proches, voire membres, de l'Église de scientologie.

Selon le Comité, la rédaction de cette première note s'inscrivait dans le cadre de ses compétences légales telles que décrites dans la Loi du 30 novembre 1998. Le Comité s'est plus précisément référé à l'article 8, 1° e) et g) relatif aux « organisations sectaires nuisibles » et à l'« ingérence ». Il n'a relevé aucune indication d'irrégularités dans le recueil des renseignements ayant servi de base à la note. De plus, cette note était nuancée.

II.2.1.2. Les destinataires de la note et leur need to know

La note en question a été remise à six destinataires, à savoir les ministres de la Justice et des Affaires étrangères, l'ambassadeur de Belgique au Congo, ainsi que le président, le chef de la sécurité et le directeur Afrique du SPF Affaires étrangères. Tous disposaient de l'habilitation de sécurité requise. En leur qualité de ministres, hauts fonctionnaires ou diplomates et en vertu de leur responsabilité en matière de diplomatie et de relations internationales, ils satisfaisaient aux exigences du *need to know*. La note portait en effet sur l'infiltration de la communauté congolaise ou d'origine congolaise en Belgique par l'Église de scientologie et son implantation en République démocratique du Congo. Le Comité a estimé que ces renseignements étaient importants pour les autorités chargées de la politique étrangère de la Belgique. Ces informations

devaient donc être transmises aux autorités concernées en application de l'article 19 L.R&S.[49]

II.2.1.3. L'obligation d'information

Durant la période sur laquelle portait l'enquête de contrôle, deux directives imposaient à la VSSE d'informer le ministre de la Justice lorsque des responsables politiques faisaient l'objet d'activités de renseignement : une directive ministérielle du 25 mai 2009 – établie à la suite des recommandations du Comité permanent R dans le cadre d'une enquête de contrôle antérieure[50] – et une instruction interne du 27 mars 2012.[51]

La directive du 25 mai 2009 stipule que le ministre de la Justice doit être informé chaque fois que le nom d'un parlementaire fédéral en fonction apparaît dans un rapport. Comme aucun des quatre intéressés n'exerçait un tel mandat pendant la période concernée, la ministre de l'époque ne devait pas être informée.

Le champ d'application de l'instruction interne du 27 mars 2012 est à la fois plus restreint et plus vaste que celui de la directive ministérielle : d'une part, cette instruction interne ne concerne que les mentions dans des rapports des services extérieurs de la VSSE, mais d'autre part, elle porte sur tous les ministres et mandataires politiques, y compris ceux des Communautés et Régions.

Concernant Justine Kasa-Vubu, la ministre ne devait pas non plus être informée, conformément à cette directive, car l'intéressée n'était pas un mandataire politique belge.

Quant aux trois autres mandataires, il convenait d'en informer la ministre. En ce qui concerne Bertin Mampaka, la VSSE avait déjà remis à la ministre de la Justice, en juillet 2012, une première note faisant état de contacts qu'il entretenait avec l'Église de scientologie. Cette note peut donc être considérée comme une information. Quant à Pierre Migisha et Gisèle Mandaila, seule la note du 11 décembre 2012 peut être considérée comme correspondant à l'information requise. La VSSE aurait donc dû informer la ministre plus rapidement en ce qui concerne les deux mandataires précités.

---

49 « *Les services de renseignement et de sécurité ne communiquent les renseignements visés à l'article 13, deuxième alinéa, qu'aux ministres et autorités administratives et judiciaires concernés, aux services de police et à toutes les instances et personnes compétentes conformément aux finalités de leurs missions ainsi qu'aux instances et personnes qui font l'objet d'une menace visée aux articles 7 et 11.* »

50 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 19-31 (II.2. « Dossiers réservés » à la Sûreté de l'État).

51 Voir également à cet égard II.4.2.1.3.

II.2.2. L'ANALYSE DE PHÉNOMÈNE RELATIVE AUX ACTIVITÉS NON ÉTATIQUES D'INGÉRENCE[52]

II.2.2.1. Le contenu de l'analyse de phénomène

Le rapport dont il est question ici constitue la quatrième analyse de phénomène rédigée par la VSSE. Le Comité permanent R a une nouvelle fois souligné[53] l'utilité de ce type de rapport qui « *expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une 'évaluation de risque' à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique […]* ».[54]

Le Comité a toutefois constaté que la direction de la VSSE n'avait donné aucune directive claire aux rédacteurs et avait omis de définir les objectifs et la méthodologie. L'objectif de cette analyse de phénomène n'était que brièvement expliqué dans l'introduction : « *La VSSE tente au travers de cette analyse de phénomène d'esquisser une image des activités d'ingérence de groupements et/ou organisations au sein des milieux politiques et économiques* ». À cet égard, la VSSE a souligné que toute organisation est en droit de faire du lobbying pour promouvoir ses objectifs. Selon la VSSE, lorsque des personnes occupant des postes à responsabilités sont contactées pour influencer les processus décisionnels ou exercer des influences, la zone grise du lobbying est dépassée et on peut parler d'« ingérence » au sens de l'article 8, 1° g) L.R&S.

Le Comité a en outre critiqué le fait que le rapport ne décrit pas clairement[55] la stratégie employée par l'Église de scientologie pour tenter d'« *influencer des processus décisionnels par des moyens illicites, trompeurs ou clandestins* » (art. 8, 1° g) L.R&S). Le rapport ne fait pas non plus mention des objectifs réels de l'organisation ni de la manière dont les contacts sont établis et entretenus. Le Comité a dès lors estimé que dans une telle analyse, il était recommandé d'expliquer, à titre d'exemple, la stratégie d'un recrutement : premier(s) contact(s) par avec un intermédiaire, approche de parlementaires, approche via des

---

52 La problématique de l'information au ministre de la Justice en cas d'activités de renseignement à l'égard de mandataires politiques est abordée dans l'enquête intitulée « le suivi de mandataires politiques par les services de renseignement » (II.4).

53 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 14-28 (II.2. Le suivi par certains services de renseignement étrangers de leur diaspora en Belgique).

54 Extrait de l'« Extrémisme islamique en Belgique, Analyse du phénomène » de la VSSE.

55 La stratégie suivie apparaît parfois de manière implicite. Les auteurs du rapport d'analyse ont probablement trop compté sur le fait qu'il s'agissait d'une évidence pour le lecteur.

organisations qui ne révèlent pas leur lien avec l'Église de scientologie, offre d'avantages ou d'aide (par exemple, participation à des cours ou aide financière pour des projets)…

Cependant, le Comité s'est surtout montré critique quant à la manière dont des noms de mandataires ou ex-mandataires politiques et de leurs collaborateurs étaient mentionnés en détail.[56] Le rapport donne une impression de nivellement, où les noms de toutes les personnes citées ont la même valeur informative, même si certains noms apparaissent à plusieurs reprises et même si l'intervention de certains est précisée. Le Comité a souligné que la mention du nom d'une personne dans un rapport de la VSSE revêt un caractère « stigmatisant », même si la diffusion du rapport est limitée à un nombre restreint de personnes.

Le Comité a insisté sur le fait que si l'énumération de noms avait pour but de démontrer la portée des contacts de l'Église de scientologie et de ses activités, il est essentiel de préciser le lien exact entre une personne donnée et l'Église de scientologie : y a-t-il eu une ou plusieurs tentatives d'approche, ces tentatives ont-elles réussi, dans quel contexte ont-elles eu lieu, l'intéressé a-t-il participé passivement ou activement aux activités (par exemple en prononçant un discours lors d'une conférence), l'intéressé est-il conscient que les activités ont été organisées par l'Église de scientologie… En d'autres termes, si la VSSE estime nécessaire de citer des noms – et il s'agit là de sa responsabilité – elle doit indiquer le degré d'implication de chaque personne dans son rapport.

En revanche, si l'objectif est bel et bien de démontrer le développement des activités de l'Église de scientologie et de démontrer par le détail qu'une stratégie de contacts et de recrutement bien précise est mise en œuvre (en d'autres termes, si l'on souhaite décrire un phénomène), il n'est pas nécessaire de citer des noms. Dans ce cas, il suffit de mentionner des exemples abstraits, en indiquant comment et où l'Église de scientologie recrute des membres et développe des réseaux.

II.2.2.2. Les destinataires de l'analyse de phénomène et leur need to know

Outre la diffusion au sein même de la VSSE, l'analyse de phénomène a été envoyée à 33 personnes.

Avant la diffusion, la VSSE avait contacté l'Autorité nationale de sécurité. Elle voulait s'assurer que les destinataires étaient titulaires d'une habilitation de sécurité du niveau requis, ce qui s'est avéré être le cas, à une exception près.[57] La VSSE a fait dûment signer un accusé de réception par le destinataire ou son officier de sécurité. Dans une lettre accompagnant l'analyse de phénomène, la VSSE a également insisté

[56] Le Comité a constaté que les auteurs du rapport d'analyse avaient décidé de citer des noms sans que la direction ne soit intervenue. Le Comité permanent R s'est interrogé sur cette décision.

[57] Un destinataire n'était pas titulaire d'une habilitation de sécurité et n'a donc pas reçu d'exemplaire de l'analyse de phénomène.

sur la nécessité de respecter scrupuleusement la Loi relative à la classification et sur le préjudice grave qui pourrait résulter d'une utilisation inappropriée du rapport.

Le Comité permanent R a toutefois dû constater qu'il n'existait pas de liste préétablie de destinataires pour ce type d'analyses : le choix des destinataires était laissé à l'appréciation des rédacteurs. Dans ce cas-ci, la hiérarchie a néanmoins ajouté quelques noms.

Il est évident que la large diffusion qui s'en est suivie a multiplié le risque de fuites. Le Comité permanent R a cependant mis l'accent sur le fait que la ou les personne(s) à l'origine des fuites est (sont) en premier lieu responsable(s) des effets négatifs pour la VSSE et les mandataires cités (naturellement dans les hypothèses de fuites volontaires ou de négligence ayant permis que les informations se retrouvent dans la presse).

À l'estime du Comité, une réflexion approfondie n'a pas été menée avant de dresser la liste de destinataires. Soit la VSSE s'est fondée de manière générale sur la « compétence légale » de certaines personnes (à savoir du Premier ministre, des vice-Premiers ou des ministres membres du Comité ministériel du renseignement et de la sécurité), soit, plus spécifiquement, sur leur présumé *need to know*. Toutefois, le problème réside dans le fait que le « besoin d'en connaître » dépend de la finalité du produit diffusé. La volonté est soit d'informer une personne d'un phénomène général d'ingérence, soit d'attirer l'attention sur des risques précis qu'une personne ou une instance peut ou pourrait rencontrer dans le cadre de sa fonction. Dans ce dernier cas, le Comité a jugé qu'il n'était pas nécessaire de remettre le rapport complet. En revanche, il est indiqué de limiter l'information à ce qui est utile pour le destinataire concerné. Néanmoins, si le rapport a pour objectif d'informer à propos d'un phénomène général, l'envoi du rapport dans son intégralité est justifié. Mais encore s'agit-il de savoir s'il appartient à la VSSE de transmettre un tel rapport à quatorze fonctionnaires/diplomates du SPF Affaires étrangères. Le Comité s'est demandé s'il ne serait pas plus opportun d'envoyer des rapports à un seul destinataire qui ferait office de point de contact au sein du département et qui est en mesure d'apprécier le « besoin d'en connaître » de chacun de ses collègues.[58]

Concrètement, en ce qui concerne l'analyse de phénomène « ingérence », le Comité a estimé qu'il eut été plus approprié de diffuser le rapport de manière plus ciblée, en fonction des besoins de chaque destinataire. Ce qui aurait probablement permis de limiter l'impact négatif de la fuite.

II.3. UN INFORMATEUR AU SEIN DU VLAAMS BELANG ?

Début 2013, deux rapports secrets de la Sûreté de l'État ont été rendus publics (voir II.2). Lors des débats parlementaires qui ont suivi, la ministre de la Justice

[58] La VSSE aurait récemment décidé de recourir désormais à un tel point de contact.

a déclaré que ce n'est pas « *de opdracht [van de VSSE] om individuele parlementsleden te volgen. Dat is niet de opdracht van die dienst en het gebeurt in de praktijk ook niet* ».[59, 60] Bart Debie, ancien commissaire de police d'Anvers et ancien conseiller en sécurité de Filip Dewinter (Vlaams Belang), a estimé qu'il devait démentir ces affirmations. Dans un article de presse[61], il a fait savoir : « *Wat ze met andere politici doen, weet ik niet. Maar de Staatsveiligheid heeft het Vlaams Belang jarenlang met héél véél aandacht gevolgd. En ik kan het weten, want ik was er zelf bij betrokken* ».[62] Bart Debie a déclaré avoir été informateur de la VSSE de 2007 à 2010 – période durant laquelle il était porte-parole/conseiller en sécurité du Vlaams Belang. Ces propos ont suscité de vives réactions de la part de Filip Dewinter, de la ministre de la Justice et de l'administrateur général de la VSSE.

Juste avant, le Comité permanent R avait ouvert une enquête générale sur le suivi de mandataires politiques.[63] Le Comité a toutefois décidé de donner suite à cette affaire et de mener une « enquête partielle » sur les contacts de la Sûreté de l'État avec Bart Debie ainsi que sur les informations qui en ont découlé, particulièrement celles concernant Filip Dewinter. Le Comité a préalablement cherché à savoir si et dans quelle mesure le suivi du Vlaams Blok/Belang était prévu au fil des ans.

II.3.1. LE SUIVI DU VLAAMS BLOK, DÉNOMMÉ PLUS TARD VLAAMS BELANG

En vertu des articles 7 et 8 L.R&S, la VSSE est compétente pour suivre l'extrémisme[64] lorsqu'il menace ou pourrait menacer la sécurité intérieure ou extérieure du pays. Le suivi d'hommes ou de partis politiques est donc possible sous cet angle. En cas de suivi, il convient toutefois de tenir compte de la

---

59 « [la] mission de la VSSE de suivre des parlementaires à titre individuel. Ce n'est pas la mission de ce service et cela ne se produit pas non plus dans la pratique. » (traduction libre).

60 *Annales*. Chambre 2012-13, 7 février 2013, CRIV53COM666, 9 et suiv. Plus loin : « *[…] ik herhaal ook dat het niet tot de opdracht van de Veiligheid van de Staat behoort om parlementsleden in de gaten te houden in hoofde van hun functie* » («[…] je répète également que la Sûreté de l'État n'a pas pour mission de surveiller des parlementaires du fait de leur fonction » (traduction libre)).

61 J. VAN DER AA et T. LE BACQ, *De Standaard*, 11 février 2013 (Ik was de mol binnen Vlaams Belang).

62 « J'ignore ce qu'ils font avec d'autres responsables politiques, mais la Sûreté de l'État a suivi très attentivement le Vlaams Belang pendant des années. Je le sais, parce que j'y ai personnellement participé. » (traduction libre).

63 Voir *infra* « II.4. Le suivi de mandataires politiques par les services de renseignement ».

64 L'extrémisme y est défini de la manière suivante : « *les conceptions ou les visées racistes, xénophobes, anarchistes, nationalistes, autoritaires ou totalitaires, qu'elles soient à caractère politique, idéologique, confessionnel ou philosophique, contraires, en théorie ou en pratique, aux principes de la démocratie ou des droits de l'homme, au bon fonctionnement des institutions démocratiques ou aux autres fondements de l'État de droit* » (art. 8, 1° c L.R&S).

Constitution, de la CEDH et de la jurisprudence de la Cour européenne des Droits de l'Homme en matière de liberté d'expression et d'association.

Jusqu'au milieu des années 1990, le Vlaams Blok était systématiquement repris dans la « liste des sujets ». Le parti n'est plus apparu sur les listes de 1996 et 1999.[65] Durant cette période, il ne devait donc plus faire l'objet d'aucun suivi.

Une situation qui a changé lorsque le ministre de la Justice a donné pour instruction à la VSSE, en 2001, de considérer à nouveau le Vlaams Blok comme un sujet à traiter conformément à la Loi du 30 novembre 1998, à l'exception des activités que les mandataires mènent dans le cadre de leur mandat parlementaire. L'exercice d'un tel mandat y était défini comme « *de meningsuiting, de parlementaire vragen en interpellaties, het indienen van een wetsvoorstel, kortom wat zich in het parlementair halfrond afspeelt* ».[66] Dans une directive interne de juillet 2001, la VSSE a défini plus précisément les contours de cette directive ministérielle : les renseignements recueillis et traités à propos du « Vlaams Blok » devaient porter sur toutes les activités individuelles et collectives directement liées à l'extrémisme, tel que défini à l'article 8, 1° L.R&S. Toutes les activités qui ne sont pas de nature extrémiste ne sont pas suivies en tant que telles. L'attention de la VSSE devait dès lors porter sur les militants extrémistes actifs.

En 2003, par le biais d'une note particulièrement bien motivée, la VSSE a demandé au Premier ministre, en sa qualité de président du Comité ministériel du renseignement et de la sécurité, de supprimer le Vlaams Blok des sujets à suivre. Cette demande est restée sans réponse. En 2004, le Vlaams Blok est devenu le Vlaams Belang. Toutefois, pour la VSSE, ce changement de nom ne justifiait pas de demander aux autorités compétentes si elles estimaient nécessaire ou non de suivre ce parti. Le Vlaams Blok (*sic*) apparaissait dès lors toujours sur la « liste des sujets » de 2006.

Depuis 2009, la VSSE n'établit plus de « liste des sujets », mais élabore chaque année un « plan d'action » que le ministre de la Justice doit approuver. Ce plan énumère les phénomènes et groupements[67] à suivre et les classe selon qu'ils requièrent un « suivi actif »[68], un « suivi réactif »[69] ou « aucun suivi ».[70] C'est ainsi

65 À l'époque, on n'établissait pas nécessairement une nouvelle liste chaque année.

66 « l'opinion exprimée, les questions et interpellations parlementaires, le dépôt d'une proposition de loi, bref tout ce qui se déroule dans l'hémicycle parlementaire » (traduction libre).

67 Mais jamais de personnes en tant que telles.

68 Cela signifie que la VSSE développe activement des activités afin d'acquérir, d'enrichir ou de renforcer son niveau d'information.

69 Un « suivi réactif » signifie que la VSSE met sur pied des activités afin d'acquérir, d'enrichir ou de renforcer son niveau d'information, mais uniquement en réaction à une demande expresse à cet égard.

70 « Aucun suivi » signifie que la VSSE n'assure pas le suivi ou, le cas échéant, ne peut pas accéder à une demande externe de renseignements. Sont concernées les problématiques pour lesquelles le service est conscient de la nécessité d'effectuer un suivi et/ou un investissement, mais pour lesquelles la capacité insuffisante empêche d'obtenir un niveau d'information

que le Plan d'action 2010 mentionne, sous la rubrique « traitement réactif », « *L'extrême droite nationaliste e/o mouvements identitaires (…) (…) néerlandophone : Vlaams Belang* ». Les Plans d'action 2011 et 2012 font entre autres mention du « *Vlaams Belang – fonctionnement interne du parti et points de vue nationaux* », mais dans la catégorie « aucun suivi ». Le Plan d'action 2013 ne mentionne plus ce parti. Depuis lors, la rubrique « aucun suivi » a été supprimée.

II.3.2. LES CONTACTS ENTRE BART DEBIE ET LA VSSE

Le premier contact avec la VSSE a eu lieu à l'initiative de Bart Debie lui-même. À la mi-août 2010[71], il a envoyé un courrier électronique à la VSSE pour proposer ses services, parce qu'il avait reçu d'un « *heel bekend politicus opdrachten [heeft gekregen] die de grenzen van het strafrecht ver overschrijden* »[72] et qu'il « *deontologisch niet langer mee [kon] verzoenen* ».[73] Cinq rencontres ont suivi et de nombreux courriers électroniques ont été échangés, et ce jusqu'en juillet 2012.

Bart Debie a fourni des informations sur les contacts étrangers et les voyages planifiés de Filip Dewinter, sur sa position au sein du Vlaams Belang et les rapports de forces au sein du parti, sur ses « sponsors » et ceux du Vlaams Belang ; sur une conférence internationale dont l'organisation pratique a été confiée au Vlaams Belang; sur les liens entre le Vlaams Belang et plusieurs organisations d'extrême droite, sur l'attentat terroriste perpétré par le Norvégien Anders Breivik en 2011[74]; et sur la visite en Europe d'hommes d'affaires et de Sénateurs américains dont Filip Dewinter a reçu une délégation à Anvers. Les faits à l'origine de la prise de contact (c'est-à-dire les activités prétendument illégales) ont naturellement aussi été évoqués.

Des e-mails ont également été échangés sporadiquement, dans lesquels Bart Debie n'avait rien de particulier à signaler. Au fil du temps, aucune des deux parties n'a tenté d'organiser d'autres rencontres. Enfin, en juillet 2012, Bart Debie a indiqué être en possession d'informations concernant « une fuite au sein du

approprié et de planifier des actions. Ce qui ne signifie donc pas que la VSSE ne peut pas recevoir, collecter ou enregistrer des informations sur ces thèmes, mais bien que la VSSE ne les approfondit pas et que leur suivi est purement occasionnel.

71 Initialement, la presse a indiqué que Bart Debie était déjà en contact avec la VSSE en 2007, ce qui ne ressort cependant pas des conclusions tirées par le Comité permanent R lors de son enquête. Il s'agit peut-être d'un malentendu puisque lors de ses contacts avec la presse, l'intéressé a évoqué des affaires qui s'étaient produites en 2007, mais qu'il n'avait mentionnées qu'en 2010. Les journalistes ont d'ailleurs reconnu par la suite qu'ils avaient probablement manqué de précision (T. NAEGELS, *De Standaard*, 27 février 2013 (« Welles-nietes-nieuws »).

72 « responsable politique très connu [lui avait confié] des missions qui dépassaient largement les limites du droit pénal » (traduction libre).

73 « ne pouvait plus tolérer d'un point de vue déontologique » (traduction libre).

74 Ce dernier citait des Belges dans son « manifeste » et l'a également envoyé à plusieurs Belges, dont un député du Vlaams Belang. La VSSE a voulu savoir si les Belges cités avaient ou non des liens avec le terroriste norvégien.

Parquet ». Une rencontre a été organisée, mais l'intéressé ne s'y est pas présenté. Aucun autre contact n'a eu lieu par la suite.

Le Comité permanent R a estimé que les contacts de la VSSE étaient restés dans les limites de ses plans d'action annuels. Le Plan d'action 2010 prévoyait un suivi « réactif » de l'extrême droite et du Vlaams Belang, ce qui signifie que la VSSE peut déployer des activités en réaction à un événement ou un développement spécifique. Le Comité permanent R a jugé que les informations que l'intéressé semblait vouloir donner initialement – sur des missions qui dépassent largement les limites du droit pénal (« *opdrachten die de grenzen van het strafrecht ver overschrijden* ») – justifiaient qu'une suite soit donnée à la proposition de Bart Debie. En outre, étant donné son statut au sein du Vlaams Belang et ses connaissances sur l'extrême droite, une telle source ne pouvait pas être tout simplement laissée de côté. Dans le Plan d'action 2011, le Vlaams Belang était repris dans la catégorie « aucun suivi », ce qui ne signifiait pas pour autant que la VSSE ne pouvait plus recevoir d'informations à ce sujet. Comme cette année-là, cette source n'a permis de consigner que peu d'informations portant directement sur le Vlaams Belang, ce suivi était également conforme au plan d'action. En 2012, les contacts avec Bart Debie ont cessé. Le plan d'action de cette année-là mentionnait toujours le Vlaams Belang sous la rubrique « aucun suivi ».

Le Comité a aussi constaté que la VSSE avait respecté l'instruction du 15 mai 2001 dans sa relation avec Bart Debie : elle n'avait recueilli aucun renseignement portant sur l'exercice du mandat parlementaire en tant que tel (expression de l'opinion et travaux au Parlement) de Filip Dewinter ou d'autres parlementaires.

Le Comité permanent R a globalement estimé que la manière dont la VSSE avait préparé et traité les contacts avec Bart Debie était peu ou pas discutable. Ainsi, les objectifs du recueil de renseignements (par exemple, concernant les intentions de Bart Debie, les activités prétendument illégales de Filip Dewinter et les canaux de financement « occulte » de son parti) ont été clairement énoncés par le service Analyse et rigoureusement suivis par les services extérieurs. Il a été rappelé explicitement à plusieurs reprises que les informations recueillies devaient porter sur des activités liées ou susceptibles d'être liées à l'extrémisme. Par exemple, les informations devaient permettre de détecter et d'analyser des tendances extrémistes (xénophobes ou racistes) au sein du Vlaams Belang et ne devaient pas porter sur l'exercice du mandat parlementaire proprement dit de Filip Dewinter ou d'autres parlementaires. Ce point a également été clairement expliqué à plusieurs reprises à la source. Les rapports ont parfois mentionné les noms de parlementaires du Vlaams Belang, mais pas en relation avec leurs activités parlementaires. Par ailleurs, il a rarement, voire jamais, été fait référence à leur qualité de parlementaire. Le Comité a toutefois dû constater que les collaborateurs de la VSSE ne pouvaient pas toujours décrire correctement les limites de leur intervention lorsqu'il s'agit de mandataires parlementaires, mais qu'ils les sentaient peut-être de manière intuitive. Les limites fixées dans la

directive concernant les informations qui peuvent être recueillies à propos d'un responsable politique n'étaient pas très claires.

Enfin, le Comité a également constaté que les circonstances matérielles dans lesquelles la VSSE a rencontré la source étaient normales. Aucun avantage financier ne lui a été octroyé. Il n'a bénéficié que d'une petite attention. Au fil des entretiens, Bart Debie avait également fait mention de problèmes personnels. Il n'avait pas reçu l'agrément lui permettant de dispenser des cours à des ambulanciers et se demandait s'il pourrait entrer en considération pour une réhabilitation à la suite d'une condamnation antérieure. Le commissaire concerné de la VSSE a fait savoir à sa source que la personne qu'il a contactée lui a affirmé qu'aucune exception ne pouvait être faite. En outre, il ne lui a fourni que des informations accessibles au public.

II.3.3. FILIP DEWINTER DANS LA BASE DE DONNÉES DE LA VSSE[75]

La VSSE disposait bien entendu d'informations relatives à Filip Dewinter avant ses contacts avec Bart Debie.[76] Dans la base données de la VSSE, qui est opérationnelle depuis 2001[77], son nom était lié à 214 reprises à des matières telles que l'« extrême droite », mais aussi au « salafisme » ou à l'« islam radical ».[78] Les rapports rédigés à la suite des contacts avec Bart Debie[79] ont également été repris dans la base de données et associés en l'espèce aux matières « Extrémisme » et « Extrême droite néerlandophone ». Dans 156 cas, il s'agissait d'un « lien pertinent » et, dans 55 cas, d'un lien « pour info ». Trois liens étaient « À déterminer ». Le Comité a posé des questions sur la signification exacte de ces concepts[80] et à leur application concrète sur le terrain.

---

75 Lors d'une interview télévisée diffusée le 11 février 2013, un dossier volumineux était visible sur le bureau de l'administrateur général de la VSSE. Sur la couverture, on pouvait lire le nom de « Dewinter Philip ». Le Comité a constaté qu'il s'agissait uniquement d'un recueil des pièces de procédure, la correspondance et les notes relatives aux nombreuses procédures introduites par l'intéressé pour avoir accès à son dossier auprès de la VSSE.

76 Le SGRS disposait lui aussi d'informations et de renseignements concernant Filip Dewinter, mais dans une moindre mesure que la VSSE. Le « dossier » Dewinter au sein du SGRS était ancien, mis à jour de manière peu systématique et principalement constitué d'informations émanant de sources ouvertes.

77 Dans le système informatique qui était opérationnel avant 2001, le nom de Filip Dewinter apparaissait dans 459 documents. Le Comité n'a pas inclus ces documents dans son enquête notamment en raison du caractère obsolète des informations qu'ils contenaient.

78 Un lien pouvait à la fois signifier que la personne était impliquée dans un phénomène et qu'elle en était la victime.

79 Comme il s'agissait d'une source humaine et vu le caractère délicat de l'affaire, les données qui ont découlé des contacts ont été reprises dans une « opération ». De cette manière, seules les personnes explicitement habilitées à prendre connaissance de cette opération ont accès aux informations de la base de données de la VSSE.

80 Voir aussi II.4.2.3.

Outre les liens établis entre un nom et une matière, il convient également de mentionner lesdits « liens opérationnels », qui relient deux noms et où la relation entre ces deux noms fait l'objet d'une qualification telle que « ami de », « opposant de », « connaissance de », « sympathisant de »…

Le Comité a estimé qu'il ne fallait pas déduire de son analyse que la VSSE a porté une attention excessive à l'intéressé. Il ressort du nombre relativement restreint de liens opérationnels établis entre Filip Dewinter et des tiers – au total 50 en douze ans – que la VSSE a fait preuve d'une grande prudence et n'a pas développé une « position d'information » importante à l'égard de l'intéressé. Le Comité permanent R a estimé que la VSSE s'est comportée de manière plutôt timorée en la matière.

II.3.4. RAPPORTS À LA MINISTRE DE LA JUSTICE

Deux directives revêtaient de l'importance en matière d'information à la ministre de la Justice en cas de suivi de mandataires politiques par la VSSE.[81] D'une part, l'instruction du 25 mai 2009 émanant du ministre de la Justice qui concerne l'information des mentions de parlementaires fédéraux. D'autre part, l'instruction interne du 27 mars 2012 qui porte sur les ministres, les secrétaires d'État et les élus des niveaux fédéral, communautaire et régional. L'intéressé est devenu sénateur communautaire le 8 juillet 2010, ce qui signifie que les deux directives s'appliquaient aux informations découlant des contacts avec Bart Debie. Toutefois, à une exception près, ces instructions n'ont pas été suivies pour ce qui concerne les informations relatives à Filip Dewinter.

II.4. LE SUIVI DE MANDATAIRES POLITIQUES PAR LES SERVICES DE RENSEIGNEMENT

À l'instar des enquêtes « *Notes secrètes sur l'Église de scientologie dans la presse* » (II.2) et « *Un informateur au sein du Vlaams Belang?* » (II.3.), la présente enquête de contrôle découle des deux mêmes notes classifiées de la Sûreté de l'État qui ont été diffusées dans la presse. Les débats (parlementaires) qui ont suivi cette divulgation ont abordé à maintes reprises la question de savoir si et dans quelle mesure les services de renseignement belges suivent ou peuvent suivre des mandataires politiques et quelles règles doivent être respectées en la matière. C'est ainsi que le Comité a décidé d'ouvrir une enquête thématique « *sur la manière dont les services de renseignement collectent des informations concernant*

[81] Voir aussi Chapitres II.2.1.3 et II.4.2.1.3.

des mandataires politiques, la manière dont ils traitent et analysent ces informations, et la manière dont ils en font rapport aux autorités compétentes».

Ce n'était d'ailleurs pas la première fois que le Comité permanent R examinait les activités des services de renseignement à l'égard de mandataires politiques.

Déjà en 1997, le Comité a ouvert une enquête «*sur la manière dont les services de renseignement font la distinction entre les activités de parlementaires en tant que pacifistes écologistes et en tant que parlementaires*».[82] Cette enquête faisait suite à une demande d'un parlementaire Ecolo et s'est intéressée aux renseignements que la VSSE et le SGRS auraient éventuellement recueillis sur des mandataires d'Ecolo ou d'Agalev (ancienne dénomination de Groen!). Le Comité est parvenu à la conclusion que les deux services possédaient des dossiers au nom de plusieurs parlementaires issus de ces partis, mais que les activités de ces personnes ne faisaient plus l'objet d'un suivi particulier depuis 1988.

Un an plus tard, en 1998, et dans le sillage de l'enquête précitée, le Comité permanent R ouvrait une enquête plus générale sur «*la collecte de données par les services de renseignement à propos de parlementaires*».[83] Cette enquête portait sur les mandataires de *tous* les partis politiques. Le Comité a conclu dans ce cadre que «*ni la VSSE ni le SGR n'effectuent d'enquêtes concernant des actes accomplis dans l'exercice proprement dit d'un mandat parlementaire*».

Enfin, en 2006, lesdits «dossiers réservés» faisaient surface à la VSSE.[84] Il est apparu que depuis la fin des années 1980, le service «Affaires générales» de la VSSE tenait à jour un certain nombre de dossiers contenant des données sur des élus, et ce en dehors du «circuit normal». Certains de ces dossiers étaient même exclusivement conservés au secrétariat de l'administrateur-directeur général de la Sûreté publique de l'époque. Dans cette enquête, le Comité a entre autres décidé que «*l'enregistrement, voulu ou non, d'hommes politiques et de personnalités dans les fichiers informatisés d'un service de renseignement demeure une question extrêmement délicate. Le Comité a toutefois estimé que le statut particulier d'une personnalité ou d'un homme politique ne peut constituer un obstacle en soi, ni à un suivi adéquat par un service de renseignement de la personne concernée, ni à la disponibilité des rapports y afférents, la mission légale de ce service étant d'exécuter ses tâches 'sans considération de personne'.*»[85] Dans le prolongement, le Comité a également formulé la recommandation suivante: «*De manière plus générale, le Comité permanent R souhaite que la Sûreté de l'État élabore des directives claires et univoques quant au recueil, au traitement, à la consultation (y compris le cloisonnement interne éventuel), au stockage et à l'archivage des données de certaines catégories de personnes qui assument ou ont*

82 COMITÉ PERMANENT R, *Rapport d'activités 1998*, 60 et suiv.
83 COMITÉ PERMANENT R, *Rapport d'activités 1999*, 13 et suiv.
84 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 20 et suiv.
85 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 28 et suiv.

assumé des responsabilités particulières. Lors de l'élaboration de ces directives et du suivi concret des (ex-)mandataires politiques, la Sûreté de l'État doit tenir compte des indications fournies dans l'arrêt que la Cour européenne des droits de l'homme a rendu dans l'affaire Segerstedt-Wiberg and others ».[86]

II.4.1. QUELQUES CHIFFRES RELEVÉS DANS LE CADRE DE LA NOUVELLE ENQUÊTE

Le 1er mars 2013, 479 personnes exactement – hors doubles mandats – occupaient soit un poste ministériel dans le gouvernement fédéral ou les gouvernements régionaux, soit une fonction de parlementaire dans une assemblée législative régionale ou fédérale. Dans son enquête de contrôle, le Comité a demandé aux deux services de renseignement de vérifier si et dans quelle mesure le nom de ces personnes apparaissait dans leurs dossiers papier et leurs banques de données.

Il s'est avéré qu'entre début juin 2010 (c'est-à-dire le début de la législature fédérale de l'époque) et le début 2013, les services extérieurs de la VSSE ont rédigé 727 documents dans lesquels au moins un des 479 mandataires était cité. Au total, 142 mandataires différents étaient mentionnés.[87]

Sur la même période, le service Analyse de la VSSE a recensé 423 documents dans lesquels 93 mandataires politiques différents étaient mentionnés. Un peu plus de la moitié de ces documents émanait de sources externes (par exemple, l'OCAM, la police ou d'autres correspondants), tandis que l'autre moitié relevait de la « production maison ». Il s'agissait de documents à usage interne (notes de synthèse décrivant l'état d'avancement d'un dossier donné et comptes rendus de réunions), de documents destinés à des personnes ou instances extérieures (notes adressées à des autorités belges et – seulement quelques-unes – à des autorités étrangères) et d'« apostilles », dans lesquelles le service Analyse posait des questions précises aux services extérieurs.

---

86 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 106-107. Dans son arrêt rendu le 6 juin 2006 dans l'affaire *Segerstedt-Wiberg and others* contre la Suède, la Cour européenne des Droits de l'Homme pose le problème du recueil et de la conservation de données concernant les opinions, affinités ou appartenances politiques, et ce au regard de l'article 8 de la CEDH. Le fait que de telles données – même si elles portent sur des faits publiquement connus – soient recueillies ou conservées constitue une ingérence grave dans la vie privée. Selon la Cour, ces ingérences ne peuvent se justifier que si elles sont proportionnelles au regard de la sécurité nationale. Pour l'évaluation de cette proportionnalité, la Cour a accordé une importance considérable au caractère violent ou non d'un parti politique. On ne peut déduire le caractère violent d'un parti de son seul programme; il doit également se refléter dans les actes posés par les dirigeants du partir et dans leurs positions.

87 Certains apparaissaient même dans plusieurs documents: 37 % des mandataires faisaient l'objet d'une seule mention, 35 % de deux à cinq mentions. Quatre mandataires figuraient dans plus de 21 documents. Un élu était cité dans 91 documents.

Le Comité a pris un échantillon de ces documents[88] et l'a étudié pour se faire une idée du travail de recueil et d'analyse de la VSSE à l'égard de mandataires politiques (*infra*).

De son côté, le SGRS[89] disposait d'informations sur papier *et* sur supports numériques. Ainsi, il y avait 115 fiches qui correspondaient à un dossier papier de mandataires politiques. La plupart des dossiers y relatifs était toutefois déjà détruite. Les archives dites « vivantes » comptaient seulement 36 dossiers, tandis que les archives dites « mortes » (parce qu'elles n'ont plus été consultées pendant quinze ans) en comportaient encore 12.

La base de données du SGRS contenait le nom de 109 mandataires. Le Comité permanent R a étudié un quart de ces dossiers et a relevé, par exemple, qu'il n'est jamais mentionné si une personne est ou non parlementaire.

Durant la période de référence de l'enquête de contrôle, le SGRS n'a rédigé aucune note d'analyse portant spécifiquement sur des ministres ou mandataires parlementaires.

II.4.2. LE SUIVI DE RESPONSABLES POLITIQUES TOUT AU LONG DU CYCLE DE RENSEIGNEMENT

Dans le cadre de son analyse des dossiers sélectionnés, le Comité a parcouru tous les aspects du cycle de renseignement, en commençant par « le pilotage des activités de renseignement », suivi de « la collecte », de « l'organisation de l'information », de « l'analyse » jusqu'à « la diffusion des renseignements ».

II.4.2.1. Le pilotage des activités de renseignement

Les activités des services de renseignement belges sont pilotées à différents niveaux. Le niveau le plus général est celui de la réglementation – à savoir les lois, arrêtés et instructions générales – qui stipule quelles activités de renseignement peuvent être exécutées et comment elles peuvent se dérouler. Ensuite vient le niveau des plans annuels d'action ou de renseignement qui – sur la proposition des services et avec l'approbation du ministre compétent – déterminent concrètement les matières qui doivent ou peuvent être couvertes au cours de l'année suivante. Enfin, il y a le pilotage *ad hoc*, dans des dossiers concrets, par le dirigeant du service ou le ministre compétent. Ces trois niveaux sont abordés ci-dessous.

---

88 Un dossier sur quatre a été examiné, à une exception près : les notes destinées à des autorités étrangères ont toutes été incluses dans l'analyse.

89 Et plus particulièrement la Division C(ounter) I(ntelligence), qui est compétente pour les menaces internes.

II.4.2.1.1. Règles applicables au recueil de renseignements concernant des mandataires politiques

La Loi du 30 novembre 1998 organique des services de renseignement et de sécurité (L.R&S) ne contient aucune disposition qui octroierait un statut particulier à un parlementaire. Par ailleurs, la loi ne fait aucune référence à des mandataires politiques. Il en va de même pour la Loi MRD du 4 février 2010, qui ne prévoit aucune protection particulière pour les responsables politiques, mais bien pour les journalistes professionnels, les avocats et les médecins. Dans cette optique, le Comité a réitéré sa position de 2008 selon laquelle le statut d'un responsable politique ne peut pas constituer un obstacle à un suivi et à un signalement adéquats. En effet, le travail de renseignement doit se dérouler « sans considération de personne ». En cas de suivi, il convient toutefois de tenir compte de la jurisprudence de la Cour européenne des Droits de l'Homme en matière de liberté d'expression et de liberté d'association. Il convient de faire preuve d'une extrême prudence en cas d'ingérence dans ces droits fondamentaux à l'égard de partis et mandataires politiques (même extrêmes).

La prise de conscience du caractère particulièrement sensible du suivi de partis ou de mandataires politiques, a donné lieu à une restriction spécifique introduite en 2001 pour le suivi de mandataires parlementaires de l'ancien Vlaams Blok[90] : la directive ministérielle du 15 mai 2001, qui donnait pour mission de suivre ce parti, stipulait que ce suivi devait porter sur toutes les activités à l'exception de celles que les mandataires menaient dans le cadre de leur mandat parlementaire. La VSSE a formulé cette restriction de la manière suivante : « *een parlementair mandaat* is *de meningsuiting, de parlementaire vragen en interpellaties, het indienen van een wetsvoorstel, kortom wat zich in het parlementair halfrond afspeelt* ».[91]

Depuis lors, cette définition – dont on peut se demander si elle était (encore) suffisamment connue ou si elle s'applique en dehors des mandataires du parti concerné et si elle est suffisamment pertinente et claire – n'a jamais été explicitement réitérée, affinée ou nuancée. Dans ses réponses à plusieurs questions parlementaires, la ministre de la Justice est toutefois revenue sur ce point en 2013 : un service de renseignement ne peut pas suivre les activités qu'un parlementaire mène « *au sein même du parlement* » dans le cadre de sa « *fonction parlementaire* » ou « *dans ses interventions en tant que parlementaire* ».[92] Le Comité estime néanmoins que ces « précisions », qui sont ultérieures à l'ouverture de la présente enquête de contrôle, ne résolvaient pas toutes les questions. En effet, dans la pratique, il est difficile de distinguer les activités qu'un mandataire

90 Voir à cet égard le chapitre II.3.

91 « *un mandat parlementaire* » *correspond à* « *l'expression d'une opinion, les questions et interpellations parlementaires, le dépôt d'une proposition de loi, bref tout ce qui se déroule dans l'hémicycle parlementaire.* » (traduction libre)

92 *Ann.* Sénat, 21 février 2013, n° 5-92, 16-18 et *Ann.* Sénat, 14 mars 2013, n° 5-95, 17-19.

parlementaire mène dans le cadre de son mandat de celles qu'il mène en dehors. En outre, certains aspects ne relèvent pas du périmètre de cette restriction (comme le rôle d'un parlementaire dans le fonctionnement interne du parti et la définition de la stratégie du parti), alors qu'ils sont bien plus « sensibles » que le fait de poser une question parlementaire ou de déposer une proposition de loi (lesquelles concernent des informations qui sont publiques par définition).

Le Comité a dès lors réitéré la recommandation qu'il a formulée dans le cadre de son enquête relative aux « dossiers réservés »[93], et qui prônait l'élaboration de directives claires et univoques pour les activités de renseignement portant sur certaines catégories de personnes assumant ou ayant assumé des responsabilités particulières.

La nécessité d'une directive claire et globale s'applique évidemment aussi au SGRS. En effet, à l'époque de l'enquête, ce service s'appuyait encore sur une instruction antérieure à la Loi du 30 novembre 1998. Une note du 25 juin 1998 énonce que des mandataires politiques ne peuvent pas être suivis en raison de leur mandat, mais qu'à l'instar de tout autre citoyen, ils peuvent retenir l'attention du SGRS lorsqu'ils ont besoin d'une habilitation de sécurité, lorsqu'ils font partie d'une organisation qui représente une menace pour les missions de la Défense, ou lorsqu'ils tentent de pénétrer dans un domaine militaire ou d'entraver les activités de la Défense.

II.4.2.1.2. Mention de partis politiques dans les plans annuels d'action ou de renseignement

En 2013, aucun parti politique représenté au Parlement ne figurait plus dans les plans annuels d'action ou de renseignement respectivement de la VSSE et du SGRS. Par le passé, certains partis ont été mentionnés en tant que « *targets* » de la Sûreté de l'État, et ce parfois à la demande explicite du ministre compétent (voir II.4.2.1.1).

Bien qu'aucun parti politique représenté au Parlement n'ait été suivi en tant que tel en 2013, le Comité permanent R a estimé que des directives claires et univoques devraient également être élaborées à cet égard.

II.4.2.1.3. Pilotage *ad hoc* par le ministre de la Justice : modalité d'application de la directive du 25 mai 2009

Le 2 mai 2009, le ministre de la Justice de l'époque avait annoncé au Parlement que « *de Veiligheid van de Staat hem telkens een waarschuwingsnota […] ter informatie zal sturen voor een actief federaal parlementslid dat werd vermeld of gelieerd is met een specifieke materie in een dossier als onderdeel van informatie of als persoon het voorwerp uitmaakt van bedreigingen ten overstaan van zijn*

93 COMITÉ PERMANENT R, *Rapport d'activités 2008*, 106-107.

persoon of als een buitenlandse inlichtingendienst interesse betoont in hem ».[94, 95] En application de ce qui précède, le ministre de la Justice a marqué son approbation, le 25 mai 2009, à une instruction fondée sur une ébauche de la VSSE. Cette directive énonçait que le ministre recevrait une « *note d'avertissement* » « *pour tout parlementaire fédéral en activité cité pour information ou lié à une matière spécifique dans un rapport, en tant qu'élément d'information, ou qui fait l'objet de l'attention de la Sûreté de l'État comme personne menacée ou encore comme cible de l'intérêt d'un agent de renseignement étranger, ces citations ou liens réalisés dans l'exercice des compétences de la Sûreté de l'État. L'avertissement serait envoyé à Monsieur le Ministre sous la forme d'une note classifiée « Secret – Loi 11.12.1998 » pour tout parlementaire fédéral cité ou lié dans un rapport produit par la Sûreté de l'État. […] La Sûreté de l'État poursuivra son activité de surveillance de manière normale (silent procedure), sauf avis contraire de Monsieur le Ministre de la Justice.* »

En 2013, l'administrateur général de la VSSE de l'époque a affirmé à cet égard : « *Grosso modo bevat de richtlijn drie aspecten. De belangrijkste vernieuwing betrof de onmiddellijke inkennisstelling van de minister van Justitie telkens de naam van een actief federaal parlementslid in een verslag van de VSSE voorkomt. De VSSE en de minister kwamen hiermee tegemoet aan de ongerustheid die bij sommige federale parlementsleden was gerezen naar aanleiding van het toezichtonderzoek van het Vast Comité I naar de zogenaamde 'gereserveerde dossiers'.* »[96, 97] L'administrateur général a souligné que cette méthode de travail permet également au ministre d'assumer sa responsabilité en donnant le cas échéant des ordres ponctuels supplémentaires à la VSSE. Il peut aussi exercer un contrôle sur l'enquête de renseignement, éventuellement par l'intermédiaire du Comité permanent R. Enfin, cette information permet au ministre de la Justice de répondre à des questions de parlementaires qui exercent leur droit de contrôle constitutionnel. Selon l'administrateur général, il est ainsi satisfait aux exigences d'un État de droit démocratique parlementaire.

---

94 « *la Sûreté de l'État (lui) enverra, pour information, une note d'avertissement […] chaque fois qu'un parlementaire fédéral en activité sera cité ou sera lié à une matière spécifique comme élément d'information, ou s'il fait l'objet de menaces personnelles, ou encore si un service de renseignement étranger s'intéresse à lui.* » (traduction libre)

95 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 3.

96 « *Cette directive englobe grosso modo trois aspects. La principale innovation portait sur l'information immédiate du ministre de la Justice chaque fois que le nom d'un parlementaire fédéral actif apparaît dans un rapport de la VSSE. La VSSE et le ministre ont ainsi répondu aux inquiétudes soulevées par certains parlementaires fédéraux à l'occasion de l'enquête de contrôle du Comité permanent R sur lesdits 'dossiers réservés'.* » (traduction libre).

97 A. WINANTS, « *Control in the circus*. Interne controle bij de Veiligheid van de Staat » in *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, W. VAN LAETHEM et J. VANDERBORGHT (eds.), Anvers, Intersentia 2013, 137.

Le Comité permanent R estimait que l'administrateur général avait très bien traduit l'importance de la directive de 2009, que le Comité avait d'ailleurs déjà accueillie favorablement. Dans son *Rapport d'activités 2009*, le Comité affirmait que cette instruction permettait « *d'apaiser en partie les inquiétudes du Comité permanent R* », exprimées dans le cadre de l'enquête sur les « dossiers réservés ».[98]

Pourtant, depuis juin 2010 (en d'autres termes, alors que l'instruction était en vigueur depuis environ un an), quelque 350[99] rapports et notes de la VSSE mentionnaient le nom de parlementaires fédéraux alors en activité. Or le/la ministre n'en a été informé(e) de la manière prescrite qu'à titre exceptionnel. Le fait que cette instruction n'a pas été respectée n'a apparemment jamais été souligné, mentionné, contrôlé et/ou problématisé au sein du service. Le Comité permanent R a d'ailleurs souligné dans son enquête de contrôle que la directive n'a pas *pu* être totalement respectée, déjà rien que par le fait que la VSSE ne disposait pas d'une liste (mise à jour en permanence) de tous les mandataires politiques. Conséquence inévitable : des rapports ont parfois été rédigés à propos de parlementaires sans que l'on soit nécessairement conscient de leur statut.

Au cours de l'enquête de contrôle, la VSSE a proposé plusieurs modifications à apporter à ses processus de travail, dont, entre autres, la notification de la mention de parlementaires dans ses rapports. Dans ce document de travail, la VSSE a proposé d'informer le ministre tous les mois (et non plus immédiatement) lorsque des parlementaires sont mentionnés dans des documents du service Analyse (et donc plus des services extérieurs). Ce document de travail a donné lieu à une nouvelle instruction après la clôture de l'enquête du Comité (voir Chapitre I.1.3).

II.4.2.2. La collecte

Le Comité permanent R a souligné que dans la plupart des cas, des parlementaires ont été mentionnés dans des rapports de collecte de la VSSE, soit parce que le mandataire concerné faisait lui-même l'objet d'une menace éventuelle, soit parce qu'il était (fortuitement) entré en contact avec une personne ou un groupement suivi. Le Comité n'a trouvé aucun élément indiquant que la VSSE visait des mandataires politiques pour des raisons étrangères aux intérêts et menaces énumérés dans la loi.

Le Comité a pu tirer la même conclusion à l'égard du SGRS : ce service n'a manifesté aucun intérêt pour des mandataires politiques en tant que tels. Lorsque le SGRS s'est exceptionnellement intéressé à des mandataires politiques,

98 COMITÉ PERMANENT R, *Rapport d'activités 2009*, 3.

99 Les 727 documents mentionnés au point II.4.1 concernent des mandataires du gouvernement fédéral et des gouvernements régionaux, alors qu'en l'espèce, il s'agit uniquement de mandataires fédéraux.

c'était en relation avec un intérêt ou une question militaire. La plupart des dossiers du SGRS étaient d'ailleurs ouverts bien avant que le responsable politique concerné assume son mandat. Preuve que le « mandat politique » n'était pas pertinent pour le SGRS.

Dans son échantillon pris au sein de la VSSE, le Comité permanent R n'a trouvé qu'un seul dossier dont il a pu établir que des données ont été recueillies à propos d'éléments qui s'inscrivaient éventuellement « dans le cadre du mandat parlementaire », comme décrit dans la directive susmentionnée du 25 mai 2001, et qui se sont déroulés « au sein même du parlement » (en l'espèce le parlement d'une entité fédérée). Il s'agissait d'informations que la VSSE avait reçues à propos d'une réunion organisée par un parti politique avec un mouvement politique étranger susceptible de représenter une menace. Pour le Comité, cet exemple démontrait une nouvelle fois que les critères énumérés dans la directive sont peu utiles et opérationnels dans la pratique. En effet, d'une part, les activités politiques ne se limitent pas à l'hémicycle et, d'autre part, il semble n'y avoir aucune bonne raison de ne pas suivre des menaces qui se prépareraient depuis le parlement. Le Comité permanent R a dès lors estimé que ces critères devaient être réexaminés.

Cependant, ce n'est pas parce que le Comité n'a trouvé aucun élément indiquant un suivi illégitime de parlementaires que toutes les données collectées se sont révélées utiles. Le Comité n'a pas manqué de constater qu'une partie des informations étaient plutôt « banales » : le responsable politique A est d'abord allé saluer la personne B avant de partir ; le responsable politique C assiste à une réunion à laquelle 1 000 personnes sont présentes ; le responsable politique D a participé à la manifestation, mais n'est arrivé qu'à la fin… Le lien avec l'une des menaces ou des intérêts décrits dans la loi n'est donc pas toujours clair à première vue.

Le Comité est bien entendu conscient qu'il n'est pas toujours évident, dans le travail de renseignement, de déterminer au moment de la collecte quelles informations seront un jour pertinentes ou non. Il n'empêche qu'il convient de respecter les exigences en la matière, telles que celles décrites dans la L.R&S et dans la Loi relative à la protection de la vie privée (principe de finalité, adéquation, exactitude…). Le fait qu'un événement donné soit mentionné ou non dans un rapport de collecte, et la manière dont il est évoqué, revêtent dès lors une importance cruciale. Le Comité a estimé que la méthode d'*input* devrait faire l'objet d'une formation permanente et être soumise à un véritable contrôle de qualité. Dans ce même cadre, le Comité a insisté sur le fait que le rapport doit clairement mentionner, par exemple, si une personne est « victime », « acteur » ou « passant » par rapport à la menace concernée.

II.4.2.3. L'organisation de l'information

La base de données de la VSSE contient évidemment un très grand nombre de données sur des personnes, groupements, lieux et événements (entités). Afin de permettre leur exploitation, ces données sont « liées » à une ou plusieurs menaces que la VSSE a pour mission légale de suivre (extrémisme, prolifération, ingérence…). C'est ce que l'on appelle des « motivations ». Quatre types de « liens » sont possibles : « Pour info », « À déterminer », « Lien pertinent » ou « Lien opérationnel ». Un « Lien pertinent » indique que le lien avec une des matières ou menaces est concret et évident.[100] Le lien est « À déterminer » lorsque la pertinence du lien n'a pas encore été établie. La portée exacte des deux autres liens est toutefois moins évidente. Un lien « Pour info » est décrit tantôt comme un « *lien pour des entités qui n'ont aucun lien avec l'une des matières ou menaces traitées par la VSSE* », tantôt comme un « *lien qui indique une implication passive ou pas encore qualifiée (par exemple, l'objet de la menace)* ». Le Comité a dès lors dû constater que ces concepts ne sont pas décrits ni appliqués de manière univoque, ce qui risque de porter préjudice à l'efficacité et l'efficience du travail de renseignement. En effet, (tous) les rapports utiles risquent de ne pas « remonter à la surface » lorsque le travail d'analyse le requiert, ce qui peut donner lieu à des conclusions erronées. Aussi le Comité permanent R a-t-il estimé que la VSSE devait réexaminer d'urgence ces concepts. Par ailleurs, le service devrait ajouter la possibilité d'indiquer le rôle (présumé) d'une personne citée dans un rapport à l'égard de la menace en question (« passant », « victime potentielle », « personne clé », « acteur »…).

II.4.2.4. L'analyse

Le Comité permanent R n'a trouvé aucune indication selon laquelle les services d'Analyse des deux services de renseignement se seraient intéressés de manière illégitime à des ministres et à des parlementaires.[101] Deux enquêtes antérieures (voir II.2 et II.3) ont déjà démontré que la VSSE était consciente du caractère

---

100 En vertu de la directive du 27 mars 2012, des ministres et mandataires politiques en fonction peuvent uniquement faire l'objet d'un « lien pertinent » lorsqu'il ressort de l'information contenue dans le rapport qu'ils sont activement impliqués dans une menace contre la pérennité de l'ordre démocratique et constitutionnel. Ils peuvent faire l'objet d'un « lien pour info » lorsque l'information contenue dans le rapport indique qu'ils font l'objet d'une menace ou lorsqu'ils sont activement impliqués dans une menace contre l'une des autres matières à propos desquelles la VSSE recueille des renseignements. Lorsque l'auteur d'un rapport estime que d'après l'information contenue dans le rapport, un lien pertinent ou pour info doit être établi pour un ministre ou un mandataire politique en fonction, il se concerte avec son chef de section.

101 Le Comité a trouvé dans un seul dossier un rapport contenant des informations portant sur des « activités parlementaires au sein du Parlement ». Ces informations ont été consignées par un collaborateur de la VSSE, qui avait été invité à assister à une réunion à huis clos au Parlement. Le rapport était destiné à la ministre de la Justice. Le Comité s'est une nouvelle

délicat du travail de renseignement lorsqu'il concerne des mandataires politiques. Il en va de même pour le service Analyse du SGRS-CI.

Le Comité a toutefois constaté que dans leurs rapports, les services d'Analyse doivent accorder l'attention requise à la « position » d'une personne citée par rapport à la menace en question (« victime », « acteur », « passant »…).

II.4.2.5. La diffusion de renseignements

Le Comité a constaté que dans la période de référence, le SGRS n'avait diffusé à d'autres services aucun document mentionnant le nom d'un ministre ou d'un parlementaire.

En revanche, la VSSE avait bien envoyé de telles notes à des autorités belges. Le Comité a toutefois souligné que ce service a précisément pour tâche principale d'informer les autorités compétentes lorsqu'une personne fait l'objet d'une menace ou contribue à une menace (art. 19 L.R&S), même s'il s'agit d'un responsable politique belge. La diffusion de ces renseignements en dehors de la VSSE doit toutefois s'appuyer sur le *need to know* ainsi que sur les exigences de l'article 19 L.R&S précité. Le Comité permanent R l'avait déjà souligné dans une enquête antérieure.[102] Ce principe et cette disposition légale sont d'application, et ce quel que soit le destinataire, entre autres le parquet, les services publics fédéraux, le Premier ministre et ministres fonctionnellement compétents, les ministres des entités fédérées, le Roi en tant que chef d'État, mais bien évidemment aussi lorsque le destinataire est un service étranger. Dans ce cadre, le Comité a pu constater que la VSSE a fait preuve de la réserve requise lorsqu'il s'est agi de communiquer les rapports visés à des services étrangers. Cette réserve s'est exprimée de différentes manières : le nombre restreint de communications, la nature de l'information communiquée et les pays auxquels l'information a été communiquée. Malgré tout, le Comité a insisté sur le fait qu'il faut toujours examiner avec soin si le nom de mandataires politiques belges (mais aussi de « simples » citoyens) peut être mentionné dans des documents destinés à des services étrangers. Le principe du *need to know* et l'exigence de l'article 19 L.R&S sont une fois de plus déterminants en la matière. Toutefois, en cas de transmission de données à caractère personnel vers l'étranger, d'autres exigences entrent en ligne de compte, par exemple celles mentionnées dans la Loi sur le respect de la vie privée. Le Comité permanent R a une nouvelle fois souligné que dans ce cadre, il était important que le Comité ministériel du renseignement et de la sécurité précise encore la portée de l'article 19 L.R&S.

fois demandé si l'objectif pouvait être de ne pas autoriser un tel compte rendu. Le Comité a estimé qu'il incombe au ministre compétent de prendre une décision en la matière.

102 Voir Chapitre II.2. « Notes secrètes sur l'Église de scientologie dans la presse ».

II.5. LA POSITION D'INFORMATION DE LA SÛRETÉ DE L'ÉTAT CONCERNANT UNE TRANSACTION INTERNATIONALE D'UNE ENTREPRISE BELGE

II.5.1. UNE PLAINTE RELATIVE À UNE LICENCE D'EXPORTATION REFUSÉE

Fin 2011, des représentants d'une société de droit belge spécialisée dans la production de matériel de haute technologie se sont plaints que le ministre compétent ait refusé de leur octroyer une licence d'exportation pour une presse isostatique à chaud.[103] Le pays de destination avait pourtant signé le Traité de non-prolifération.[104] En outre, les plaignants ont affirmé que l'entreprise avait reçu précédemment une licence d'exportation pour le même produit à destination du même pays. Ce refus résulterait de la pression exercée par un gouvernement étranger sur les instances belges. Les plaignants ont évoqué une ingérence néfaste pour leurs intérêts économiques.

Début 2012, le Comité permanent R a décidé d'ouvrir une enquête de contrôle sur la position d'information de la VSSE à l'égard de cette transaction internationale aussi bien dans le cadre de la lutte contre la prolifération que celui de la protection du potentiel scientifique et économique du pays.[105]

Il s'agissait d'ailleurs de la troisième enquête de contrôle du Comité qui concernait la société en question. En 2005 déjà, le Comité avait examiné comment la VSSE avait traité des informations émanant d'un service étranger sur l'exportation vers l'Iran d'une presse isostatique à chaud.[106] Le Comité permanent R était alors arrivé à la conclusion que la VSSE avait fait preuve d'une certaine nonchalance dans sa manière de traiter, d'analyser et de diffuser ces informations.

En 2011, le Comité a bouclé une seconde enquête sur la manière dont la VSSE a suivi l'entreprise en question.[107] Le Comité a conclu que le service avait suivi

---

103 Une presse isostatique à chaud est une machine destinée à renforcer la résistance et la durabilité de certains matériaux en les soumettant à une pression très élevée à haute température. Ces presses sont utilisées dans l'industrie aéronautique, mais peuvent aussi être employées pour la fabrication de fusées et d'armes nucléaires. Il s'agit de ce que l'on appelle un outil « à double usage » (« *dual use* »), civil et/ou militaire, dont l'exportation est soumise aux mesures de contrôle prévues par les directives 1334/2000 et 428/2009 du Conseil de l'Union européenne.

104 « Traité sur la non-prolifération des armes nucléaires », voir : https://treaties.un.org/doc/Publication/UNTS/Volume%20729/volume-729-I-10485-French.pdf.

105 Dans ce cadre, le Comité ne s'est pas contenté d'interroger la VSSE. Il a aussi interrogé deux acteurs majeurs dans la mise en œuvre de la politique de non-prolifération en Belgique, à savoir Théo Van Rentergem, président de la Commission d'avis pour la non-prolifération des armes nucléaires (CANPAN) et Werner Bauwens, envoyé spécial du SPF Affaires étrangères pour le désarmement et la non-prolifération. Le rapport final a été approuvé en novembre 2013.

106 COMITÉ PERMANENT R, *Rapport d'activités 2005*,16-35.

107 COMITÉ PERMANENT R, *Rapport d'activités 2011*, 37-40.

attentivement certaines transactions avec un ou plusieurs pays sensibles, mais que ce suivi était surtout réactif et ponctuel, en ce sens qu'il n'avait été effectué qu'en fonction d'informations livrées par des services de renseignement étrangers. Un élément positif méritait toutefois d'être souligné : la VSSE ne s'est pas seulement intéressée aux intérêts sécuritaires liés au développement d'armes chimiques, bactériologiques ou nucléaires, mais aussi à la problématique de la concurrence et aux indices d'une éventuelle ingérence étrangère.[108] À l'instar de la VSSE, le Comité a estimé que dans la lutte contre la prolifération, l'intérêt sécuritaire doit prévaloir sur l'intérêt économique d'une entreprise.

II.5.2. LES CONSTATATIONS

Le 1er février 2011, la VSSE a été informée de l'exportation prévue d'une presse isostatique à chaud par le biais du secrétariat de la Commission d'avis pour la non-prolifération des armes nucléaires (CANPAN).[109] Le dossier figurait effectivement à l'ordre du jour de la réunion suivante organisée par la CANPAN, où siège un analyste de la VSSE. La VSSE s'est étonnée de ne pas avoir été avisée de ladite exportation par la société elle-même. En effet, en janvier 2011, le service avait contacté à deux reprises un cadre de la société, et ce précisément en vue d'échanger des informations sur la présentation d'éventuels dossiers délicats devant la CANPAN. Pour le Comité, ces contacts démontraient que dans l'intervalle, la VSSE avait adopté une attitude plus proactive à l'égard de l'entreprise concernée. Cependant, comme cette dernière avait dans ce cas-ci omis d'informer la VSSE, le suivi de ce dossier a une nouvelle fois été réactif.

Aussitôt après avoir été mise au courant de la transaction prévue, plusieurs vérifications ont été effectuées auprès de services partenaires étrangers. Les informations de ces correspondants, ajoutées aux éléments contextuels tirés d'une analyse de sources ouvertes, ont donné lieu à une note de synthèse sur la situation de la société. Cette note a été envoyée au ministre de la Justice début 2011.

En mars 2011, la VSSE a également envoyé deux notes classifiées à la CANPAN et au SPF Économie. Dans ces notes, le service a exposé les éléments indiquant que l'utilisateur final de la presse à chaud pouvait être relié à une entité ayant pris part dans le passé à un programme nucléaire militaire.

---

108 Les analyses de la VSSE portent généralement à la fois sur la protection du potentiel scientifique et économique et sur la prolifération. La CANPAN n'a toutefois pas pour mission de tenir compte des aspects économiques liés aux dossiers qui lui sont soumis.

109 Pour en savoir plus, voir la composition et les compétences de cette commission : l'Arrêté royal du 12 mai 1989 relatif au transfert à destination de pays non dotés d'armes nucléaires, des matières nucléaires, des équipements nucléaires, des données technologiques nucléaires et leurs dérivés (*M.B.* 15 juin 1989) et le Règlement d'ordre intérieur de la Commission d'avis pour la non-prolifération des armes nucléaires (*M.B.* 8 février 2010).

Lors des réunions de la CANPAN, la VSSE a laissé entendre qu'il s'agissait d'un dossier d'exportation délicat. Dans son analyse prudente et nuancée, elle a surtout formulé des hypothèses et des suspicions, et ce en l'absence d'informations plus précises.[110] Il est ressorti des éléments livrés par d'autres membres de la commission que les autorités du pays de destination étaient réticentes à fournir des renseignements complémentaires et à laisser s'organiser une visite de contrôle sur place après la livraison de la presse isostatique.

Avec ces doutes concernant le destinataire définitif de la presse à chaud et le contrôle de son utilisation, la CANPAN a certes émis un avis d'exportation favorable le 16 juin 2011, mais à la condition que le client fournisse davantage d'explications et que les autorités du pays concerné puissent donner des garanties quant à une visite de contrôle.

Étant donné qu'il était également d'avis que les autorités concernées ne donnaient pas de garanties suffisantes concernant la visite sur place, le ministre compétent a refusé la licence d'exportation. Il a renvoyé son dossier à la CANPAN, accompagné de l'avis qu'il avait reçu d'une autorité étrangère.

La VSSE a demandé au correspondant concerné des renseignements complémentaires sur l'avis que les autorités étrangères avaient fait parvenir au ministre compétent.[111] Le service n'a reçu qu'une réponse très « minimaliste », qui ne lui a pas permis de compléter ou d'affiner son analyse initiale.

En août 2011, le client étranger aurait accepté de donner un droit d'accès inconditionnel à la presse à chaud. Cependant, comme aucune autorité belge n'a pu s'engager à effectuer cette visite de contrôle sur place, la CANPAN a émis un avis défavorable pour l'exportation le 17 octobre 2011.

La VSSE a déclaré que les informations que les autorités étrangères avaient envoyées directement au ministre compétent ont joué un rôle déterminant dans la révision de l'avis de la CANPAN. Bien que la VSSE n'exclue jamais la possibilité d'un réflexe protectionniste de la part d'autorités étrangères lorsque le pays concerné possède des entreprises ou des industries concurrentes, elle n'a vu en l'espèce aucune tentative visant à influencer la concurrence économique. L'avis négatif aurait plutôt été dicté par une méfiance générale de ce gouvernement étranger à l'égard de certaines transactions d'exportation vers le pays concerné et par le fait que les autorités belges ne pouvaient exercer aucun contrôle effectif chez l'utilisateur final. La VSSE a aussi souligné qu'elle n'avait d'autre possibilité

110 Selon le directeur de la CANPAN, les notes que la VSSE transmet à la CANPAN contiennent généralement surtout des hypothèses et des suppositions et rarement des faits établis. La Commission trouve difficilement des motivations formelles pour ses avis dans les notes de la VSSE. Ce manque de certitude a de nombreuses causes. La VSSE a fait valoir le très haut degré de technicité de la matière, la complexité des réseaux d'approvisionnement, la difficulté d'obtenir des informations précises et actualisées sur les programmes en cours, l'absence d'accès aux données financières de ces réseaux, alors que le service souffre d'un déficit de personnel en la matière.

111 La VSSE a ensuite qualifié cet avis de « *laconique et négatif* ».

que de faire appel au service de renseignement étranger concerné, certainement dans le cadre d'une enquête sur une société étrangère active dans un secteur réputé de haute technologie. En outre, les autorités étrangères concernées figuraient sur l'« *Entity List* » du ministère américain des Affaires économiques (« *Department of Commerce* »). Ce qui signifie que, pour cette administration, les exportations vers l'entité concernée doivent être soumises à des exigences plus restrictives.

Le Comité permanent R a dès lors conclu qu'aucun dysfonctionnement ni aucune illégalité ne pouvait être imputé(e) à la VSSE dans ce dossier.

Le Comité s'est toutefois demandé si et de quelle manière la mise en place d'un système d'inspection sur place des destinataires finaux à l'étranger serait de nature à renforcer les capacités d'analyse et de contrôle en matière de prolifération d'armes de destruction massive dans un contexte international. À quelque niveau de compétence que l'on place ce système de contrôle (régional, fédéral, voire européen), une telle mission ne peut être confondue avec la promotion des intérêts économiques du pays.

II.6. FAITS PRÉTENDUMENT RÉPRÉHENSIBLES D'UN SERVICE DE RENSEIGNEMENT ÉTRANGER ET POSITION D'INFORMATION DE LA VSSE

En janvier 2010, le Comité permanent R a reçu un e-mail bref. Son auteur – de nationalité étrangère – affirmait qu'un gouvernement étranger avait organisé l'enlèvement de sa famille sur un territoire étranger. Le Comité s'est toutefois déclaré incompétent puisqu'il ne semblait y avoir aucun lien avec ses compétences. Il a néanmoins remis une copie de cet e-mail aux autorités judiciaires et à la VSSE.

Début décembre 2011, l'intéressé a déposé une nouvelle plainte. Il a ajouté à sa dénonciation une plainte avec constitution de partie civile auprès du juge d'instruction. Le Comité a cette fois décidé d'ouvrir une enquête de contrôle « *sur la position d'information de la VSSE à l'égard des faits dénoncés dans une plainte adressée aux autorités judiciaires belges par un ressortissant étranger et imputé à des agents d'un service de renseignement étranger* ». De nouveaux éléments indiquaient en effet un lien avec ses missions. L'enquête a démarré en janvier 2012 et a été finalisée à la fin février 2013.

L'intéressé était employé dans une ambassade à l'étranger. En 2003, il avait constaté, selon ses dires, que des responsables de l'ambassade et des personnes qui travaillaient pour les services de sécurité étrangers avaient des contacts réguliers avec des personnes qui défendaient un islam extrémiste, voire violent. Comme il ne trouvait aucune audience auprès ses supérieurs, il avait décidé d'en

informer les médias. En outre, il avait demandé d'emblée l'asile politique et obtenu un permis de séjour.

En octobre 2006, sa famille et lui se seraient rendus sous la menace à Bruxelles, où ils auraient été mis dans un vol à destination de son pays d'origine.

La Sûreté de l'État était informée des faits allégués depuis la mi-janvier 2010 par le biais du Comité (*supra*). De plus, le service avait reçu, à la fin janvier, un rapport de l'ambassadeur belge du pays d'origine de l'intéressé, qui avait pris contact avec lui peu de temps auparavant. L'ambassadeur ne se prononçait pas quant au fond de cette affaire, mais indiquait qu'il serait utile que les services de sécurité ouvrent une enquête. En effet, l'ambassadeur n'excluait pas totalement une tentative de compromission de l'ambassade. La VSSE a posé plusieurs devoirs d'enquête[112] qui ont donné lieu à un rapport d'information sommaire. Dans ce rapport, le service ne tirait aucune conclusion sur la crédibilité de l'histoire. De plus, aucune analyse n'a été effectuée par le service pour savoir si cette affaire avait été organisée afin de nuire à la diplomatie belge. La VSSE a estimé qu'il n'était pas nécessaire de rédiger une note d'évaluation pour des tiers « *au vu de la maigreur et de la non-pertinence en termes de renseignement des éléments récoltés* ». L'ambassadeur en question n'a pas été informé de la suite que la VSSE a donnée à son courrier parce que, selon la VSSE, le SPF Affaires étrangères n'avait jamais interrogé « officiellement » le service.

À la mi-août 2011, l'intéressé et sa famille sont parvenus à fuir le pays.

À la fin octobre 2011, l'intéressé a déposé plainte auprès du juge d'instruction concernant des faits d'enlèvement, de privation de liberté, de coups et blessures, commis à l'étranger et poursuivis en Belgique, et ce à l'encontre de personnes qui font probablement partie d'un service de renseignement étranger. Un peu plus tard, il a réitéré sa plainte, mais cette fois auprès du Comité permanent R.

Dans le courant du mois de février 2012, et juste après avoir été mise au courant par le Comité de l'ouverture d'une enquête de contrôle et de la plainte déposée auprès du juge d'instruction, la VSSE a pris contact avec le parquet compétent. Il s'est avéré que le parquet n'avait pas encore connaissance de la plainte en question.

En avril 2012, la VSSE a procédé à de nouvelles vérifications, qui n'ont toutefois apporté aucune preuve.

La VSSE considérait cette affaire comme très peu crédible à tous les égards. Les documents et les informations que l'intéressé a fournis, ainsi que leur formulation et le mode d'envoi, ont levé de sérieux doutes quant à leur véracité. D'après la VSSE, les informations obtenues par le correspondant étranger n'ont livré aucun élément pertinent qui aurait justifié une analyse approfondie et la communication des informations à un partenaire belge ou étranger.

---

[112] Une consultation des sources ouvertes, une demande d'information à un service étranger homologue, une vérification (qui s'est avérée négative vu que l'intéressé n'était pas encore connu de la VSSE en 2010)…

La VSSE a dès lors décidé que cette affaire n'était pas pertinente dans le cadre du travail de renseignement : *« En définitive, la dénonciation d'un enlèvement, comme le dépôt d'une plainte en justice sont des dossiers judiciaires et policiers qui ne relèvent pas de la compétence légale de la VSSE. »*

Le Comité permanent R s'est rallié à l'avis de la VSSE dans le sens où le traitement d'un dossier judiciaire ou policier ne relève évidemment pas de la compétence du service. Cependant, lorsque les faits dénoncés sont liés à l'une des menaces que la VSSE a pour mission légale de suivre (en l'espèce, l'ingérence), il est bel et bien pertinent de procéder à un suivi dans le cadre de la mission de renseignement. Le Comité a également estimé que la VSSE devait consigner par écrit les conclusions – même provisoires – de ses analyses, et ce dans le cadre de toute menace réelle ou potentielle dont elle est informée, de quelque manière et par qui que ce soit.

II.7. ATTEINTE ÉVENTUELLE À LA RÉPUTATION À LA SUITE DE DÉCLARATIONS DE LA VSSE

À la mi-juillet 2012, le Comité permanent R a reçu une plainte d'un particulier actif dans le secteur du recueil de renseignements économiques.[113] Il affirmait que la VSSE salissait sa réputation dans son secteur d'activités et que cela nuisait au bon développement de son réseau professionnel. En septembre 2012, le Comité permanent R a décidé d'ouvrir une enquête de contrôle *« sur les informations éventuellement diffusées par la VSSE à propos d'un particulier »*.[114]

Le Comité a constaté que le plaignant et ses associés étaient connus de la VSSE, et ce dans le cadre d'une enquête générale sur des entreprises de renseignement privées. L'enquête a été menée par le service qui, au sein de la VSSE, est chargé de la protection du potentiel scientifique et économique du pays (PSE). Le Comité a estimé que l'intérêt de la VSSE pour les activités de recueil de renseignements économiques du plaignant était légitime. Le Comité avait d'ailleurs lui-même déjà recommandé à la VSSE d'examiner ce genre d'activités.[115]

Cependant, les informations dont disposait la VSSE n'ont pas donné lieu à une quelconque analyse qui aurait dû démontrer quelle menace les activités du plaignant représenteraient pour le PSE. Les données recueillies ont donc été conservées dans le cadre des informations générales récoltées sur des sociétés de renseignement privées actives en Belgique. En outre, aucun rapport d'information ni aucune analyse à propos des activités du plaignant n'a été remis à des tiers.

Le Comité a conclu que les éléments sur lesquels se fondait la plainte n'ont pu être démontrés en aucune manière.

---

113 Conformément à l'article 40 L.Contrôle, le plaignant a demandé à conserver l'anonymat.
114 Le rapport final a été approuvé en avril 2013.
115 COMITÉ PERMANENT R, *Rapport d'activités 2003*, 25-108.

II.8. DIFFUSION PRÉTENDUMENT ILLÉGITIME DE DONNÉES PERSONNELLES PAR LA VSSE

II.8.1. LE CONTEXTE

À la mi-octobre 2012, un particulier a déposé plainte auprès du Comité permanent R. Plusieurs articles de presse[116] l'amenaient à supposer que la VSSE disposait d'un « dossier secret » à son égard. Il se demandait comment ce dossier est arrivé entre les mains de journalistes. Le plaignant a demandé au Comité une copie de tous les renseignements que la VSSE aurait recueillis à son propos, ainsi que l'ouverture d'une enquête sur les membres de la VSSE, qui selon lui ont commis un délit en communiquant des informations classifiées aux médias.

En avril 2013, le Comité a décidé d'ouvrir une enquête de contrôle, qui a été finalisée début septembre 2013.

Le Comité permanent R n'est bien sûr pas compétent pour fournir des renseignements sur les données éventuellement en possession de la VSSE. À cette fin, le Comité se réfère aux différentes possibilités prévues dans la Loi du 11 avril 1994 relative à la publicité de l'administration (LPA) et la Loi du 8 décembre 1992 relative à la protection de la vie privée (Loi Vie privée).

Le Comité a également vérifié si la VSSE avait effectivement constitué un dossier sur l'intéressé et si la presse avait eu connaissance de ces informations[117] ; si la VSSE avait porté atteinte aux droits que la Constitution et la loi confèrent au plaignant (plus particulièrement le droit au respect de la vie privée) et si la publication des prétendues informations avait porté préjudice au fonctionnement efficace de la VSSE.

II.8.2. CONSTATATIONS DE L'ENQUÊTE

L'enquête a démontré que la VSSE avait effectivement recueilli et conservé des renseignements (le plus souvent classifiés « confidentiels ») sur le plaignant. Il était connu au sein de la VSSE, ayant attiré l'attention du service en février 2006. En outre, le plaignant expose ses convictions extrémistes et son engagement sur son blog. L'intéressé ne cache pas son activisme au sein de *Sharia4Belgium*, dont il se présente comme étant le porte-parole. La VSSE a dès lors estimé que le comportement très inquiétant du plaignant devait faire l'objet d'un suivi.

---

116 PLA, LVDK et GVV, *Het Laatste Nieuws*, 22 septembre 2012 (Niet te temmen) ; JDB et JVC, *Het Nieuwsblad*, 24 septembre 2012 (Kopstuk Sharia4Belgium werkte even op Vlaams Kabinet).

117 Par exemple, en application de l'article 19, 2e alinéa de la L.R&S qui définit les conditions en matière de communication de renseignements à la presse par l'administrateur général de la VSSE ou par une communication inappropriée qui serait contraire aux règles de classification (L.C&HS).

Le Comité a estimé que ce suivi était légitime eu égard à la mission légale du service, qui consiste plus particulièrement à rechercher, analyser et traiter le renseignement relatif à toute activité qui menace ou pourrait menacer la sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel.[118]

La VSSE a déclaré n'avoir communiqué aucun renseignement à la presse à propos du plaignant. Si ce n'est les déclarations du plaignant lui-même, le Comité n'a trouvé aucun élément permettant d'affirmer ou de supposer une telle communication. Comme le plaignant s'est lui-même exprimé dans les médias et sur les réseaux sociaux, il n'était pas difficile pour la presse de trouver des indications de son engagement au sein de *Sharia4Belgium*. En l'absence d'indication portant sur une éventuelle diffusion illégitime de données à caractère personnel, le Comité permanent R a conclu que la VSSE n'avait en aucune façon porté atteinte aux droits que la Constitution et la loi confèrent au plaignant.

II.9. PLAINTE RELATIVE AU VOL D'UN ORDINATEUR PORTABLE

Début 2013, la présidente du Sénat a reçu un courriel d'une personne affirmant que son ordinateur portable lui avait été dérobé dans le courant de l'année 2007. Cette personne souhaitait savoir s'il était possible que le vol ait été commis par un service de renseignement belge. C'est ainsi que la présidente a demandé au Comité permanent R d'ouvrir une enquête.

Durant la période 2006-2007, le plaignant, qui travaillait en tant que journaliste, a écrit plusieurs articles sur la situation au Congo. Selon ses dires, ces publications lui auraient été reprochées, et il aurait été interpellé à plusieurs reprises par différents responsables politiques. Lorsqu'un ordinateur disparaît de chez lui – ainsi que chez une des personnes mentionnées dans ses articles – il déclare le vol à la police.[119] Il n'émet toutefois aucun soupçon à ce moment-là quant aux éventuels auteurs de ce vol. Ce n'est que plus tard qu'il se dit convaincu qu'un service de renseignement belge pouvait se cacher derrière ce vol : il est arrivé à cette conclusion à la suite d'une déclaration de son avocat et d'un tiers que le plaignant soupçonnait d'entretenir des liens avec un service de renseignement étranger. Lorsque la presse fait état du suivi de responsables politiques par la VSSE au début de l'année 2013 (voir Chapitre II.2), il n'exclut pas que des journalistes puissent également faire l'objet d'une attention particulière des services de renseignement.

---

118 Le Comité permanent R a également souligné à cet égard que le plaignant a été placé sous mandat d'arrêt le 29 août 2013 pour « menaces écrites » à l'encontre de plusieurs personnes. Il a été condamné par le tribunal correctionnel d'Anvers début janvier 2014.

119 Selon toute vraisemblance, cette enquête pénale a été classée sans suite.

Si le Comité permanent R n'est pas compétent pour examiner le caractère pénal de l'affaire, il a toutefois pour mission de traiter les plaintes et dénonciations relatives au fonctionnement, à l'intervention, l'action ou l'abstention d'action des services de renseignement. Aussi le Comité a-t-il interrogé le SGRS et la VSSE à ce propos.

Le SGRS connaissait uniquement le plaignant comme étant l'auteur des articles de presse mentionnés.

La VSSE disposait également de ces articles de presse, parce qu'ils traitaient d'une matière qui relève de sa compétence légale et qu'elle suit. Le plaignant lui-même n'a toutefois jamais fait l'objet d'une attention particulière de la part de ce service. La VSSE était néanmoins informée de la disparition de l'ordinateur portable et a même rédigé un bref rapport à cet égard, sans autre analyse et/ou commentaire.

Le Comité a conclu que le plaignant avait fait l'objet, à la fin de l'année 2007, d'une attention passive et restreinte des deux services de renseignement en raison de ses articles. Il n'a en outre trouvé aucun élément susceptible d'indiquer la moindre participation du SGRS ou de la VSSE dans les faits concernés.[120]

II.10. RAPPORTS INTERMÉDIAIRES DANS LES ENQUÊTES FAISANT SUITE AUX RÉVÉLATIONS D'EDWARD SNOWDEN

Les révélations d'E. Snowden ont donné lieu à l'ouverture de plusieurs enquêtes de contrôle (cf. II.11.11). Le Comité permanent R n'a pas pu clôturer ces enquêtes en 2013 en raison de leur complexité et de l'impact de ces révélations.

En revanche, dans le cadre de son enquête de contrôle *« relative à la position d'information des services de renseignement belges concernant les capacités de récolte massive et l'exploration de méta-data et le datamining par certains États et la manière dont ces États pratiqueraient l'espionnage politique de soi-disant « États amis » »*, le Comité a pu boucler un rapport intermédiaire circonstancié et le transmettre aux autorités compétentes. Ce rapport intermédiaire contient principalement l'analyse des sources ouvertes du Dr. Mathias Vermeulen[121], que le Comité permanent R avait sollicité en tant qu'expert en vertu de l'article 48 § 3 L.Contrôle. Son travail a donné lieu à l'étude *« Les révélations Snowden, interception massive de données et espionnage politique »*. Ce rapport était précédé d'une introduction du Comité permanent R qui situait les révélations d'E. Snowden dans un cadre plus large, et ce afin de faciliter la compréhension du rapport de l'expert. À la lumière de l'importance de cette enquête de

120 L'enquête de contrôle s'est clôturée en octobre 2013.

121 *Research Fellow* à l'Institut universitaire européen (EUI) de Florence et au sein du « Centre for Law, Science and Technology Studies » de la VUB.

contrôle, le rapport intermédiaire est joint en Annexe D au présent rapport d'activités.

Une deuxième enquête de contrôle[122], qui a également fait suite aux révélations d'E. Snowden, traite, entre autres des règles de droit nationales et internationales en vigueur en matière de protection de la vie privée à l'égard de moyens autorisant l'interception l'interception et l'exploitation à grande échelle des données de personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique). Dans le cadre de cette enquête, le Comité permanent R s'est également adjoint une spécialiste, le professeur Annemie Schaus, de l'Université Libre de Bruxelles. Sa « *Consultation sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle des données relatives à des personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique)* » figure également en annexe au présent rapport d'activités.

II.11. ENQUÊTES DE CONTRÔLE POUR LESQUELLES DES DEVOIRS D'ENQUÊTE ONT ÉTÉ POSÉS EN 2013 ET ENQUÊTES QUI ONT DÉBUTÉ EN 2013

Cette section énumère et situe brièvement toutes les enquêtes que le Comité permanent R a démarrées en 2013, ainsi que les enquêtes sur lesquelles il a continué de travailler au cours de cette même année, mais qui n'ont pas encore pu être clôturées.

II.11.1. LE SUIVI D'ÉLÉMENTS EXTRÉMISTES DANS L'ARMÉE

À l'occasion de briefings donnés par le SGRS dans le courant de l'année 2012, le Comité permanent R a pris connaissance de la problématique de militaires évoluant dans des milieux extrémistes et de militaires membres ou sympathisants de bandes criminelles de motards. Durant cette même période, les médias ont fait mention de la présence (temporaire), au sein du Bataillon de Chasseurs ardennais, d'un militant djihadiste qui aurait rédigé un manuel de combat en s'appuyant sur l'expérience acquise. Le Comité a dès lors décidé

[122] Enquête de contrôle « *sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle des données relatives à des personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique)* ». Les résultats de cette enquête ont été présentés à la Commission sénatoriale de suivi et aux ministres compétents à la mi-février 2014.

d'ouvrir une enquête de contrôle sur *« la recherche et le suivi par le SGRS d'éléments extrémistes au sein du personnel de la Défense et des Forces armées »*. L'enquête a pour but de vérifier si le SGRS aborde cette problématique de manière efficace et si ce service respecte les droits des citoyens dans ce cadre.

Au cours de l'enquête, la réglementation relative à la vérification (également appelée « screening ») des candidats à la Défense a fait l'objet de modifications. Il a été décidé d'élargir l'enquête à cette matière afin de se pencher sur deux processus : le screening durant la phase de recrutement, d'une part, et la détection et le suivi des éléments radicaux ou extrémistes déjà recrutés, d'autre part.

II.11.2. LA VSSE ET SA MISSION LÉGALE DE PROTECTION DES PERSONNES

En marge de l'*« enquête de contrôle conjointe relative aux évaluations de la menace effectuées par l'OCAM concernant des personnalités étrangères en visite en Belgique »*[123], le Comité a posé des questions à propos de la disponibilité de la VSSE lors de l'exécution de certaines missions de protection. La VSSE a évoqué à plusieurs reprises des raisons impératives de surcharge et de manque de moyens à cet égard.

Aussi le Comité permanent R a-t-il décidé d'ouvrir une enquête de contrôle afin d'examiner si la Sûreté de l'État mène ses activités de protection des personnes conformément à la loi et si elle fait preuve d'efficacité dans ce domaine.

La version classifiée « SECRET – Loi 11/12/1998 » du rapport final a été remise à l'administrateur général de la VSSE fin décembre 2013, et ce pour qu'il puisse émettre des remarques et proposer des ajouts aux fins de l'exhaustivité et la clarté du rapport. L'enquête a été clôturée et discutée au sein de la Commission de suivi du Sénat début 2014.

II.11.3. LA MANIÈRE DONT LES FONDS SPÉCIAUX SONT GÉRÉS, UTILISÉS ET CONTRÔLÉS

En 2011-2012, les autorités judiciaires ont ouvert deux enquêtes judiciaires sur l'éventuelle utilisation abusive de fonds destinés à la rémunération d'informateurs. En vertu de sa mission judiciaire, le service d'Enquêtes R a été sollicité dans les deux enquêtes (voir Chapitre VI). Vu les éléments mettant au jour d'éventuels problèmes structurels, le Comité permanent R a décidé, début septembre 2012, d'ouvrir une enquête thématique sur *« la manière de gérer,*

123 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 35-37.

d'employer et de contrôler les fonds destinés à la rémunération des informateurs de la VSSE et du SGRS».

Toutefois, compte tenu des enquêtes judiciaires en cours, l'enquête de contrôle a été suspendue immédiatement. Fin mars 2014, le Comité a décidé que l'enquête de contrôle pouvait reprendre.

II.11.4. ENQUÊTE DE CONTRÔLE SUR LA *JOINT INFORMATION BOX*

Pour ses initiateurs, la création d'une «*Joint Information Box*» (JIB) – approuvée par le Comité ministériel du renseignement et de la sécurité – constituait le point fort du «Plan d'action Radicalisme». Ce fichier de travail implanté au sein de l'OCAM vise à la «*collecte structurelle d'informations sur les entités suivies dans le cadre du Plan d'action Radicalisme*».

Lors d'une réunion commune des Comités permanents P et R à la mi-novembre 2012, il a été décidé d'ouvrir une enquête de contrôle «*sur la manière dont l'OCAM gère, analyse et diffuse les informations stockées dans la Joint Information Box (JIB), en rapport avec l'exécution du Plan Radicalisme*».

En 2013, les deux services d'Enquêtes P et R ont posé plusieurs actes d'enquête et rédigé un premier rapport de synthèse.

II.11.5. AGENTS DE RENSEIGNEMENT ET MÉDIAS SOCIAUX

Fin novembre 2012, les médias ont évoqué la présence de collaborateurs de services de renseignement sur des réseaux sociaux tels que Facebook et LinkedIn. La Commission sénatoriale de suivi a dès lors demandé au Comité permanent R d'ouvrir une enquête de contrôle sur «*l'ampleur du phénomène de publicité que donnent des collaborateurs de la Sûreté de l'État, mais aussi éventuellement du SGRS et de l'OCAM, de leur qualité d'agent de ces institutions sur Internet via des médias sociaux*». Le Comité a aussi reçu pour mission d'examiner les risques liés à une telle publicité et les mesures qui peuvent ou doivent être prises à cet égard.

Le Comité permanent R a démarré son enquête de contrôle concernant les collaborateurs du SGRS et de la VSSE en décembre 2012. Plusieurs actes d'enquête ont été posés. Un rapport définitif sera finalisé en 2014.

II.11.6. MEMBRES DU PERSONNEL DE L'OCAM ET MÉDIAS SOCIAUX

Quant au volet relatif aux collaborateurs de l'OCAM et leur présence sur des sites de réseaux sociaux, une enquête de contrôle commune a été ouverte début 2013 avec le Comité permanent P. En effet, en vertu de l'article 56, 6° L.Contrôle, le contrôle externe du fonctionnement de l'OCAM est exercé conjointement par les deux Comités.

Ce rapport sera également clôturé en 2014.

II.11.7. LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT ET DE L'OCAM CONCERNANT UN ÉLÈVE PILOTE

En juillet 2012, des articles de presse ont cité des «*flux d'informations dans les aéroports*» mentionnés dans une enquête de contrôle du Comité permanent P. Ces articles ont, entre autres, fait référence à une personne qui a pu suivre une formation de pilote dans un aéroport belge, alors que des signes de radicalisation avaient été relevés dans son passé. Cet exemple pouvait pointer une défaillance de l'échange d'informations entre les différents services de police dans les aéroports. Après que le Comité permanent R a pris connaissance du rapport, les deux comités ont décidé, en juin 2013, d'ouvrir une enquête de contrôle commune «*concernant la position d'information et le suivi par les services d'appui de l'OCAM – ainsi que l'évaluation de la menace par l'OCAM – à propos d'un particulier X ayant obtenu l'autorisation de suivre une formation de pilote d'avion en Belgique*».

L'enquête se trouve dans sa phase finale.

II.11.8. UNE PLAINTE DE L'ÉGLISE DE SCIENTOLOGIE CONTRE LA SÛRETÉ DE L'ÉTAT

Dans le courant des mois de janvier et février 2013, plusieurs articles de presse ont mentionné que la Sûreté de l'État vérifiait si et quand des responsables politiques étaient en contact avec des organisations telles que l'Église de scientologie (voir II.2). Dans ce cadre, les articles citaient des extraits d'une note classifiée et de l'«Analyse de phénomène sur des activités d'ingérence non étatiques» de la VSSE. En mars 2013, l'Église de scientologie a déposé une plainte auprès du Comité permanent R. Celui-ci a décidé d'ouvrir une enquête de contrôle sur la plainte de l'Église de scientologie relative à la manière dont la Sûreté de l'État a rédigé et diffusé un rapport qui la concerne. La plupart des

actes d'enquête ont été bouclés en 2013. Le rapport final a été bouclé à la mi-2014.

II.11.9. LES CONTACTS INTERNATIONAUX DE L'OCAM

L'Organe de coordination pour l'analyse de la menace a notamment pour mission d'entretenir des contacts avec des « services étrangers ou internationaux homologues » (art. 8, 3° L. OCAM). Lors de leur réunion commune de début mai 2013, les Comités permanents P et R ont décidé de mener une enquête sur la manière dont l'OCAM remplit cette mission.[124] Tous les acteurs concernés ont été interrogés de manière approfondie en 2013.

II.11.10. ENQUÊTE DE CONTRÔLE RELATIVE AUX ÉLÉMENTS TRANSMIS PAR LA VSSE DANS LE CADRE D'UN DOSSIER DE NATURALISATION

Un procureur du Roi s'est opposé à l'octroi de la nationalité belge à un particulier, s'appuyant sur des informations de la VSSE concernant des « *faits personnels graves* ». Ces informations constitueraient un empêchement à sa naturalisation. L'intéressé a estimé être victime d'un malentendu, qui a donné lieu à une violation de ses droits individuels par la VSSE. À la fin juillet 2013, il a déposé plainte auprès du Comité permanent R, qui a alors ouvert une enquête de contrôle. Cette enquête a été finalisée en février 2014.

II.11.11. PLAINTE RELATIVE À LA MANIÈRE DONT LA VSSE SUIT LE GÉRANT D'UNE SOCIÉTÉ D'EXPORTATION BELGE

À la suite d'une plainte, le Comité permanent R a ouvert, début octobre 2013, une enquête de contrôle « *concernant la manière dont la VSSE contacte un gérant d'une entreprise belge, qui dispose de données spécifiques quant à des exportations vers l'Iran et agit envers lui* ». Plusieurs actes d'enquête ont été posés. Le plaignant et des représentants du service de renseignement concerné ont été entendus à plusieurs reprises. L'enquête sera clôturée dans le courant de l'année 2014.

---

124 « Enquête de contrôle commune sur la manière dont l'OCAM entretient des relations internationales avec des services étrangers ou internationaux homologues en application de l'article 8, 3° de la L.OCAM du 10 juillet 2006 ».

II.11.12. QUATRE ENQUÊTES DE CONTRÔLE DANS LE CADRE DES RÉVÉLATIONS D'EDWARD SNOWDEN

Le 6 juin 2013, les journaux *The Guardian*[125] et *The Washington Post*[126] ont publié des informations émanant de dizaines de milliers de documents (classifiés) rendus publics par Edward Snowden, qui a occupé différentes fonctions dans et pour les services de renseignement américains. Depuis lors, de nouvelles révélations se sont rapidement succédé.

Ces articles donnaient un aperçu du contenu de programmes extrêmement secrets, principalement de la *National Security Agency* (NSA) américaine. Ils révélaient entre autres l'existence du programme « PRISM », dans le cadre duquel la NSA obtient des (méta)données de télécommunications. Ils dévoilaient par ailleurs que des services américains, mais aussi britanniques, avaient monté des opérations de renseignement à l'égard de certaines institutions internationales et structures de coopération (ONU, UE et G20), opérations qui visaient également des pays dits « amis ».

Ces révélations ont donné lieu à l'ouverture de nombreuses enquêtes (parlementaires, judiciaires et de renseignement) aux quatre coins du monde, ainsi qu'en Belgique. Le 1er juillet 2013, la Commission de suivi du Sénat a demandé au Comité permanent R *« […] une mise à jour des informations existantes relatives aux pratiques d'exploitation des données ('datamining'). Le service de renseignement américain NSA ne serait pas le seul à le faire. Des données seraient également interceptées et analysées massivement par le Royaume-Uni. La commission de suivi souhaite d'autre part que le Comité R examine les conséquences pour la protection du potentiel scientifique et économique de notre pays et des missions légales de nos services de renseignement. Enfin, la commission de suivi souhaite que le Comité R confronte ces pratiques aux règles de droit nationales et internationales qui protègent la vie privée des citoyens.* »

Aussi le Comité permanent R a-t-il ouvert trois enquêtes de contrôle qui sont naturellement étroitement liées. Il en va de même pour une quatrième enquête[127] également initiée à la suite d'une plainte du président de l'Ordre néerlandais des avocats auprès du Barreau de Bruxelles.

La première enquête de contrôle[128] – qui a fait l'objet de discussions début 2014 au sein de la Commission de suivi du Sénat – répond aux questions suivantes :

---

125 G. GREENWALD et E. MACASKILL, *The Guardian*, 6 juin 2013 (« NSA Taps in to Internet Giant's Systems to Mine User Data, Secret files Reveals »).

126 B. GELLMAN et L. POITRAS, *The Washington Post*, 6 juin 2013 (« US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program »).

127 Enquête de contrôle « suite à la plainte d'un bâtonnier sur l'utilisation d'informations issues des récoltes massives de méta-data d'origine étrangère dans des affaires pénales belges ».

128 Enquête de contrôle « relative à la position d'information des services de renseignement belges concernant les capacités de récolte massive et l'exploration de méta-data et de

- De quels moyens les grandes puissances telles que les États-Unis et la Grande-Bretagne disposent-elles pour intercepter et exploiter à grande échelle des données de personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique) et de quelles données s'agit-il (tant d'un point de vue quantitatif que qualitatif) ?
- Dans quelle mesure les services de renseignement belges étaient-ils au courant des moyens dont disposaient ces grandes puissances (ou dans quelle mesure devaient-ils en être informés compte tenu de leurs missions légales) ? Des renseignements ont-ils été recueillis à cet égard ou cela n'a-t-il pas été jugé souhaitable ? Nos services offrent-ils une protection suffisante en la matière ?
- Quelle est la signification/valeur de la notion de « pays ami » dans le contexte des services de renseignement, et dans quelle mesure cette notion détermine-t-elle l'attitude de nos propres services de renseignement ? Bien que les questions soulevées par la Commission de suivi ne mentionnaient pas explicitement cet aspect des révélations (c'est-à-dire certaines opérations de services de renseignement de « pays amis » à l'égard d'institutions internationales ou supranationales au sein desquelles la Belgique est représentée ou à l'égard d'intérêts belges), le Comité permanent R a décidé de s'y intéresser également, et ce vu l'intérêt intrinsèque de cette matière.

La deuxième enquête de contrôle[129] – qui a également déjà fait l'objet de discussions au sein de la Commission sénatoriale – traite des règles de droit nationales et internationales en vigueur en Belgique en matière de protection de la vie privée à l'égard de moyens autorisant l'interception et l'exploitation à grande échelle des données relatives à des personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique). Quant aux règles internationales, l'attention s'est naturellement portée sur l'article 8 CEDH (où sont développés tant l'« effet horizontal » de ces dispositions que les éventuelles « obligations positives » qui en découlent pour un État), sur l'article 17 de la Convention internationale relative aux droits civils et politiques (D.C.P), sur la Directive 95/46/CE du 24 octobre 1995, sur le Traité n° 108 du 28 janvier 1981 du Conseil de l'Europe, ainsi que sur les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. D'autres règles plus spécifiques ont aussi été prises en considération : les règles relatives au *Passenger*

datamining par certains États et la manière dont ces États pratiqueraient l'espionnage politique de soi-disant « États-amis » ». Les résultats de cette enquête ont été discutés avec la Commission sénatoriale de suivi et présentés aux ministres compétents à la mi-avril 2014.

129 Enquête de contrôle « sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique) ». Les résultats de cette enquête ont été présentés à la Commission sénatoriale de suivi et aux ministres compétents à la mi-février 2014.

Name Record, à Swift, à Safe Harbour… Enfin, les règles de droit internes portant sur la protection de la vie privée et des données ont été examinées : la Loi relative au traitement des données à caractère personnel et son arrêté d'exécution, ainsi que les dispositions spécifiques au fonctionnement des services de renseignement. Cette deuxième enquête de contrôle propose également un aperçu des moyens juridiques dont disposent les États, les citoyens ou les entreprises pour introduire un recours contre des violations (éventuelles) des droits (fondamentaux).

La troisième enquête de contrôle[130] – qui n'a pas encore été finalisée – traite des implications éventuelles de l'exploitation de données sur la protection du potentiel scientifique et économique du pays. Elle entend vérifier si les services de renseignement belges :

- se sont intéressés à ce phénomène ;
- ont détecté une menace réelle ou éventuelle pour le potentiel scientifique et économique belge ;
- en ont informé les autorités compétentes et ont proposé des mesures de protection ; et
- disposent de moyens suffisants et adéquats pour suivre cette problématique.

La quatrième enquête, lancée après dénonciation d'un bâtonnier, porte principalement sur l'utilisation éventuelle dans des affaires pénales de données qui ont été interceptées de manière massive (et illégale).

130 Enquête de contrôle « sur l'attention que les services de renseignement belges portent (ou non) sur les menaces que peuvent représenter pour le potentiel scientifique et économique de la Belgique des programmes de surveillance électronique sur les systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou des services de renseignement étrangers ».

CHAPITRE III
CONTRÔLE DES MÉTHODES PARTICULIÈRES DE RENSEIGNEMENT

L'article 35 § 1er, 1° L.Contrôle stipule que le Comité doit consacrer, dans son rapport d'activités annuel, *« une attention spécifique aux méthodes spécifiques et exceptionnelles de recueil de données, telles qu'elles sont visées dans l'article 18/2 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité [et] à l'application du chapitre IV/2 de la même loi »*.[131] Ce chapitre traite dès lors de la mise en œuvre des méthodes particulières de renseignement par les deux services de renseignement et de la manière dont le Comité permanent R exerce son rôle juridictionnel à cet égard. Ce rapport est un condensé des deux rapports semestriels que le Comité doit rédiger pour sa Commission de suivi.[132] Dans ces deux rapports semestriels, il convient non seulement de se pencher sur une série de données quantitatives (nombre d'autorisations, durée des méthodes, personnes concernées), mais aussi sur les « résultats obtenus » par la mise en œuvre des méthodes MRD. Vu l'importance de ce dernier aspect, le Comité tenait à reprendre brièvement son analyse en la matière dans ce rapport d'activités.

III.1. LES RÉSULTATS OBTENUS

'Although the financial costs of an intelligence operation are often tangible, the benefits that it produces are often intangible… This is especially true when the object of an operation is the non-occurrence of an event, such as a terrorist attack'.[133] Cette citation résume d'emblée la difficulté de mesurer, dans un contexte de renseignement, le résultat d'une opération ou d'une méthode déterminée. Le problème de la mesure des « résultats » ne concerne d'ailleurs pas seulement le milieu du renseignement. Le monde judiciaire y est lui aussi

131 Pour une analyse des méthodes particulières de renseignement et du contrôle exercé sur celles-ci, voir : COMITÉ PERMANENT R, *Rapport d'activités 2010,* 49-61 en W. VAN LAETHEM, D. VAN DAELE et B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

132 Art. 35 § 2 et 66*bis* § 2, alinéa 3, L.Contrôle.

133 H. BORN en A. WILLS, *Overseeing Intelligence Services – A Toolkit*, DCAF, 2012.

confronté lorsqu'il veut évaluer les résultats de ses méthodes particulières de recherche (MPR). Nous constatons dès lors que les autorités judiciaires ne procèdent pas à une telle analyse, et ce malgré la formulation de l'article 90*decies* du Code d'instruction criminelle.[134]

Nonobstant cette difficulté, le Comité a tenté d'avoir une vue sur « l'utilité » des méthodes MRD mises en œuvre, dans un premier temps simplement en interrogeant les deux services de renseignement, et ensuite en procédant à une analyse approfondie de quatre cas assez larges.

Les questions posées aux services de renseignement concernaient 238 décisions et autorisations MRD couvrant la période allant de septembre 2010 à décembre 2012, ou autrement dit, sur un peu plus de 9 % du nombre total d'autorisations.[135] Les deux services ont été interrogés sur la manière dont ils évaluaient l'efficacité des méthodes mises en œuvre en fonction des objectifs visés dans l'autorisation. La VSSE était d'avis que dans 84 % des cas, tous les objectifs visés étaient atteints, dans 8,5 % des cas, une partie des objectifs, et dans 7,5 % des cas, aucun des objectifs. Le SGRS a répondu comme suit : dans 72 % des cas, le service estimait que tous les objectifs visés étaient atteints, dans 16 % des cas, une partie des objectifs, et dans 12 % des cas aucun des objectifs.

En se basant sur cette auto-évaluation, le Comité a mené une enquête de contenu, dans laquelle toutes les méthodes qui ont été mises en œuvre à l'égard de quatre cibles différentes (personne ou organisation) ont été analysées en détail. Pour chaque cible, le Comité a examiné quelles méthodes MRD ont été employées successivement et ce qu'elles ont livré en terme de contenu, et ce en fonction de la finalité de la méthode (p. ex. découvrir le réseau d'une personne ou acquérir la certitude de son implication dans le cadre d'une menace). Au total, 160 méthodes ont été appliquées pour les quatre cibles.

La première cible a fait l'objet d'une méthode MRD à 18 reprises. Les résultats obtenus n'ont toutefois pas permis de confirmer les soupçons du service, mais bien de les renforcer, notamment parce que le service a eu une meilleure vue sur le réseau de la personne concernée. C'était d'ailleurs aussi l'objectif préalablement défini. Les méthodes MRD ont fourni en la matière des informations qui ne pouvaient pas être recueillies avec des méthodes de

---

134 « *Enfin, il convient d'émettre une remarque concernant l'examen du 'résultat' des diverses mesures. Dans la pratique, il s'avère très difficile de définir le 'résultat' des diverses mesures de façon suffisamment adéquate ainsi que d'examiner le résultat 'isolé' (par mesure), étant donné qu'il est (généralement) question d'utilisation parallèle de différentes méthodes de recherche et d'enquête. En outre, il est impossible de rendre le 'résultat' de façon correcte ou du moins de manière satisfaisante sans quelques informations supplémentaires sur le contexte dans lequel les mesures ont été utilisées et sans informations sur le jugement du juge du fond.* » (Service de la Politique Criminelle, *Rapport 2013 en application de l'article 90decies Code d'instruction criminelle (2012), s.l.*, 6).

135 En ce qui concerne la VSSE, il s'agit de 94 méthodes spécifiques et de 71 méthodes exceptionnelles, et en ce qui concerne le SGRS, il s'agit de 48 méthodes spécifiques et de 25 méthodes exceptionnelles.

renseignement « ordinaires ». Ce cas a également montré que le suivi de l'intéressé avait débuté sur indication d'un service de renseignement étranger. Conformément à l'article 20 L.R&S, les informations obtenues ont été partagées avec ce service de renseignement.

Une deuxième cible – une organisation – a fait l'objet de 47 méthodes. Pour découvrir qui est en contact avec qui, l'identification d'abonnés de moyens de communication électroniques a été utilisée à de multiples reprises. De plus, il a été fait usage de la possibilité de localiser des personnes au moyen de leur télécommunication et ces personnes ont été prises en filature. L'on peut affirmer dans le cas présent que les objectifs préalablement définis par les méthodes MRD ont été globalement atteints. En outre, ce cas illustre très bien la cohérence entre les méthodes « ordinaires » et les méthodes MRD, et entre les diverses méthodes MRD, où une méthode servait de base à une autre.

Dans un troisième cas, 79 méthodes MRD ont été appliquées. Il s'agissait ici aussi majoritairement d'identifications et de localisations. Et dans ce cas-ci également, la cible a été « amenée » au service belge de renseignement par un service partenaire. Les méthodes n'ont cependant pas permis de confirmer que cette personne représentait effectivement une menace. Il s'est néanmoins avéré qu'elle était en contact avec des personnes qui représentaient une menace réelle. Par ailleurs, il a pu être établi, via l'accès à des données bancaires, que certains flux financiers coïncidaient dans le temps avec certaines activités de personnes qui étaient elles aussi dans le collimateur des services de renseignement. Le Comité a dû constater dans ce dossier que la position d'information du service concerné ne s'en est somme toute pas trouvée grandement renforcée malgré la mise en œuvre de 79 méthodes.

Dans le dernier cas, 16 méthodes MRD ont été employées à l'égard d'une organisation déterminée. Il s'agissait principalement d'une observation (de longue durée) avec l'aide de moyens techniques et la consultation de données bancaires. L'enquête avait pour objectif d'examiner qui pouvait compter parmi les membres du réseau de l'organisation. Le Comité a constaté que les moyens techniques utilisés présentaient parfois des défaillances, si bien que les résultats faisaient défaut. De plus, une partie des données obtenues (des images) ne pouvaient être que partiellement traitées par manque de temps et de personnel. Les données qui pouvaient être analysées ont été traitées dans des dizaines de rapports de renseignement. Il ressort de l'étude du Comité que les observations et l'analyse des données financières ont certainement contribué à la réalisation de l'objectif préalablement défini.

III.2. LES CHIFFRES RELATIFS AUX MÉTHODES SPÉCIFIQUES ET EXCEPTIONNELLES

Entre le 1er janvier et le 31 décembre 2013, 1378 autorisations ont été accordées par les deux services de renseignement confondus pour l'utilisation de méthodes particulières de renseignement, 1224 pour la VSSE (1102 spécifiques et 122 exceptionnelles) et 154 par le SGRS (131 spécifiques et 23 exceptionnelles).

Le tableau ci-dessous établit une comparaison avec les chiffres de 2011 et de 2012. En outre, il convient de noter que depuis janvier 2013, le Comité utilise une autre méthode de calcul pour une méthode particulière déterminée. Auparavant, le nombre de « Prises de connaissance de données d'identification de moyens de communication électroniques » était mentionné en note de bas de page, mais n'était pas repris comme tel dans les totaux. C'est cette option qui avait été retenue puisque la plupart des « Prises de connaissance de données d'identification » sont autorisées par les dirigeants des services de renseignement dans un seul document, où est aussi autorisée, par exemple, une « Prise de connaissance de données d'appel » ou une « Prise de connaissance de données de localisation ». Étant donné qu'il s'agit *stricto sensu* d'autres méthodes, le Comité permanent R a jugé qu'un calcul séparé de telles « Prises de connaissance de données d'identification » donne une vue plus juste du nombre de méthodes spécifiques effectivement mises en œuvre. En d'autres termes, lorsque le nombre de méthodes particulières mentionnées dans ce rapport est plus élevé qu'à la même période l'année dernière, cela tient principalement à une méthode de calcul différente, et donc pas au fait que d'autant plus de méthodes ont été employées. L'impact de cette nouvelle manière de procéder est immédiatement visible dans le tableau ci-dessous.

	SGRS		VSSE		TOTAL
	Méthodes spécifiques	Méthodes exceptionnelles	Méthodes spécifiques	Méthodes exceptionnelles	
2011	60	7	731	33	831
2012	67	24	655	102	848
2013	131	23	1102	122	1378

La nette augmentation – à première vue – doit donc être nuancée. En se basant sur le calcul tel qu'il a été effectué les années précédentes, cela équivaudrait à 960 méthodes seulement pour l'année 2013. Par rapport à 2012, il y a donc eu un accroissement de quelque 13 % du nombre de méthodes MRD mises en œuvre. Les tableaux ci-après montrent clairement où se situe cet accroissement.

Dans ce qui suit, trois grandes rubriques sont établies pour chaque service : des données chiffrées sur les méthodes spécifiques, sur les méthodes exceptionnelles et sur les menaces visées par les différentes méthodes ainsi que les intérêts à protéger.

III.2.1. LES AUTORISATIONS RELATIVES AU SGRS

III.2.1.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	7	8	14
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	0	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	0	0	0
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou l'accès direct à des fichiers de données	23 dossiers	25 dossiers	66 méthodes[136]
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	17	30	15
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	13	4	36
TOTAL	60	67[137]	131[138]

En ce qui concerne les méthodes spécifiques mises en œuvre par le SGRS, la comparaison avec les années précédentes fait ressortir deux tendances : le nombre d'observations et le nombre de localisations ont considérablement augmenté.

136 En comparaison avec les années précédentes, une diminution est à noter : les 66 autorisations concernent en effet 16 dossiers.

137 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

138 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

III.2.1.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0	1	1
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	0	0	0
Création ou recours à une personne morale fictive	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	0	0	0
Collecte de données concernant des comptes bancaires et des transactions bancaires	5	7	5
Intrusion dans un système informatique	0	2	0
Écoute, prise de connaissance et enregistrement de communications	2	14	17
TOTAL	7	24[139]	23[140]

III.2.1.3. Les intérêts et les menaces justifiant le recours à des méthodes particulières[141]

Le SGRS est autorisé à utiliser les méthodes spécifiques et exceptionnelles dans le cadre de trois de ses missions, qui elles-mêmes comprennent des intérêts spécifiques à protéger :

- La mission de renseignement orientée vers les menaces visant, entre autres, l'intégrité du territoire national, les plans de défense militaires et le potentiel scientifique et économique en rapport avec la défense (art. 11, 1° L.R&S) ;
- La mission en matière de sécurité militaire qui vise par exemple le maintien de la sécurité militaire du personnel relevant de la Défense, des installations militaires et des installations militaires et des systèmes informatiques et de communications militaires (art. 11, 2° L.R&S) ;
- La protection des secrets militaires (art. 11, 3° L.R&S).

139 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

140 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

141 Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

NATURE DE LA MISSION	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Mission de renseignement	38	63	183
Sécurité militaire	8	7	26
Protection des secrets	19	21	50

Contrairement à la VSSE, les menaces auxquelles le SGRS peut ou doit être attentif ne sont pas définies dans la loi. Cependant, ce service mentionne systématiquement dans ses autorisations quelle menace est visée. Une telle transparence mérite en effet d'être soulignée. En ce qui concerne la mise en œuvre de méthodes particulières, les chiffres montrent que la lutte contre l'espionnage est restée la première priorité du service de renseignement militaire.

NATURE DE LA MENACE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Espionnage	54	78	157
Terrorisme (et processus de radicalisation)	10	3	11
Extrémisme	3	3	42
Ingérence	0	2	2
Organisations criminelles	0	1	28
Autres	0	5	29

III.2.2. LES AUTORISATIONS RELATIVES À LA VSSE

III.2.2.1. Les méthodes spécifiques

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Pénétration et observation dans des lieux accessibles au public à l'aide d'un moyen technique	89	75	109
Pénétration et inspection de lieux accessibles au public à l'aide d'un moyen technique	0	1	0
Prise de connaissance de données d'identification du trafic postal et réquisition du concours d'un opérateur postal	4	2	0

NATURE DE LA MÉTHODE SPÉCIFIQUE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Prise de connaissance des données d'identification de moyens de communication électroniques ; réquisition du concours d'un opérateur ; ou l'accès direct à des fichiers de données	355 dossiers	254 dossiers	613[142] méthodes
Prise de connaissance des données d'appel de moyens de communication électroniques et réquisition du concours d'un opérateur	237	147	136
Prise de connaissance des données de localisation de moyens de communication électroniques et réquisition du concours d'un opérateur	46	176	244
TOTAL	731	655[143]	1102[144]

En ce qui concerne les méthodes spécifiques mises en œuvre par la VSSE, la comparaison avec les années précédentes fait ressortir deux tendances : le nombre d'observations et le nombre de localisations ont considérablement augmenté.

III.2.2.2. Les méthodes exceptionnelles

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Pénétration et observation, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	2	8	6
Pénétration et inspection, à l'aide ou non d'un moyen technique, de lieux privés qui ne sont pas accessibles au public	3	6	6
Création ou recours à une personne morale fictive	0	0	0
Ouverture et prise de connaissance d'un courrier confié ou non à un opérateur postal	4	12	6
Collecte de données concernant des comptes bancaires et des transactions bancaires	10	16	11

142 En comparaison avec les années précédentes, une diminution est à noter : les 613 autorisations concernent en effet 243 dossiers.

143 Dans dix-sept cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel. L'année dernière, il s'agissait de neuf cas.

144 Dans neuf cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel. On dénombrait le même nombre de cas l'année dernière.

NATURE DE LA MÉTHODE EXCEPTIONNELLE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Intrusion dans un système informatique	3	10	12
Écoute, prise de connaissance et enregistrement de communications	11	50	81
TOTAL	33	102[145]	122[146]

Les chiffres montrent à nouveau une augmentation frappante du nombre de mesures d'écoutes : de 11 en 2011 à 50 en 2002 et jusqu'à 81 en 2013. En ce qui concerne les autres méthodes exceptionnelles, aucune différence significative n'a été constatée.

III.2.2.3. Les menaces et les intérêts justifiant le recours aux méthodes particulières[147]

La VSSE n'est autorisée à intervenir que pour la sauvegarde des intérêts suivants :
- La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel ;
- La sûreté intérieure de l'État et les relations internationales ;
- Les éléments essentiels du potentiel scientifique et économique.

INTÉRÊTS PROTÉGÉS	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
La sûreté intérieure de l'État et la pérennité de l'ordre démocratique et constitutionnel	694	704	1994
La sûreté extérieure de l'État et les relations internationales	571	693	1965
La sauvegarde des éléments essentiels du potentiel scientifique et économique	24	15	18

Le tableau suivant reprend les menaces (potentielles) visées par la VSSE dans le contexte de la mise en œuvre des méthodes spécifiques et exceptionnelles. Une méthode peut naturellement viser plusieurs menaces. La VSSE peut utiliser les méthodes spécifiques dans le cadre de toutes les menaces qui relèvent de ses compétences (art. 8 L.R&S). Les méthodes exceptionnelles ne peuvent pas être employées dans le cadre de l'extrémisme et de l'ingérence. Elles sont toutefois

145 Dans cinq cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

146 Dans un cas, l'autorisation concernait une des catégories professionnelles protégées, c'est-à-dire un avocat, un médecin ou un journaliste professionnel.

147 Plusieurs intérêts et menaces peuvent figurer dans une même autorisation.

autorisées dans le cadre du processus de radicalisation menant au terrorisme (art. 3, 15° L.R&S).

NATURE DE LA MENACE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
Espionnage	193	243	561
Terrorisme (et processus de radicalisation)	371	288	1086
Extrémisme	319	177	602
Prolifération	17	28	27
Organisations sectaires nuisibles	4	7	15
Ingérence	3	10	27
Organisations criminelles	3	5	18

Ces chiffres montrent que le terrorisme et l'extrémisme – mais aussi l'espionnage – demeurent les points d'attention de la VSSE, du moins pour ce qui est de la mise en œuvre des méthodes MRD.

III.3. LES ACTIVITÉS DU COMITÉ PERMANENT R EN SA QUALITÉ D'ORGANE JURIDICTIONNEL ET D'AUTEUR D'AVIS PRÉJUDICIELS EN MATIÈRE DE MÉTHODES MRD

III.3.1. LES CHIFFRES

Le Comité permanent R peut être saisi de cinq manières pour se prononcer sur la légalité des méthodes particulières de renseignement (art. 43/4 L.R&S) :
- D'initiative ;
- A la demande de la Commission de la protection de la vie privée ;
- Par le dépôt d'une plainte d'un citoyen ;
- De plein droit chaque fois que la Commission BIM a suspendu une méthode spécifique ou exceptionnelle pour cause d'illégalité et a interdit l'exploitation des données ;
- De plein droit quand le ministre compétent a donné son autorisation sur base de l'article 18/10, § 3 L.R&S.

De plus, le Comité peut aussi être saisi en sa qualité d'« auteur d'avis préjudiciels » (articles 131*bis*, 189*quater* et 279*bis* CIC). Le Comité rend, sur demande, un avis

sur la légalité de renseignements recueillis au moyen de méthodes spécifiques ou exceptionnelles, et qui sont utilisés dans le cadre d'une affaire pénale. Les demandes d'avis sont introduites par les juridictions d'instruction ou par les juridictions de fond. Le Comité n'intervient pas alors *stricto sensu* comme un organe juridictionnel.

TYPE DE SAISINE	NOMBRE 2011	NOMBRE 2012	NOMBRE 2013
1. D'initiative	13	19	16
2. Commission Vie Privée	0	0	0
3. Plainte	0	0	0
4. Suspension par la Commission BIM	15	17	5
5. Autorisation du ministre	0	2	2
6. Auteur d'avis préjudiciel	0	0	0
TOTAL	28	38	23

Les chiffres montrent que la diminution du nombre de saisines tient au fait que la Commission BIM a prononcé moins de suspensions.

Une fois saisi, le Comité peut prendre plusieurs types de décisions (intermédiaires). Toutefois, dans les deux cas (1. en 2. ci-après), une décision est prise avant la saisine proprement dite.

1. Constater la nullité de la plainte pour cause de vice de forme ou absence d'un intérêt personnel et légitime (art. 43/4, alinéa 1er, L.R&S) ;
2. Décider de ne pas donner suite à une plainte qui est manifestement non fondée (art. 43/4, alinéa 1er, L.R&S) ;
3. Suspendre la méthode contestée dans l'attente d'une décision définitive (art. 43/4, dernier alinéa, L.R&S) ;
4. Demander des informations complémentaires à la Commission BIM (43/5 § 1er, alinéa 1er et alinéa 3, L.R&S) ;
5. Demander des informations complémentaires au service de renseignement concerné (43/5 § 1er, alinéa 3, L.R&S) ;
6. Ordonner une mission d'enquête pour le service d'Enquêtes R (art. 43/5 § 2 L.R&S). Dans cette rubrique, on fait référence à la fois aux multiples informations complémentaires recueillies par le service d'Enquêtes R d'une manière plutôt informelle avant la saisine proprement dite et aux informations recueillies par le Comité après la saisine ;
7. Procéder à l'audition des membres de la Commission BIM (art. 43/5 § 4, alinéa 1er, L.R&S) ;

8. Procéder à l'audition du dirigeant du service de renseignement ou des membres du service de renseignement concerné (art. 43/5 § 4, alinéa 1er, L.R&S) ;
9. Statuer sur les secrets relatifs à une information ou instruction judiciaire en cours dont les membres des services de renseignement sont dépositaires, après concertation avec le magistrat compétent (art. 43/5 § 4, alinéa 2, L.R&S) ;
10. Pour le président du Comité permanent R, statuer sur la demande du dirigeant du service ou le membre du service de renseignement qui estime devoir garder le secret dont il est dépositaire parce que sa divulgation est de nature à porter préjudice à la protection des sources, à la protection de la vie privée de tiers ou à l'accomplissement des missions du service de renseignement (art. 43/5 § 4, alinéa 3, L.R&S) ;
11. Mettre fin à la méthode concernée si celle-ci est toujours en cours ou si elle a été suspendue par la Commission BIM, et interdire l'exploitation des données recueillies grâce à cette méthode et leur destruction (art. 43/6 § 1er, alinéa 1er, L.R&S) ;
12. Mettre fin partiellement à une méthode autorisée. Il est question ici, par exemple, d'une situation où une méthode est limitée dans le temps, pas d'une situation où une seule autorisation d'un dirigeant du service autorise plusieurs méthodes et où le Comité ne met fin qu'à une seule d'entre elles ;
13. Lever totalement ou partiellement la suspension et l'interdiction qui ont été décidées par la Commission BIM (art. 43/6 § 1er, alinéa 1er, L.R&S), ce qui implique que la méthode autorisée par le dirigeant du service a bien été considérée par le Comité comme (partiellement) légale, proportionnelle et subsidiaire ;
14. Constater l'incompétence du Comité permanent R ;
15. Déclarer le caractère infondé de l'affaire pendante et permettre la poursuite de la méthode ;
16. Délivrer un avis préjudiciel (articles 131*bis*, 189*quater* en 279*bis* CIC).

Le Comité permanent R doit statuer définitivement dans un délai d'un mois suivant la date à laquelle il a été saisi (art. 43/4 L.R&S). Ce délai a été respecté dans tous les dossiers.

NATURE DE LA DÉCISION	2011	DÉCISION FINALE 2011	2012	DÉCISION FINALE 2012	2013	DÉCISION FINALE 2013
1. Plainte frappée de nullité	0		0		0	
2. Plainte manifestement non fondée	1		0		0	
3. Suspension de la méthode	3		1		0	
4. Information complémentaire de la Commission BIM	4		0		0	
5. Information complémentaire du service de renseignement	9		6		**0**	
6. Mission d'enquête du Service d'Enquêtes R	17		11		50	
7. Audition membres de la Commission BIM	0		0		0	
8. Audition membres des services de renseignement	1		0		0	
9. Décision relative au secret de l'instruction	0		0		0	
10. Informations sensibles lors de l'audition	0		0		0	
11. Cessation de la méthode	12		4		9	
12. Cessation partielle de la méthode	7		18		5	
13. Levée (partielle) de l'interdiction de la Commission BIM	5	**39**	13	**38**	2[148]	**23**
14. Incompétence	0		0		0	
15. Autorisation légale/ Non- cessation de la méthode/Non-fondement	15		3		7	
16. Avis préjudiciel	0		0		0	

148 En fait, le Comité a décidé que la suspension prononcée par la Commission BIM était sans objet (voir dossier 2013/1728).

III.3.2. LA JURISPRUDENCE

La substance des 23 décisions finales prises par le Comité permanent R en 2013 est reprise ci-après. Les synthèses sont expurgées des données opérationnelles. Seuls sont mentionnés les éléments qui présentent un intérêt d'un point de vue juridique.[149]

Les décisions ont été regroupées en cinq rubriques :

- Les exigences légales (de forme) préalables à la mise en œuvre d'une méthode ;
- La motivation de l'autorisation ;
- Les exigences de proportionnalité et de subsidiarité ;
- La légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace ;
- Les conséquences d'une méthode (mise en œuvre) illégale(ment).

Certaines décisions ont été reprises dans plusieurs rubriques lorsque cela s'avérait pertinent.

III.3.2.1. Exigences légales (de forme) préalables à la mise en œuvre d'une méthode

Aucune méthode particulière ne peut être utilisée sans l'autorisation écrite préalable du dirigeant du service. Pour les méthodes exceptionnelles, il convient en outre de présenter un projet d'autorisation et un avis conforme de la Commission BIM. Si des méthodes sont mises en œuvre sans l'autorisation écrite ou l'avis conforme, le Comité peut naturellement intervenir.

III.3.2.1.1. Aucune compétence pour le service de renseignement

Un service de renseignement voulait procéder au repérage des appels entrants et sortants d'un numéro de GSM donné (dossier 2013/1835). En effet, une autre méthode MRD avait fortuitement révélé que la cible était peut-être impliquée dans un trafic ou une escroquerie à l'échelle internationale. Le service voulait en avoir la certitude. Il souhaitait également vérifier si les autorités étrangères, dont la cible faisait partie, étaient également impliquées dans cette affaire. Dans la description de la menace, le service a uniquement fait mention du « *schade aangericht door criminele organisaties en het clandestien karakter van de beschreven zwendel die ten minste een potentiële bedreiging vormen voor de economische belangen van België* ».[150] Le Comité a toutefois remarqué que la

[149] Toutes les décisions du Comité en cette matière sont revêtues de la mention « diffusion restreinte ». Une décision a été classifiée au niveau « confidentiel » et une au niveau « secret ».

[150] « *dommage causé par des organisations criminelles et [du] caractère clandestin de l'escroquerie décrite qui représentent au moins une menace potentielle pour les intérêts économiques de la Belgique* » (traduction libre)

compétence de suivi des organisations criminelles se limite aux organisations « *qui se rapportent intrinsèquement aux activités d'espionnage, de terrorisme, d'extrémisme, de prolifération, d'organisations sectaires nuisibles et d'ingérence* » (art. 8, 1°, f L.R&S). Comme ce point n'a pas été suffisamment rendu plausible dans l'autorisation, la méthode a été considérée comme illégale.

III.3.2.1.2. Autorisation donnée par le ministre compétent

Comme l'an dernier[151], le service de renseignement a saisi son ministre à deux reprises en vertu de l'article 18/10 § 3, alinéa 3, L.R&S, parce que la Commission BIM ne pouvait pas valablement se réunir en raison de la période de vacances (dossiers 2013/2327 et 2013/2328). L'article de loi permet au service de renseignement de demander à son ministre d'autoriser la méthode si la commission ne rend pas d'avis dans un délai de quatre jours après réception du projet d'autorisation. Le Comité avait déjà décidé que, vu les circonstances concrètes et vu la nécessité pour le service de pouvoir continuer à remplir ses missions légales, il n'avait aucune objection à ce que le ministre soit immédiatement saisi. Dans les deux nouveaux dossiers, le ministre avait signé (mais pas daté) le projet d'autorisation. En outre, il n'était pas non plus mentionné à quel moment le dirigeant du service avait dû rendre compte du déroulement de la méthode et le ministre a omis de communiquer la décision au Comité. Ces deux obligations figurent pourtant à l'article 18/10 § 3, alinéas 3 et 4, L.R&S. Le Comité a néanmoins estimé que la méthode était valable. Il a réitéré que, vu les circonstances et vu la nécessité pour le service de renseignement de remplir correctement ses missions légales, il n'avait aucune objection à un recours à l'article 18/10 § 3, alinéa 3, L.R&S. De surcroît, le Comité a souligné que cette disposition requiert simplement l'autorisation du ministre compétent sans imposer d'autres obligations que celles prévues à l'article 18/10 § 1er L.R&S. Le Comité a ajouté que « *niet-bestaan van dergelijke vermelding de wettigheid van de beslissing niet aantast, noch afbreuk doet aan de toelating van de Minister* ».[152]

III.3.2.1.3. Méthode non couverte par l'autorisation (requise)

Lorsqu'une observation à l'aide d'un moyen technique a été prolongée pour la deuxième fois, le Comité a remarqué que cette prolongation avait été demandée par erreur sept jours trop tard (dossier 2013/2653). En d'autres termes, la caméra a continué à enregistrer pendant cette courte période sans l'autorisation requise. Le service de renseignement est parti du principe que le Comité ne devait pas

151 COMITÉ PERMANENT R, *Rapport d'activités 2012*, 56.

152 « *l'absence d'une telle mention [c'est-à-dire le délai dans lequel le dirigeant du service doit faire rapport, ndr] n'affecte pas la légalité de la décision et ne porte pas préjudice à l'autorisation du ministre* » (traduction libre)

intervenir étant donné qu'il ne stockerait pas les images enregistrées dans ses fichiers et ne pourrait donc pas les exploiter. Le Comité a toutefois affirmé que la décision du service de ne pas stocker les images « *ne peut avoir pour effet de priver le Comité des prérogatives que la loi lui a octroyées quant au sort à réserver aux données qui ont été recueillies et enregistrées sans une autorisation légale* ». Les images devaient dès lors être détruites.

La même situation s'est présentée dans un autre dossier : entre la deuxième et la troisième prolongation de la méthode, la caméra a continué à filmer pendant 25 jours sans l'autorisation requise (dossier 2013/2663). Dans ce cas-ci non plus, le Comité n'a pu accéder à la requête de ne pas détruire les données parce qu'elles ne pouvaient être/ne seraient pas exploitées. Le Comité a également insisté sur le fait que « *la mise en œuvre illégale d'une méthode visée par l'article 18/17 L. R&S est susceptible de constituer une infraction visée à l'article 259bis du Code pénal.* »

Dans un troisième dossier (2013/1760), le responsable du service de renseignement concerné a décidé d'effectuer une courte observation à l'aide d'une caméra, sur la porte d'accès d'une salle accessible au public où un événement donné allait se dérouler. Le service de renseignement estimait qu'il s'agissait d'une méthode spécifique. Cependant, il est ressorti des informations complémentaires recueillies par la Commission BIM que la porte d'accès « *est séparée de la voie publique par une bande de terrain pourvue d'une grille pouvant être fermée, et qu'elle est par conséquent située dans un lieu privé qui n'est pas accessible au public.* » En d'autres termes, il s'agissait d'une méthode exceptionnelle pour laquelle la procédure requise n'a pas été suivie. Le Comité s'est dès lors rangé à l'avis de la Commission BIM et a déclaré la méthode illégale.

III.3.2.2. Motivation de l'autorisation

En 2013, le Comité a trouvé cinq décisions qui indiquaient un manque de motivation (suffisante ou cohérente) de l'autorisation.

Un service de renseignement souhaitait procéder au repérage, à l'identification et à la localisation des données d'appel de trois appareils (dossier 2013/2618). Mais seule la localisation d'un appareil était explicitement motivée dans l'autorisation. Le service de renseignement a mentionné à la Commission BIM, comme suite à sa demande, que l'objectif consistait uniquement à localiser un des trois appareils. La mention de la localisation des trois appareils tant dans l'autorisation elle-même que dans la réquisition remise à l'opérateur aurait constitué une erreur administrative. La Commission BIM a dès lors décrété une suspension partielle. Le Comité, qui a été « *saisi d'office de l'ensemble de la décision* », ne partageait cependant pas cet avis. En effet, il était impossible de déterminer s'il s'agissait réellement d'une erreur administrative. Aussi la demande de localisation des deux numéros pour

lesquels aucune motivation n'avait été indiquée a-t-elle été considérée comme illégale.

Dans un autre dossier (2013/1912), le service de renseignement souhaitait identifier le titulaire d'un numéro de GSM. Il serait très régulièrement en contact avec un membre actif d'une organisation extrémiste étrangère donnée, qui serait notamment dirigée contre l'OTAN. Mais, selon le Comité, « *l'examen des pièces ne fait pas apparaître que la condition de légalité de la méthode ainsi que les principes de subsidiarité et de proportionnalité, comme déterminés dans l'article 18/3, § 1 premier alinéa de la L. R&S, ont été respectés.* » En effet, la menace qui émanerait de l'organisation n'a été précisée par aucun élément concret dans la décision. Le Comité s'est saisi de l'affaire afin d'obtenir de plus amples informations. Il souhaitait en savoir plus sur « *le caractère potentiellement menaçant de la cible de la méthode spécifique concernée* » et « *le degré de priorité qu'occupe la (les) problématique(s) […] dans son Plan d'action.* » Comme le service concerné a pu fournir des réponses concrètes aux deux questions, le Comité a estimé que la méthode autorisée était légale, proportionnelle et subsidiaire.

Un service de renseignement voulait savoir, au moyen d'une observation, qui participerait à une réunion au cours de laquelle il était probable qu'une nouvelle initiative politique et un nouveau régime dans un pays donné soient discutés (dossier 2013/2420). On s'attendait également à la présence de membres du service de renseignement étranger concerné. Dans son autorisation, le service affirmait que les intérêts suivants étaient menacés : « *de uitwendige veiligheid van de Staat en de internationale betrekkingen, spionage, inmenging* ».[153] La motivation de la gravité des menaces se limitait à ce qui suit : « *een reële mogelijkheid [dat] inlichtingenofficieren clandestiene activiteiten ontplooien op Belgisch grondgebied* ».[154] Le Comité a estimé que « *Considérant qu'à défaut de constituer une mission en soi [du service de renseignement], la surveillance des activités que déploient les services de renseignement étrangers sur le territoire national ne se justifie que par une menace concrète pour la sûreté de l'État belge et ses relations internationales* ». Étant donné que les informations complémentaires ne révélaient pas en quoi ces éventuelles activités clandestines pouvaient représenter une menace pour la sûreté de l'État et les relations internationales, la méthode n'était pas légale.

Dans le dernier dossier, le Comité a estimé que la méthode ne pouvait pas être autorisée parce que « *la motivation de la méthode est incohérente d'une part et insuffisante d'autre part et ne permet pas au Comité d'en apprécier la légalité* » (dossier 2013/2447). Le service de renseignement avait projeté de procéder à une

153 « *la sûreté extérieure de l'Etat et les relations internationales, l'espionnage et l'ingérence* » (traduction libre)

154 « *une possibilité réelle que des officiers de renseignement déploient des activités clandestines sur le territoire belge* » (traduction libre)

observation avec des *« bewakingscamera's gericht op niet-besloten en voor het publiek toegankelijke besloten plaatsen, zoals luchthavens of treinstations »*.[155] À cette fin, le service se référait à l'article 18/4 L.R&S, qui prévoit l'observation à l'aide de moyens techniques dans des lieux publics ou des lieux privés accessibles au public. Il est toutefois ressorti de la motivation de la décision que l'objectif était de vérifier quelles personnes résidaient ou visitaient une habitation dont le propriétaire était à l'époque privé de liberté. Comme le logement faisait partie d'un complexe d'habitations, le Comité a demandé des explications complémentaires sur le déroulement concret de l'observation. Il est alors clairement apparu que l'objectif n'était absolument pas d'observer des lieux tels que des gares et aéroports. *« Les renseignements fournis au Comité, suite à sa demande, vont au-delà d'une simple explication complémentaire, mais révèlent l'objectif réel de la méthode »*. La méthode incriminée avait plus précisément pour but de préparer une autre méthode (à savoir l'observation des personnes qui avaient accès à l'habitation).

III.3.2.3. Les exigences de proportionnalité et de subsidiarité

L'exigence de proportionnalité et/ou de subsidiarité a été déterminante dans six décisions.

Dans deux dossiers (qui portaient sur une même opération), un service de renseignement souhaitait procéder au repérage et à l'identification des données d'appel de numéros de téléphone de quatre personnes (dossier 2013/2067) et en même temps à leur localisation (dossier 2013/2068). Mais les numéros n'étaient pas encore connus à ce moment-là ; ils seraient obtenus par le biais d'une autre méthode. Le Comité a affirmé qu'*« en l'absence d'informations obtenues par cette première méthode, il n'est pas permis de juger du respect des principes de subsidiarité et de proportionnalité et donc de la légalité de la présente méthode »*. Le Comité a dès lors ordonné la cessation de la méthode.

Le Comité est arrivé à la même conclusion dans un dossier ultérieur (2013/2337). Le service de renseignement concerné souhaitait mettre sur écoute plusieurs numéros de GSM, mais certains de ces numéros n'étaient pas encore connus au moment de l'autorisation. En effet, le service souhaitait aussi écouter plusieurs numéros qui étaient liés ou étaient susceptibles d'être liés à un GSM bien déterminé et connu. Or, pour connaître le nombre exact de numéros et savoir de quels numéros il s'agissait précisément, il fallait d'abord mettre en œuvre la méthode. Comme la méthode portait *« sur un nombre indéterminé de numéros de GSM ; qu'en l'absence d'informations sur le nombre de ces numéros et sur les numéros eux-mêmes qui devraient être écoutés »*, il était impossible d'en

155 *« caméras de surveillance orientées sur des lieux ouverts et des lieux fermés accessibles au public, comme des aéroports ou des gares ferroviaires »* (traduction libre)

évaluer la subsidiarité ou la proportionnalité. Par conséquent, il a été mis fin à la méthode pour ce qui concerne les numéros inconnus.

Lorsqu'un service de renseignement a souhaité procéder au repérage des données d'appel du GSM d'une personne donnée et obtenir dans le même temps les données de localisation (dossier 2013/2417), la Commission BIM a suspendu les méthodes : « *Men beschikt evenwel over geen verdere informatie over deze [persoon]. Zijn profiel en zijn activiteiten blijken moeilijk te evalueren… Ook wordt in de beslissing niet aannemelijk gemaakt dat er een effectieve bedreiging van deze persoon zou uitgaan* ».[156] Dans son autorisation, le service de renseignement avait mentionné plusieurs considérations relatives à la personne elle-même, ainsi qu'à plusieurs autres aspects généraux de nature géopolitique. Le Comité a demandé des informations complémentaires au service. Il en est ressorti une certaine contradiction entre les déclarations qu'avait faites la personne à une autorité belge et ses activités. « *Attendu que ce comportement étrange et ambigu permet de le considérer comme constituant une menace potentielle pour la sécurité intérieure et extérieure du pays* ». Mais le Comité a d'autre part affirmé qu'« *en l'absence de renseignements plus précis sur ses activités effectives, la demande de données de localisation apparait à ce stade disproportionnée.* » Aussi la première méthode (repérage des données d'appel) a-t-elle été déclarée légale, tandis que la seconde méthode (localisation) a été invalidée.

En appui à une filature, le service de renseignement souhaitait pouvoir filmer pendant les observations sur une période d'un an (dossier 2013/2446). Le Comité s'est interrogé sur la durée de cette méthode spécifique. Le Comité avait déjà honoré des autorisations portant sur l'utilisation de caméra pendant une année, mais il s'agissait alors d'une caméra fixe qui était par exemple dirigée vers une entrée située sur la voie publique. Or, il s'agissait ici d'une filature. « *Attendu que même si la filature est une mesure ordinaire, non susceptible de contrôle juridictionnel par le Comité permanent R, l'utilisation d'une méthode spécifique pendant une période d'un an doit être justifiée, eu égard aux principes de légalité en ce compris les principes de proportionnalité et de subsidiarité; Attendu que la seule explication fournie quant à la durée, dans ce cas précis, est que pour des raisons pratiques, sur le plan opérationnel, une période longue permet la planification de filatures (et donc des observations au moyen d'une caméra) en tenant compte d'autres opérations de filatures en cours ou à venir* ». Le Comité a estimé qu'une telle motivation ne répondait pas aux principes de proportionnalité et de subsidiarité et que l'observation accessoire à la filature devait se limiter à un délai raisonnable de quatre mois.

156 « *On ne dispose toutefois d'aucune information complémentaire sur cette [personne]. Son profil et ses activités semblent difficiles à évaluer… En outre, la décision n'a pas rendu crédible le fait que cette personne représenterait une menace effective.* » (traduction libre)

Dans le dernier dossier (2013/2662), un service de renseignement souhaitait procéder à l'observation, à l'aide de moyens techniques, de plusieurs membres d'une certaine organisation étrangère qui était active en Belgique. L'observation devait durer un an. Le service ne souhaitait pas seulement observer les collaborateurs qui séjournaient en Belgique, mais aussi les personnes qui venaient de temps à autre en Belgique et qui faisaient partie de l'entourage direct du mouvement. Cette méthode avait pour objectif d'« *identifier les contacts et activités des membres influents de* [mouvement surveillé] *présents en Belgique.* » Selon cette formulation, les personnes qui ne séjournaient pas en Belgique n'étaient pas couvertes par l'autorisation. De plus, il n'était pas clairement indiqué si les personnes faisant partie de l'entourage direct étaient aussi des personnes influentes. Il s'est également avéré que la méthode n'était pas encore mise en œuvre, alors qu'elle pouvait l'être depuis environ un an, selon l'autorisation du dirigeant du service. Le Comité a finalement estimé que l'autorisation d'observer pendant une année les personnes qui avaient parfois séjourné en Belgique n'était pas proportionnelle. En ce qui les concerne, la durée de l'autorisation devait se limiter au temps qu'elles passaient en Belgique.

III.3.2.4. Légalité de la méthode concernant les techniques utilisées, les données recueillies, la durée de la mesure et la nature de la menace

III.3.2.4.1. Le contrôle de l'exécution de la méthode MRD

La Loi du 30 novembre 1998 stipule que seul un agent de renseignement belge tel que décrit à l'article 3, 2° L.R&S peut effectivement mettre en œuvre une méthode spécifique ou exceptionnelle. Cependant, l'article 13/1 § 2, alinéa 5 L.R&S prévoit la possibilité de solliciter l'aide ou l'assistance d'autres personnes. Tant qu'un ou plusieurs agents de renseignement belges « *gardent le contrôle direct de la méthode* », il n'y a pas le moindre problème. Ce critère a été concrètement évalué à deux reprises par le Comité.

Dans le premier dossier (2013/1950), le service souhaitait procéder à une observation dans un lieu privé. La méthode serait mise en œuvre par un agent d'un service de renseignement étranger et par un particulier. Comme le service « *n'a pas le contrôle direct de cette méthode comme voulu par le législateur* », il a été mis fin à la méthode.[157]

Le second dossier (2013/2226) était différent à cet égard. Le service de renseignement a sollicité l'aide de trois agents de renseignement étrangers afin de procéder à l'enlèvement d'un dispositif dans un véhicule. Cet appareil avait été placé par le biais d'une méthode antérieure. La méthode était légale puisque les

[157] En outre, le service avait omis d'examiner si le lieu où se déroulerait l'observation était soumis à un statut juridique particulier en vertu du droit international.

agents étrangers, forts de leur expérience technique, ont uniquement prêté assistance et que les agents belges ont conservé le contrôle direct.

III.3.2.4.2. La suspension d'une méthode à laquelle il avait été mis fin

Le dossier 2013/1728 a soulevé une autre problématique. Le jour même de l'autorisation d'une mesure d'écoute, le dirigeant du service de renseignement concerné a décidé de mettre fin à la mesure. Il s'est effectivement avéré que le numéro de GSM que l'on souhaitait mettre sur écoute n'appartenait pas à la cible. La Commission BIM a dès lors suspendu la méthode concernée et a ordonné son arrêt. Le Comité a toutefois estimé que « *la constatation du fait que l'un des numéros de GSM interceptés n'est pas utilisé par la cible de la méthode concernée n'est pas de nature, en soi, à rendre illégale ladite méthode, celle-ci ayant été décidée et exécutée en parfaite conformité avec la loi* ». Le dirigeant du service a correctement réagi en mettant fin à la méthode dès l'instant où elle n'était plus utile à la finalité initiale, et ce conformément aux dispositions de l'article 18/10 L.R&S. Le Comité a estimé que la compétence de la Commission BIM de suspendre ou d'arrêter une méthode (art. 18/10, § 6 L.R&S) n'avait de sens que si le dirigeant du service avait omis de mettre fin à la mesure. Pour le Comité, la décision de la commission était donc sans objet.

III.3.2.4.3. Le statut d'avocat

Dans trois dossiers (2013/2518, 2013/2519 et 2013/2536), un service de renseignement a décidé de recourir à une méthode exceptionnelle à l'égard d'un avocat qui opère en cette qualité dans un pays hors UE, mais qui était présent en Belgique lors de la mise en œuvre des méthodes. Le Comité s'est demandé si l'intéressé pouvait bénéficier de la protection des articles 2 § 2[158] et 18/2 § 3 L.R&S.[159] S'appuyant sur les articles 428 et 428*bis* du Code

158 « *Il est interdit aux services de renseignement et de sécurité d'obtenir, d'analyser ou d'exploiter des données protégées par le secret professionnel d'un avocat ou d'un médecin ou par le secret des sources d'un journaliste.*
À titre exceptionnel et lorsque le service en question dispose au préalable d'indices sérieux révélant que l'avocat, le médecin ou le journaliste participe ou a participé personnellement et activement à la naissance ou au développement de la menace potentielle, au sens des articles 7, 1°, 8, 1° à 4°, et 11, il est permis d'obtenir, d'analyser ou d'exploiter ces données protégées. »

159 « *Si une méthode visée aux §§ 1er et 2 est mise en œuvre à l'égard d'un avocat, d'un médecin ou d'un journaliste, ou de leurs locaux ou de moyens de communication qu'ils utilisent à des fins professionnelles, ou de leur résidence, ou de leur domicile, cette méthode ne peut être exécutée sans que, suivant le cas, le président de l'Ordre des barreaux francophone et germanophone ou le président de l'Orde van de Vlaamse balies, le président du Conseil national de l'Ordre des médecins ou le président de l'Association des journalistes professionnels, en soit averti au préalable par le président de la commission visée à l'article 3, 6°. Le président de la commission est tenu de fournir les informations nécessaires au président de l'Ordre ou de l'association des journalistes professionnels dont fait partie l'avocat, le médecin ou le journaliste. Le président*

judiciaire[160], le Comité a affirmé que la protection ne peut pas s'appliquer à l'intéressé qui « *het beroep van advocaat in België niet kan uitvoeren, noch de titel van advocaat dragen* ».[161]

III.3.2.4.4. La durée d'une méthode exceptionnelle

La Commission BIM a rendu un avis conforme pour l'inspection de bagages dans un lieu privé qui n'est pas accessible au public (dossier 2013/2520). Elle a toutefois émis une réserve : l'autorisation ne pouvait durer plus de cinq jours, et non deux mois comme mentionné dans le projet d'autorisation. Ce seuil est prévu à l'article 18/12 § 1er L.R&S. Pourtant, cet élément n'a pas été pris en compte dans l'autorisation, qui était valable pour deux mois. La Commission BIM a dès lors procédé à la suspension partielle. Le Comité a confirmé la décision de la Commission BIM.

III.3.2.4.5. Les conséquences d'une méthode (mise en œuvre) illégale(ment)

Dans le dossier 2013/1728, le Comité a décidé que la mesure d'écoute d'un GSM qui n'appartenait pas à la cible était légale (voir III.3.2.4.2). Toutefois, il était clair que l'objectif n'était pas de recueillir ces données. Le Comité a néanmoins estimé qu'il « *n'est pas compétent pour apprécier l'utilité pour un service de renseignement de conserver ou non des données recueillies au moyen d'une méthode exceptionnelle légalement mise en œuvre ; que ce pouvoir d'appréciation appartient au service de renseignement lui-même en vertu de l'art. 13 L. R&S et de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel* ».

Dans le dossier 2013/1835, le repérage de la communication d'un numéro de GSM donné a été considéré comme illégal (voir II.3.2.1.1). Le Comité a ordonné la cessation de cette méthode pour autant qu'elle fût toujours mise en œuvre. Il a également estimé que « *de gegevens, verkregen en gebeurlijk nog te verkrijgen ingevolge de onwettig bevonden methoden* »[162] ne pouvaient pas être exploitées et devaient être détruites.

---

concerné est tenu au secret. Les peines prévues à l'article 458 du Code pénal s'appliquent aux infractions à cette obligation de garder le secret. »

160 *Art. 428. « Nul ne peut porter le titre d'avocat ni en exercer la profession s'il n'est Belge ou ressortissant d'un état membre de l'Union européenne, porteur du diplôme de docteur ou de licencié en droit, s'il n'a prêté le serment visé à l'article 429 et s'il n'est inscrit au tableau de l'Ordre ou sur la liste des stagiaires. Il peut être dérogé à la condition de nationalité dans les cas déterminés par le Roi, sur l'avis de l'Ordre des barreaux francophone et germanophone et de l'Orde van Vlaamse balies. Sauf les dérogations prévues par la loi, aucune qualification complémentaire ne peut être ajoutée au titre d'avocat.* »

161 « *ne peut pas exercer la profession d'avocat en Belgique et ne peut porter le titre d'avocat* » (traduction libre)

162 « *les données obtenues et éventuellement à obtenir en vertu de cette méthode jugée illégale* » (traduction libre)

Dans le dossier 2013/2446, où la méthode a été jugée disproportionnelle (voir II.3.2.3), le Comité a affirmé que l'observation demandée, qui était accessoire à la filature, devait se limiter à un délai raisonnable de quatre mois et *« que la méthode est illégale pour la période de temps au-delà des 4 mois »*.

Quand, dans son autorisation, le service de renseignement n'a pas tenu compte du fait qu'une méthode exceptionnelle donnée ne pouvait être mise en œuvre que pendant cinq jours (dossier 2013/2520 – voir aussi II.3.2.4.4), le Comité a constaté l'illégalité de la méthode *« DOCH SLECHTS voor zover zij zou zijn uitgevoerd NA het verstrijken van een periode van vijf dagen, te rekenen vanaf de machtiging van het diensthoofd »*.[163] En d'autres termes, seules *« de gegevens, verkregen en gebeurlijk nog te verkrijgen op basis van het onwettig bevonden gedeelte van de methode, […] mogen [niet] worden geëxploiteerd en moeten worden vernietigd »*.[164]

Dans le dernier dossier (2013/2662 – voir aussi II.3.2.3), un service de renseignement souhaitait procéder à l'observation, à l'aide de moyens techniques, de plusieurs membres d'une certaine organisation étrangère qui était active en Belgique. L'observation devait durer un an. Le Comité a estimé que la méthode n'était pas proportionnelle à l'égard des cibles qui ne se trouvaient que sporadiquement en Belgique et *« qu'il conviendrait dès lors de limiter leur observation à la durée de leur séjour en Belgique et d'utiliser la procédure d'urgence si nécessaire […] Déclare la méthode illégale en ce qu'elle concerne les « anciens responsables » qui ne résident plus en Belgique mais qui reviennent « parfois » [et] les personnes faisant « partie de l'entourage direct » du mouvement ciblé; La méthode n'ayant pas encore été mise en œuvre, il n'y a pas lieu d'en ordonner la cessation ni la destruction des données recueillies sur ces dernières personnes. »*

III.4. CONCLUSIONS

En ce qui concerne l'année d'activités 2013, le Comité tire les conclusions suivantes :

- En comparaison avec 2011 et 2012, le nombre de méthodes mises en œuvre a augmenté. Cependant, on ne peut pas vraiment parler d'une utilisation « débridée » de méthodes particulières.
- Cette augmentation tient en grande partie au fait que le nombre d'observations et de localisations effectuées par la VSSE s'est considérablement accru.

163 *« MAIS SEULEMENT pour autant qu'elle ait été exécutée APRÈS la fin d'une période de cinq jours, à partir de l'autorisation du dirigeant du service »* (traduction libre)

164 *« les données obtenues et éventuellement à obtenir sur la base de la partie jugée illégale de la méthode […] [ne] peuvent [pas] être exploitées et doivent être détruites »* (traduction libre)

- Pour la troisième année consécutive, il convient de noter un accroissement du nombre de mesures d'écoutes autorisées.
- Il ressort de l'enquête sur les résultats obtenus qu'une cible déterminée peut faire l'objet de très nombreuses méthodes.
- Pour le SGRS, la lutte contre l' « espionnage » continue de mobiliser la plupart des méthodes particulières. La VSSE a elle aussi accordé davantage d'attention à cette menace (du moins en ce qui concerne les MRD). D'autre part, les deux services se sont vu accorder moins d'autorisations dans le cadre de la lutte contre le terrorisme.
- 12 méthodes spécifiques et exceptionnelles ont été mises en œuvre à l'égard d'un avocat, médecin ou journaliste professionnel, contre 24 encore l'année précédente. Étant donné que plusieurs méthodes MRD peuvent être appliquées à une seule personne, ce chiffre ne révèle rien sur le nombre de praticiens professionnels qui ont fait l'objet d'une méthode MRD.
- En 2013, le Comité permanent R a été saisi à 23 reprises, contre 38 l'année précédente. Cette diminution s'explique par le nombre moins élevé de suspensions prononcées par la Commission BIM.

CHAPITRE IV
LE CONTRÔLE DE L'INTERCEPTION DE COMMUNICATIONS ÉMISES À L'ÉTRANGER

Depuis le début de l'année 2011, la VSSE et le SGRS peuvent tous deux, dans des conditions très strictes, écouter des communications, en prendre connaissance et les enregistrer (art. 18/17, § 1er L.R&S).

Il convient toutefois d'établir une distinction claire entre les « interceptions MRD » et « *la recherche, la captation, l'écoute, la prise de connaissance ou l'enregistrement, par le Service Général du Renseignement et de la Sécurité des Forces armées de toute forme de communications émises à l'étranger.* » Cette forme d'écoute est possible depuis longtemps déjà et peut être mise en œuvre tant à des fins militaires dans le cadre des missions définies à l'article 11 § 2, 1° et 2°, L.R&S, que pour des motifs de sécurité et de protection des troupes belges et alliées lors de missions à l'étranger ainsi que des ressortissants belges établis à l'étranger (art. 11, § 2, 3° et 4°, L.R&S). Ces écoutes sont elles aussi généralement désignées par l'appellation « interceptions de sécurité », mais elles sont soumises à un tout autre cadre de contrôle. Ce contrôle externe est en effet exclusivement confié au Comité permanent R, et ce à la fois avant, pendant et après les interceptions (art. 44*bis* L.R&S). Le Comité est chargé de faire cesser les interceptions en cours lorsqu'il apparaît que les conditions dans lesquelles elles sont réalisées ne respectent pas les dispositions légales et/ou l'autorisation ministérielle (art. 44*ter* L.R&S). Chaque année, au début du mois de décembre, le SGRS doit en effet présenter au ministre de la Défense sa liste motivée d'organisations ou d'institutions dont les communications pourront faire l'objet d'interceptions dans le courant de l'année suivante, et ce dans le but d'octroyer à ces interceptions l'autorisation ministérielle. Le ministre doit prendre sa décision dans les dix jours ouvrables et la communiquer au SGRS. Ensuite, le SGRS est tenu de transmettre la liste et l'autorisation ministérielle au Comité permanent R.

En 2013, le Comité permanent R a effectué les vérifications requises par le législateur. En outre, un courrier circonstancié a été adressé au SGRS à la fin décembre 2013, et ce en rapport avec le Plan d'écoutes pour l'année d'activités 2014. Dans ce courrier, le Comité a demandé des éclaircissements sur les limites

tant de l'art. 259*bis* § 5 du Code pénal que de l'art. 44*bis* L.R&S à l'interception de communications à l'étranger. Les questions concernaient notamment les choix et la description des « organisations ou institutions » qui feraient l'objet d'interceptions et la motivation de celles-ci, et ce sur la base des missions légales du service de renseignement militaire, telles que décrites à l'article 11 L.R&S. Le Comité permanent R a reçu, en mars 2014, une réponse détaillée qui a été analysée en vue d'un éventuel examen ultérieur.

CHAPITRE V
AVIS, ÉTUDES ET AUTRES ACTIVITÉS

V.1. VINGT ANS DE CONTRÔLE DÉMOCRATIQUE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ

En 2013, le Comité permanent R a fêté ses vingt années d'existence. À l'occasion de cet anniversaire, le Comité a édité un recueil et organisé une séance académique.

Pour l'édition du 20ème anniversaire, intitulée *« Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement »*[165], pas moins de 38 représentants du milieu académique, du monde politique et des experts belges et étrangers ont accepté de prendre la plume pour évoquer le contrôle des services de renseignement, chacun selon son expérience, son expertise et ses centres d'intérêt. Tous les thèmes traités ont été réunis dans cinq chapitres : (1) Le contrôle démocratique sur les services de renseignement de 1830 à 2013 ; (2) Le contrôle sur les services de renseignement dans un cadre élargi ; (3) Le Comité permanent R sous le feu des projecteurs ; (4) Le Comité permanent R et ses relations avec les services contrôlés et les quatre pouvoirs ; et (5) L'herbe (n')est (pas toujours) plus verte ailleurs (où plusieurs auteurs étrangers portent un regard sur le système de contrôle belge). C'est le professeur émérite Cyrille Fijnaut qui a rédigé l'épilogue de cet ouvrage.

Ce livre a été présenté au Parlement fédéral le 24 mai 2013 lors d'une séance solennelle, en présence de plusieurs représentants des plus hautes instances du pays, de la communauté du renseignement, des médias, du monde académique et de quelques organes de contrôle étrangers.

V.2. DOSSIERS D'INFORMATION

Outre les enquêtes de contrôle (voir Chapitre II), le Comité permanent R ouvre également des « dossiers d'information » qui doivent permettre d'apporter une

165 W. VAN LAETHEM et J. VANDERBORGHT (eds.), *Regards sur le contrôle. Vingt ans de contrôle démocratique sur les services de renseignement*, Intersentia, Anvers, 2013, 565 p.

réponse structurée à des questions relatives au fonctionnement des services de renseignement et de l'OCAM.[166] Si de tels dossiers révèlent des indices de dysfonctionnement ou des aspects du fonctionnement des services de renseignement qui requièrent un examen approfondi, le Comité peut procéder à l'ouverture d'une enquête de contrôle. En revanche, s'il apparaît clairement qu'une telle enquête n'apporterait aucune plus-value au regard des objectifs du Comité permanent R, le dossier d'information est clôturé.

En 2013, le Comité a par exemple ouvert des dossiers d'information sur la problématique relative au respect de la législation en matière de classification lors de l'envoi de documents, sur l'intention de centraliser certains services (extérieurs) du SGRS, et sur les éventuelles activités de renseignement du Bataillon ISTAR récemment mis sur pied au sein des Forces armées. En ce qui concerne ISTAR, la Commission de suivi du Sénat a été informée du point de vue juridique du Comité.

V.3. EXPERT DANS DIVERS FORUMS

En 2013, des représentants du Comité permanent R ont été sollicités à plusieurs reprises en tant qu'experts par des institutions publiques et privées tant belges qu'étrangères.

C'est ainsi que le président du Comité a été invité, le 20 février 2013, à la Commission de l'Intérieur, où se tenaient des auditions relatives à la loi du 19 juillet 1991 organisant la profession de détective privé. Le président a expliqué la position du Comité quant à la question du rôle que l'organe de contrôle peut jouer dans le contrôle du secteur du renseignement privé.[167]

Le président a également été entendu par la Commission de l'Intérieur et des Affaires administratives du Sénat le 18 juin 2013. Une proposition de résolution avait été déposée au Sénat, visant l'élaboration rapide d'une stratégie fédérale en matière de protection des systèmes d'information et de communication.[168] Cette proposition a trouvé son origine dans les constatations et conclusions de l'enquête de contrôle que le Comité a menée concernant l'attitude des services de renseignement belges quant à la nécessité de protéger les systèmes de communication contre des interceptions et cyberattaques étrangères. Ces auditions se situaient dans ce contexte.

---

166 Le Comité permanent R peut ouvrir un dossier d'information pour des raisons très diverses : une plainte a été déposée et le Comité permanent R souhaite exclure le plus rapidement possible l'absence manifeste de fondement ; la direction d'un service de renseignement fait état d'un incident et le Comité souhaite contrôler comment cet incident a été traité ; les médias signalent un événement et le Comité souhaite déterminer si ces faits sont conformes à la réalité et s'ils relèvent d'une problématique plus générale…

167 *Doc. parl.* Chambre 2012-13, 53-2711/001, 7-9.

168 *Doc. parl.* Sénat 2010-11, 4 octobre 2011, n° 5-1246/1 et *Doc. parl.* Sénat 2012-13, 28 novembre 2012, n° 5-1855/1.

Début juin 2013, un représentant du Comité permanent R a participé à la table ronde organisée à Tunis par le *Democratic Centre of Armed Forces* (DCAF) à propos de « La transition démocratique et la réforme des services de renseignement ».[169] En mettant son expertise à disposition dans de tels forums, le Comité tente de contribuer au processus de démocratisation de certains pays. Cette réunion a donné lieu à la création d'un groupe de travail interministériel dirigé par le Premier ministre, en vue d'aboutir à de nouvelles réglementations légales pour les services de renseignement tunisiens. Par la suite, le président de l'Instance nationale de la Protection des Données personnelles et un magistrat lié au tribunal administratif ont effectué une visite de travail au Comité permanent R.

Une rencontre s'est déroulée à l'ambassade de Lituanie à Bruxelles entre les présidents du Comité de la Défense et de la Sécurité, d'une part, et du Comité permanent R, d'autre part. Cette réunion a elle aussi principalement porté sur l'organisation du contrôle démocratique des services de renseignement et sur la présentation du modèle belge.

Comme indiqué ci-dessus (Chapitre II.10 et II.11.12), les révélations d'E. Snowden ont donné lieu à l'ouverture de nombreuses enquêtes dans le monde entier, y compris au Parlement européen. Dans le sillage de la Résolution du Parlement européen du 4 juillet 2013, la Commission Libertés civiles, Justice et Affaires intérieures (ou Commission LIBE) du Parlement européen a organisé une série d'auditions visant à recueillir des informations et à évaluer les répercussions des activités d'espionnage sur les droits fondamentaux et les règles de protection des données. Le président du Comité permanent R, M. Guy Rapaille, a été invité dans ce cadre avec le Sénateur et membre de la Commission sénatoriale de suivi, M. Armand De Decker, à la mi-novembre 2013. Ils ont brièvement expliqué les enquêtes belges en cours.[170]

Depuis 2011, le président du Comité permanent R assure également la présidence du *Belgian Intelligence Studies Centre* (BISC). Ce centre d'études sur le renseignement entend rapprocher les services de renseignement et de sécurité et la communauté scientifique, et contribuer à la réflexion sur des problèmes sociétaux en matière de renseignement.[171] En 2013, le BISC a organisé trois journées d'étude : « Chronique de ma guerre cachée, 1941-1944 » (mars 2013), « L'espionnage pendant et après la Guerre froide 'revisited' » (juin 2013) et « Open source and social media intelligence » (décembre 2013).

En 2013, la fréquence des travaux du « Groupe de travail Analyse », où siègent des représentants des deux services de renseignement et du Comité permanent R,

169 www.dcaf-tunisie.org.

170 European Parliament, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, The role of parliamentary oversight of intelligence services at national level in an era of mass surveillance, Statement by Mr Guy Rapaille, Chair of the Belgian Intelligence Services Oversight Committee, 14 novembre 2013 (www.europarl.europa.eu).

171 www.intelligencestudies.be.

s'est intensifiée. Ce groupe de travail s'est chargé des préparatifs liés à la mise en place de la *Belgian Intelligence Academy* (BIA)[172], une académie qui organisera des formations pour analystes issus tant du service de renseignement civil que militaire. Dans l'intervalle, les organes de gestion de cette académie du renseignement ont vu le jour : un Comité de direction, un Comité exécutif avec nomination d'un directeur et d'un secrétariat, ainsi qu'un Comité scientifique. Le président du Comité permanent R intervient en tant qu'observateur auprès du Comité de direction, et au moins un représentant du Comité fait partie du Comité scientifique. Un premier « test case Intelligence and Analysis Course » (IAC), qui s'est déroulé de la mi-juin à la mi-juillet 2013, a fait l'objet d'une évaluation et a donné lieu à l'élaboration d'un protocole d'accord entre les ministres concernés. En outre, début juin 2013, des représentants de la VSSE, du SGRS et du Comité permanent R ont effectué une visite de travail à l'Académie française du Renseignement de Paris.

Enfin, le Comité permanent R a été consulté par le monde académique en 2013. Le président du Comité a fait partie d'un jury pour la défense d'une thèse au Centre français des Hautes Études du ministère de l'Intérieur.[173] Par ailleurs, le Comité a participé en tant qu'expert à une enquête sur les « nouveaux défis de la politique de renseignement en France », menée par le professeur Sébastien Laurent, lié à l'Université de Bordeaux. Le Comité a également été invité à dispenser des cours dans les universités de Liège et Louvain-la-Neuve. Il a participé au Jobday de la faculté de Droit, Science politique et Criminologie de l'université de Liège, ainsi qu'à une table ronde de la Ligue flamande des Droits de l'homme sur la vie privée et la sécurité.

V.4. MEMBRE D'UN COMITÉ DE SÉLECTION

Le président du Comité permanent R a été désigné, aux côtés du président de la Cellule de traitement des informations financières (CTIF) et du directeur de l'Organe de coordination pour l'analyse de la menace (OCAM), dans le comité de sélection chargé de remettre un avis circonstancié aux ministres de l'Intérieur et de la Justice concernant les candidatures pour le poste de directeur adjoint de l'Organe de coordination pour l'analyse de la menace.[174]

---

172 L'académie est investie de la mission suivante : « *La Belgian Intelligence Academy vise à être le moteur et la référence en matière de formation professionnelle dans le renseignement civil et militaire, et à être reconnue pour son expertise et ses compétences. Elle a pour mission de dispenser des formations communes et structurées, de qualité, au personnel des services de renseignement* ».

173 Cette thèse avait pour thème « L'action des services de renseignement à l'épreuve du droit : quelles insuffisances, quelles améliorations ? ».

174 A.M. du 29 mars 2013 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour le poste de directeur adjoint de l'Organe de coordination pour l'analyse de la menace, *M.B.* 8 avril 2013.

V.5. PROJET DE PROPOSITION DE LOI MODIFIANT LA LOI RELATIVE À LA CLASSIFICATION

À la mi-2013, la Commission de suivi du Sénat a chargé le Comité d'élaborer une proposition de loi visant à adapter la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité (L.C&HS). L'objectif est de mettre en place une procédure d'*overruling* ou une déclassification automatique lorsqu'une classification donnée ne semble pas suffisamment justifiée. La demande du Sénat s'inscrivait dans le cadre de recommandations antérieures du Comité.[175] Le Comité n'a pas été en mesure de finaliser cette proposition en raison d'autres priorités. Une proposition sera élaborée et transmise à la nouvelle Commission de suivi de la Chambre des Représentants.

V.6. CONTRÔLE DES FONDS SPÉCIAUX DU SGRS

La Cour des Comptes contrôle l'utilisation des moyens financiers par les services publics au nom de la Chambre des Représentants. Dans ce cadre, elle est amenée à contrôler la légalité et la légitimité de toutes les dépenses, y compris en principe de toutes les dépenses des services de renseignement. Cependant, en raison du caractère sensible de la matière, la Cour des Comptes n'examine pas une partie des comptes de la VSSE et du SGRS (à savoir les « fonds spéciaux » qui englobent des dépenses destinées, par exemple, aux opérations et aux informateurs). Pour la VSSE, le contrôle de ces dépenses est effectué par le chef de cabinet du ministre de la Justice. Depuis 2006, c'est le chef des Forces armées (CHOD) qui exerce seul le contrôle sur des fonds spéciaux du SGRS, et ce à raison de quatre fois par an. À la suggestion de la Cour des Comptes, ce contrôle se déroule en présence du président du Comité permanent R depuis 2010.

V.7. PRÉSENCE DANS LES MÉDIAS

Le Comité permanent R est de plus en plus souvent sollicité par la presse écrite et audiovisuelle pour fournir des explications sur ses travaux ou ceux des services de renseignement. Le Comité permanent R a accédé à plusieurs reprises à ces requêtes.

175 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 133.

Date	Sujet/titre	Lieu
Printemps 2013	Interview avec Guy Rapaille, président du Comité permanent R	Diplomatic World nr. 38
4 avril 2013	'Filip Dewinter et le Vlaams Belang visés par la Surêté'	L'Echo
4 avril 2013	'Staatsveiligheid stak dossier Dewinter niet in doofpot'	De Tijd
6 mai 2013	'Nieuw gezicht in controlecomité inlichtingendiensten	MO*
24 mai 2013	'De cultuur van het geheim neemt toe'	MO*
25 mai 2013	'Leger in opspraak over 'geheime' geheime dienst	De Tijd
6 juin 2013	'Staatsveiligheid gecontroleerd'	VRT, Radio 1, Joos
10 juin 2013	'Les renseignements belges'	RTBF, Radio Première, Face à l'info
27 juin 2013	'Des renseignements plus professionnels'	Le Soir
5 août 2013	'Controlecomité inlichtingen-diensten start groot Prism-onderzoek'	MO*
18 septembre 2013	'NSA kreeg blanco cheque in België'	De Morgen
22 septembre 2013	'Vision stratégique de la cyber-sécurité : un désintérêt général'	RTBF-TV, Mise au point
23 octobre 2013	'Staatsveiligheid leeft meldings-plicht aan minister niet na'	De Morgen
23 octobre 2013	'142 namen van politici in dossiers Staatsveiligheid'	MO*
31 octobre 2013	'A quoi sert l'espionnage ?'	RTBF, Radio Première, Le forum du midi

CHAPITRE VI

LES INFORMATIONS ET INSTRUCTIONS JUDICIAIRES

Parallèlement aux enquêtes de contrôle, le service d'Enquêtes R du Comité permanent R effectue également, à la demande des autorités judiciaires, des enquêtes sur des membres des services de renseignement soupçonnés d'avoir commis un crime ou un délit. Cette compétence est décrite à l'article 40, alinéa 3 de la Loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace. La Loi du 10 juillet 2006 relative à l'analyse de la menace a élargi cette compétence aux crimes et délits commis par des membres de l'Organe de coordination pour l'analyse de la menace (OCAM). En ce qui concerne les membres des autres « services d'appui », cette disposition s'applique uniquement à l'obligation de communiquer à l'OCAM tout renseignement pertinent (art. 6 et 14 L.OCAM).

Lorsqu'ils remplissent une mission de police judiciaire, les membres et le directeur du service d'Enquêtes R sont soumis à l'autorité du procureur général près la cour d'appel ou du procureur fédéral (art. 39 L.Contrôle). Le Comité permanent R n'a alors aucune autorité sur eux. Le président du Comité permanent R doit toutefois veiller à ce que l'exécution des missions de police judiciaire n'entrave pas l'exécution des enquêtes de contrôle, et ce pour une raison évidente : l'organe de contrôle est avant tout à la disposition du Parlement. Cette mission pourrait être mise en péril si trop de temps était consacré à des dossiers judiciaires. Le président peut, le cas échéant, se concerter avec les autorités judiciaires quant à la participation des membres du service d'Enquêtes R à des enquêtes pénales (art. 61*bis* L.Contrôle). Cette concertation ne s'est encore jamais avérée nécessaire.

Quand le service d'Enquêtes R effectue des enquêtes pénales, le directeur doit remettre un rapport au Comité permanent R au terme de l'enquête. Dans ce cas, « *le rapport se limite aux informations qui sont nécessaires à l'accomplissement par le Comité permanent R de ses missions* » (art. 43, alinéa 3, L.Contrôle).

En 2013, le service d'Enquêtes R a mené un nombre considérable de devoirs judiciaires dans le cadre de deux enquêtes importantes. Ainsi, par exemple, 56 procès-verbaux ont été dressés.

Une première enquête, lancée fin 2011 et menée au profit du parquet fédéral, sur d'éventuelles malversations financières commises par des agents de

renseignement, a été finalisée en 2013. Ce dossier judiciaire a été classé sans suite par le parquet fédéral, mais il a permis de mettre en lumière la nécessité d'adapter fondamentalement la gestion des fonds destinés à la rétribution des sources des services de renseignement.

Le second dossier, basé sur des faits similaires et qui était entre les mains du parquet d'Anvers, n'a pas pu être clôturé en 2013.

Ces deux dossiers judiciaires ont montré la nécessité de procéder à une analyse détaillée des règles et de la pratique en vigueur en matière de gestion des fonds destinés à la rétribution d'informateurs, et ce au sein des deux services de renseignement. Aussi, le Comité a-t-il décidé d'ouvrir une enquête de contrôle sur ce sujet (cf. II.10.3).

CHAPITRE VII
LE GREFFE DE L'ORGANE DE RECOURS EN MATIÈRE D'HABILITATIONS, D'ATTESTATIONS ET D'AVIS DE SÉCURITÉ

Le président du Comité permanent R assure également la présidence de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. La fonction de greffe est exercée par le greffier du Comité permanent R (ou son suppléant) et par son administration.

L'Organe de recours est compétent pour les contentieux qui portent sur des décisions dans quatre domaines : les habilitations de sécurité, les attestations de sécurité qui doivent permettre l'accès à des lieux où se trouvent des documents classifiés, les attestations de sécurité qui permettent l'accès à des lieux précis faisant l'objet de menaces et, enfin, les avis de sécurité. L'Organe de recours intervient également en tant que « juge d'annulation » contre des décisions d'autorités publiques ou administratives lorsqu'elles imposent des avis ou des attestations de sécurité pour un secteur, un lieu ou un événement donné.[176]

Ces activités de l'Organe de recours ont un impact direct tant sur le budget que sur le personnel du Comité permanent R. En effet, tous les frais de fonctionnement sont supportés par le Comité permanent R, qui met à disposition non seulement son président et son greffier, mais aussi son personnel administratif. Le traitement et le règlement des recours constituent une charge de travail de plus en plus lourde pour le Comité.

Ce chapitre mentionne les chiffres relatifs à la nature des décisions contestées, la qualité des autorités compétentes et des requérants, ainsi que la nature des décisions de l'Organe de recours dans le cadre des différentes procédures de recours. À des fins de comparaison, les chiffres de ces deux dernières années sont également repris.

En 2013, le nombre de recours et de décisions a connu un accroissement spectaculaire par rapport à 2012 : 189 recours contre 91 et 187 décisions contre 81. Cette augmentation tient surtout au fait que dans le courant de l'année 2013, de nombreux recours ont été introduits par des candidats militaires ayant reçu un avis

176 Pour plus de détails, voir le *Rapport d'activités 2006* du Comité permanent R (87-115).

de sécurité négatif du SGRS, qui, en la matière, agit en qualité d'autorité de sécurité dans le contexte d'une nouvelle procédure de sélection et de recrutement.[177]

Par ailleurs, il convient de noter l'augmentation significative du nombre de recours contre des avis de sécurité négatifs rendus dans le cadre de l'octroi des badges d'accès aux zones sécurisées des aéroports.

Tableau 1. Autorités de sécurité concernées

	2011	**2012**	**2013**
Autorité nationale de Sécurité	21	40	98
Sûreté de l'État	2	0	1
Service général du renseignement et de la sécurité	39	27	78[178]
Direction générale du Centre de Crise	0	0	0
Agence fédérale de Contrôle nucléaire	7	11	9
Police fédérale	1	1	1
Police locale	0	2	2
Commission aéroportuaire locale	1	10	–[179]
TOTAL	**71**	**91**	**189**

Tableau 2. Nature des décisions contestées

	2011	2012	2013
Habilitations de sécurité			
Confidentiel	14	7	5
Secret	31	29	56
Très secret	9	9	5
Total habilitations de sécurité	54	45	66

177 Voir l'article 9 de la Loi du 28 février 2007 fixant le statut des militaires du cadre actif des forces armées et modifiant certaines dispositions relatives au statut du personnel militaire tel que modifié par l'article 24 de la Loi du 31 juillet 2013 (*M.B.* 20 septembre 2013).

178 Comme indiqué dans l'introduction de ce chapitre, l'accroissement significatif du nombre de dossiers émanant du SGRS est dû au système par lequel les candidats militaires peuvent être soumis à une vérification de sécurité.

179 Depuis 2013, les avis dans le cadre de l'octroi de badges de sécurité donnant accès aux zones sécurisées des aéroports ne sont plus rendus par les commissions aéroportuaires locales mais par l'Autorité Nationale de Sécurité, ce qui explique aussi l'augmentation du nombre de dossiers émanant de l'ANS par rapport aux années précédentes.

	2011	2012	2013
Refus	32	33	41
Retrait	21	12	5
Refus et retrait	–	–	4
Habilitation pour une durée limitée	0	0	1
Habilitation pour un niveau inférieur	1	1	0
Pas de décision dans les délais	0	1	15
Pas de décision dans les nouveaux délais	0	0	0
Total habilitations de sécurité	54	45	66
SOUS-TOTAL HABILITATIONS DE SÉCURITÉ	**54**	**45**	**66**
Attestations de sécurité documents classifiés			
Refus	0	23	0
Retrait	0	0	0
Pas de décision dans les délais	0	0	0
Attestations de sécurité lieu ou événement			
Refus	14	0	15
Retrait	0	0	0
Pas de décision dans le délai	0	0	0
Avis de sécurité			
Avis négatif	3	23	106
Pas d'avis	0	0	2
« Révocation » d'un avis positif	0	0	0
Actes normatifs d'une autorité administrative	0	0	0
Décision d'une autorité publique d'exiger des attestations	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des attestations	0	0	0
Décision d'une autorité administrative d'exiger des avis	0	0	0
Refus de l'ANS d'effectuer des vérifications pour des avis	0	0	0
SOUS-TOTAL ATTESTATIONS ET AVIS	**17**	**46**	**123**
TOTAL DÉCISIONS CONTESTÉES	**71**	**91**	**189**

Tableau 3. Nature du requérant

	2011	**2012**	**2013**
Fonctionnaire	4	5	4
Militaire	37	26	26
Particulier	29	54	159
Personne morale	1	6	0

Tableau 4. Langue du requérant

	2011	2012	2013
Français	32	51	92
Néerlandais	39	40	97
Allemand	0	0	0
Autre langue	0	0	0

Tableau 5. Nature des décisions interlocutoires prises par l'Organe de recours[180]

	2011	2012	2013
Demande du dossier complet (1)	68	90	187
Demande d'informations complémentaires (2)	5	5	12
Audition d'un membre d'une autorité (3)	4	10	3
Décision du président (4)	0	0	0
Soustraction d'informations du dossier par l'Organe de recours (5)	24	44	68
Soustraction d'informations du dossier par le service de renseignement (6)	0	0	0

180 Le « nombre de décisions interlocutoires » (tableau 5), les « manières dont les requérants font usage de leurs droits de défense » (tableau 6), ou encore la « nature des décisions de l'Organe de recours » (tableau 7) ne correspondent pas nécessairement au nombre de requêtes introduites (voir tableaux 1 à 4). En effet, certains dossiers ont par exemple déjà été ouverts en 2012, alors que la décision n'a été rendue qu'en 2013.

(1) L'Organe de recours peut demander l'intégralité du dossier d'enquête aux autorités de sécurité. Comme ce dossier contient davantage de données que le rapport d'enquête seul, cette requête est systématique.
(2) L'Organe de recours peut également demander tout complément d'informations qu'il juge nécessaire pendant la procédure.
(3) L'Organe de recours peut décider d'entendre les membres des services de renseignement et de police ou des autorités de sécurité qui ont participé à l'enquête ou à la vérification de sécurité.
(4) Le président de l'Organe de recours peut décider de permettre au membre du service de renseignement de garder secrètes certaines données pendant son audition.
(5) Si le service de renseignement concerné le requiert, l'Organe de recours peut décider que certaines informations soient retirées du dossier communiqué au requérant.
(6) Si l'information concernée provient d'un service de renseignement étranger, c'est le service de renseignement belge qui décide si elle peut être communiquée. Il s'agit d'un aspect de l'application de la « règle du tiers service ».

Tableau 6. Manières dont les requérants font usage de leurs droits de défense

	2011	2012	2013
Consultation du dossier par le requérant /l'avocat	48	54	103
Audition du requérant /avocat[181]	55	65	138

Tableau 7. Nature des décisions de l'Organe de recours

	2011	2012	2013
Habilitations de sécurité			
Recours irrecevable	5	0	2
Recours sans objet	1	1	3
Recours non fondé	29	19	20
Recours fondé (avec octroi partiel ou complet)	19	23	35
Devoir d'enquête complémentaire par l'autorité	1	1	0
Délai supplémentaire pour l'autorité	0	0	14[182]

181 Dans le cadre de certains dossiers, le requérant/avocat est auditionné à plusieurs reprises.
182 Ces dossiers concernaient principalement l'octroi d'habilitations de sécurité pour des membres du personnel du SHAPE. Vu que l'autorité belge de sécurité attendait parfois en vain des informations devant être communiquées par la France, les délais légaux ont été dépassés. Dans 14 cas, l'Organe de recours a décidé d'accorder un délai supplémentaire à l'Autorité nationale de sécurité pour encore prendre une décision.

	2011	2012	2013
Attestations de sécurité pour documents classifiés			
Recours irrecevable	0	0	0
Recours sans objet	0	0	0
Recours non fondé	0	0	0
Recours fondé (avec octroi)	0	0	0
Attestations de sécurité pour lieux ou événements			
Recours irrecevable	1	3	1
Recours sans objet	0	1	0
Recours non fondé	7	8	6
Recours fondé (avec octroi)	4	6	11
Avis de sécurité			
Organe de recours non compétent	0	5	0
Recours irrecevable	0	1	4
Recours sans objet	0	0	1
Confirmation de l'avis négatif	0	9	25
Transformation en avis positif	3	4	65[183]
Recours contre des actes normatifs d'une autorité administrative	0	0	0
TOTAL	70	81	187

[183] Comme indiqué dans l'introduction de ce chapitre, l'augmentation du nombre de dossiers en matière d'avis de sécurité s'explique par les recours de candidats militaires et de personnes qui doivent se voir attribuer un badge d'accès aux zones sécurisées des aéroports.

CHAPITRE VIII
LE FONCTIONNEMENT INTERNE DU COMITÉ PERMANENT R

VIII.1. COMPOSITION DU COMITÉ PERMANENT R

Lors de sa séance plénière du 2 mai 2013, le Sénat a procédé à la nomination de deux membres effectifs, de deux présidents suppléants et de quatre membres suppléants du Comité permanent R.[184] M. Gérald Vande Walle (F) a été à réélu comme membre effectif francophone. M. Pieter-Alexander De Brock (N), expert détaché de l'Organe de coordination pour l'analyse de la menace, a été élu comme conseiller néerlandophone. Ils ont prêté serment le 8 mai 2013 entre les mains de la présidente du Sénat. M. Guy Rapaille (F), avocat général près la cour d'appel de Liège, avait déjà été reconduit dans ses fonctions. Le service d'Enquêtes R a connu lui aussi quelques changements. Un commissaire auditeur néerlandophone et un commissaire auditeur francophone ont décidé de quitter le service. Ils ont été remplacés respectivement en mars 2013 et en janvier 2014. À la fin de l'année 2013, le directeur du service d'Enquêtes R, M. Pierre Nivelle, a également décidé de quitter le service. Il a été remplacé le 2 décembre 2013 par M. Frank Franceus, qui exerçait jusque-là la fonction de commissaire auditeur. Il a été nommé pour un mandat de cinq ans, à compter du 1er janvier 2014. L'effectif de ce service est retombé à cinq équivalents temps plein.

Le cadre du personnel administratif du Comité permanent R, placé sous la direction du greffier M. Wouter De Ridder, n'a pas été modifié et comptait toujours seize personnes.

VIII.2. RÉUNIONS AVEC LA OU LES COMMISSION(S) DE SUIVI

Dans le courant de l'année 2013, six réunions ont été tenues avec la Commission de suivi du Sénat. Lors de ces réunions – à huis clos – les rapports des enquêtes

184 *M.B.* 21 mai 2013. M. Pierre Vanderheyden, avocat général près la cour d'appel de Liège, a été désigné comme premier président suppléant; M. Emile Dejehansart, conseiller près la cour d'appel de Mons, l'a été comme second président suppléant. M. Carmelo Zaïti, M. Philippe Meire, M. Herman Daens et M. Frank Franceus ont été désignés comme membres suppléants.

de contrôle ont été discutés. Le « rapport semestriel sur l'application des méthodes spécifiques et exceptionnelles par les services de renseignement et de sécurité et le contrôle effectué sur celles-ci par le Comité permanent R pour l'année d'activités 2012 » a également fait l'objet d'une discussion. En outre, une réunion a eu lieu en octobre 2013 avec les Commissions de suivi de la Chambre des Représentants et du Sénat. Lors de cette réunion, le *Rapport d'activités 2012* du Comité permanent R a été discuté[185], et une enquête de contrôle commune des Comités permanents R et P a été mise à l'agenda.

La composition de la Commission du Sénat a été modifiée. Madame Sabine de Bethune (CD&V), en sa qualité de présidente du Sénat, a pris la présidence de la commission. Messieurs Dirk Claes (CD&V), Armand De Decker (MR), Philippe Mahoux (PS) et Danny Pieters (N-VA) faisaient également partie de cette commission. Le 17 juillet 2013, Monsieur Danny Pieters (N-VA) a été remplacé par Monsieur Karl Vanlouwe (N-VA).[186]

Conformément à la Loi du 6 janvier 2014 (*M.B.* 31 janvier 2014), le point de contact du Comité permanent R est passé du Sénat à une unique « Commission chargée de l'accompagnement du Comité permanent P et du Comité permanent R » à la Chambre des Représentants, qui contrôlera à la fois les services de police et les services de renseignement.

VIII.3. RÉUNIONS COMMUNES AVEC LE COMITÉ PERMANENT P

Les articles 52 à 55 L.Contrôle déterminent les cas où et la manière dont le Comité permanent R et le Comité permanent P doivent organiser des réunions communes. Ces réunions poursuivent un double objectif: échanger des informations et discuter d'enquêtes de contrôle communes. En 2013, cinq réunions communes ont eu lieu.

VIII.4. MOYENS FINANCIERS ET ACTIVITÉS DE GESTION

Pour l'année d'activités 2013, le Comité permanent R a bénéficié d'une dotation de 3,86 millions d'euros contre 3,93 millions d'euros en 2012.[187] En 2013, le Comité permanent R a pu conserver tout le bénéfice des économies réalisées par les économies d'échelle découlant de son déménagement vers le bâtiment Forum

185 *Doc. parl.* Sénat 2013-14, n°5-2426/1 et *Doc parl.* Chambre 2013-14, n°53-3496/1.
186 *Ann. parl.* Sénat 2012-13, 17 juillet 2013, n°5-113,7.
187 Loi du 4 mars 2013 contenant le budget général des dépenses pour l'année budgétaire 2013, *M.B.* 15 mars 2013 et *Doc. parl.* Chambre, 2012-2013, n° 53-2578/001.

de la Chambre des Représentants. Par ailleurs, en matière de frais de fonctionnement, de nouvelles synergies ont été développées avec la Chambre.

VIII.5. FORMATION

Vu l'intérêt pour l'organisation, le Comité permanent R encourage ses collaborateurs à suivre des formations générales (informatique, management…) ou propres au secteur. Concernant cette dernière catégorie, un ou plusieurs membres (du personnel) du Comité ont assisté aux journées d'étude mentionnées ci-dessous.

DATE	TITRE	ORGANISATION	LIEU
2012-2013 2013-2014	Hautes études de sécurité et de défense	IRSD	Bruxelles
14 janvier 2013	Le renseignement en réseaux	Métis	Paris
17 janvier 2013	Renseignement de sources ouvertes : sommes-nous tous des capteurs ?	IRSD	Bruxelles
1er mars 2013	Cybercriminalité – Enjeux et actualités	Université de Namur – B-CCentre – CRIDS	Namur
19 mars 2013	Chronique de ma guerre cachée, 1941-1944	BISC	Bruxelles
26 mars 2013	De conflicten tussen het Belgische recht en het lokaal recht	Studiecentrum voor Militair recht en Oorlogsrecht	Bruxelles
26 mars 2013	Le paysage nucléaire militaire en mutation	Académie royale de Belgique	Bruxelles
27 mars 2013	Cybercrime – Risks to Operative Derived from Smart Phones, the Internet en Social Media	Ambassade du Royaume- Uni	Bruxelles
4 avril 2013	Modernisation et cadre juridique du renseignement en France	Université de Lille	Lille
29 avril 2013	Le renseignement en question : les sources ouvertes	Métis	Paris
22-23 mai 2013	Changing Intelligence Challenges	GFF – CATS – Swedish National Defence College – SUPO	Stockholm
3 juin 2013	Rencontre coordination du renseignement	BIA	Paris

DATE	TITRE	ORGANISATION	LIEU
10 juin 2013	L'espionnage pendant et après la Guerre froide 'revisited'	BISC	Bruxelles
13 juin 2013	L'action des services de renseignement à l'épreuve du droit	Centre des hautes études du Ministère de l'Intérieur	Paris
13 juin 2013	Intelligence stratégique	HEC Liège – BISC	Seraing
21 juin 2013	Diplomatic security conference	ECSA	Bruxelles
24 juin 2013	Le renseignement en question : les sources ouvertes	Métis	Paris
27 juin 2013	Security & Defence Day Conference	Security & Defence– SDA – CEIS – KAS	Bruxelles
10 juillet 2013	Le rapport Urvoas : quel contrôle des services de renseignement ?	HCFDC	Paris
19 septembre 2013	Beyond the security vs privacy debate	Security & Defence	Bruxelles
20 septembre 2013	Single table lunch meeting (Mr Leonard H. Schrank)	ECSA	Bruxelles
30 septembre 2013	Éthique et renseignement	GERER	Paris
16 octobre 2013	TIGFI Finance Lunch	The Institute for Global Financial Integrity	Luxembourg
21 octobre 2013	De Belgische wapenhandel	Vlaams Vredesinstituut – GRIP	Bruxelles
24 octobre 2013	Single table lunch meeting (Mr André Vandoren)	ECSA	Bruxelles
15 novembre 2013	Les Assises de l'Intelligence Stratégique	Agence de Stimulation économique – Université Louvain-la-Neuve	Louvain-la-Neuve
21 novembre 2013	Avonddebat 'Privacy'	Liga voor Mensenrechten	Bruxelles
27 novembre 2013	10 ans de MPR – bilans et défis	Police fédérale (DJO/ BTS)	Bruxelles
6 décembre 2013	Open source & social media intelligence	BISC	Bruxelles
16 décembre 2013	Éthique et renseignement	GERER	Paris

VIII.6. ÉVALUATION DES PROCESSUS DE TRAVAIL INTERNES

Comme en 2009, le Comité permanent R a procédé à une évaluation approfondie de ses processus de travail internes. Il s'agit plus spécifiquement des flux de travail dans le cadre de l'exécution des enquêtes de contrôle, du suivi des dossiers MRD ou encore de la gestion des dossiers de l'Organe de recours en matière d'habilitations, d'attestations et d'avis de sécurité. En s'appuyant sur ses constatations, le Comité permanent R a pu optimaliser son fonctionnement interne.

CHAPITRE IX
RECOMMANDATIONS

À la lumière des enquêtes de contrôle clôturées en 2013 et des dossiers MRD traités, le Comité permanent R formule les recommandations reprises ci-après. Elles portent plus particulièrement sur la protection des droits que la Constitution et la loi confèrent aux personnes (IX.1), sur la coordination et l'efficacité des services de renseignement, de l'OCAM et des services d'appui (IX.2) et, enfin, sur l'optimalisation des possibilités de contrôle du Comité permanent R (IX.3).

IX.1. RECOMMANDATIONS RELATIVES À LA PROTECTION DES DROITS QUE LA CONSTITUTION ET LA LOI CONFÈRENT AUX PERSONNES

IX.1.1. EXÉCUTION DES ARTICLES 19 ET 20 L.R&S[188]

Le Comité rappelle une fois encore que conformément aux articles 19 et 20 L.R&S, il incombe aux ministres compétents et au Comité ministériel du renseignement et de la sécurité de déterminer dans quelles conditions les services de renseignement belges doivent ou peuvent collaborer avec des services de renseignement étrangers. Le Comité permanent R estime nécessaire que les deux services de renseignement formulent, au plus tard à la mi-2015, une proposition conjointe traitant de tous les aspects de la problématique à l'intention du Comité ministériel.

Plus particulièrement en ce qui concerne le SGRS, le Comité permanent R recommande qu'une étude soit réalisée sur l'éventuelle responsabilité du service lorsque celui-ci échange des informations et/ou renseignements avec un service de renseignement ou un organe étranger.

---

188 Cette recommandation découle des enquêtes concernant « Le rôle du Service général du renseignement et de la sécurité dans le suivi du conflit en Afghanistan » (voir II.1) et « Le suivi de mandataires politiques par les services de renseignement » (II.4).

IX.1.2. UNE DIRECTIVE SUR LE TRAVAIL DE RENSEIGNEMENT À L'ÉGARD DE PERSONNES EXERÇANT DES RESPONSABILITÉS PARTICULIÈRES ET DE PARTIS POLITIQUES[189]

Le Comité permanent R souhaite que la Sûreté de l'État et le Service général du renseignement et de la sécurité prennent une initiative conjointe à l'égard du Comité ministériel du renseignement et de la sécurité, aux fins de l'adoption d'une directive uniforme avec des règles claires et univoques quant au recueil, au traitement, à la consultation (y compris le cloisonnement interne éventuel), au stockage et à l'archivage des données de certaines catégories de personnes qui assument ou ont assumé des responsabilités particulières ainsi que des partis politiques. Lors de l'élaboration de cette directive, il convient de tenir compte de la liberté d'association, de la liberté d'expression et du cadre tracé dans l'arrêt rendu par la Cour européenne des Droits de l'Homme dans l'affaire « Segerstedt-Wiberg and others », et de donner corps au principe énoncé à l'article 2 de la Loi du 30 novembre 1998 : « *Dans l'exercice de leurs missions, ces services veillent au respect et contribuent à la protection des droits et libertés individuels, ainsi qu'au développement démocratique de la société* ».

Enfin, le Comité fait remarquer qu'il incombe au législateur de prévoir, sur demande, des garanties particulières pour des mandataires politiques par le biais d'une adaptation éventuelle de la législation (par exemple dans la Loi MRD) et/ou en chargeant le Comité permanent R d'une mission de contrôle spécifique. Dans ce cadre, il convient toutefois de tenir compte de l'importance d'un fonctionnement normal et d'une évolution normale des institutions démocratiques ainsi que des missions légales des services de renseignement.

IX.1.3. DIRECTIVES UNIVOQUES CONCERNANT L'INFORMATION SUR LE SUIVI DE RESPONSABLES POLITIQUES

Faisant suite à la recommandation précédente, le Comité estime qu'il incombe aux ministres compétents – en tant qu'autorités responsables sur les plans hiérarchique et politique – de déterminer dans quels cas et quand ils souhaitent être informés. À cet égard, il importe que les ministres décrivent clairement la finalité et les modalités[190] d'une telle information.

---

189 Cette recommandation a été formulée dans le sillage des enquêtes de contrôle « Notes secrètes sur l'Église de scientologie dans la presse » (II.2.), « Un informateur au sein du Vlaams Belang ? » (II.3) et « Le suivi de mandataires politiques par les services de renseignement » (II.4). Le Comité reprend ainsi la recommandation de son enquête sur les « dossiers réservés » (voir COMITÉ PERMANENT R, *Rapport d'activités 2008*, 106-107).

190 Information immédiate ou périodique ; information des seuls documents de collecte, rapports d'analyse et/ou rapports destinés à des services externes ; information également pour des

IX.1.4. FORMATION PERMANENTE ET CONTRÔLE RÉEL DE LA QUALITÉ DES RAPPORTS DE COLLECTE[191]

Le Comité est conscient du fait qu'il n'est pas toujours évident, dans le travail de renseignement, de déterminer au moment de la collecte quelles informations se révéleront un jour pertinentes ou non. Il n'empêche qu'il convient de respecter les exigences en la matière, telles que celles décrites dans la L.R&S ainsi que dans la Loi relative à la protection de la vie privée (principe de finalité, adéquation, exactitude…). Ce qui signifie, par exemple, que le fait qu'un événement donné soit mentionné dans un rapport de collecte et la manière dont il y est repris revêtent une importance cruciale. La manière dont cet *input* doit avoir lieu devrait faire l'objet d'une formation permanente et être soumise à un sérieux contrôle de qualité.

IX.2. RECOMMANDATIONS RELATIVES À LA COORDINATION ET L'EFFICACITÉ DES SERVICES DE RENSEIGNEMENT, DE L'OCAM ET DES SERVICES D'APPUI

IX.2.1. RECOMMANDATIONS DANS LE CADRE DES MISSIONS DU SGRS À L'ÉTRANGER

Dans le cadre de son enquête de contrôle sur « Le rôle du Service général du renseignement et de la sécurité dans le suivi du conflit en Afghanistan » (II.1), plusieurs recommandations ponctuelles ont été formulées.[192] Le Comité permanent R :

– recommande que le SGRS définisse les liens qui doivent être établis entre des renseignements opérationnels, tactiques et stratégiques et les missions légales décrites dans la L.R&S ;

---

ministres et parlementaires régionaux et/ou hauts dignitaires du pouvoir judiciaire ; contrôle éventuel par le Comité permanent R par le biais d'un accès autonome à la base de données…

191 Cette recommandation découle de l'enquête de contrôle concernant les « faits prétendument répréhensibles d'un service de renseignement étranger et le niveau d'information de la VSSE » (II.6).

192 En réaction au rapport, le SGRS a affirmé que les recommandations « *een wezenlijke bijdrage kunnen leveren voor de optimalisatie van organisatie en werking van ADIV. Hoewel het onderzoek zich focust op één operatie, die in meer dan 10 jaren grondige wijzigingen heeft ondergaan, blijft het zeker representatief voor het actuele inlichtingenwerk van ADIV* ». (« *peuvent constituer une contribution essentielle à l'optimalisation de l'organisation et au fonctionnement du SGRS. Bien que l'enquête se concentre sur une seule opération, qui en plus d'une décennie a subi de profondes modifications, elle reste certainement représentative du travail de renseignement actuel du SGRS.* » (traduction libre)). Il s'avère également que le service a déjà commencé à mettre en œuvre diverses recommandations. Le Comité ne peut que s'en réjouir.

- conseille au SGRS de rassembler les textes qui sont d'application lors d'un déploiement du SGRS, en y incluant les règles internationales et nationales. Eu égard à ce dernier point, une meilleure intégration et une plus grande cohérence du contenu s'imposent ;
- estime qu'il est nécessaire de renforcer la formation du personnel avant un départ en mission et exhorte le SGRS à poursuivre les améliorations déjà entreprises ;
- estime nécessaire que le SGRS applique la méthode « *Comprehensive Preparation of the Operational Environnement* » (ou toute autre méthodologie qui vise le même objectif) et prenne surtout en considération les besoins exprimés par les partenaires militaires dans le cadre de la préparation des missions ;
- recommande que le SGRS adopte une attitude proactive à l'égard de ses clients afin de pouvoir déterminer plus précisément leurs attentes, mais aussi afin de leur donner une idée précise de ce que le SGRS peut leur fournir ;
- conseille au SGRS de réaliser une estimation générale des risques encourus par le personnel civil et militaire déployé dans la zone de conflit et de formuler des propositions pour les gérer ;
- exhorte le SGRS à définir de manière plus détaillée le rôle des analystes déployés dans un environnement de collecte de renseignements, en particulier pour garantir l'objectivité de la fonction d'analyse ;
- conseille au SGRS de mettre en œuvre une approche plus systématique lors du déploiement du personnel dans la zone de conflit. Cette approche, qui prend pour point de départ les menaces que le SGRS doit suivre dans le cadre de la L.R&S, est essentielle pour déterminer les moyens humains et matériels à déployer ;
- estime que le personnel du SGRS qui est déployé dans la zone de conflit doit disposer du matériel adéquat, particulièrement les moyens de communication et les véhicules mis à la disposition du BENIC.

IX.2.2. UN DÉBAT SUR LA MISE EN ŒUVRE DE MÉTHODES MRD À L'ÉTRANGER

Pour intercepter des communications émises à l'étranger, par exemple pour des raisons de sécurité et de protection de nos troupes et de celles de nos alliés lors de missions à l'étranger, le SGRS dispose d'un mandat légal spécifique (art. 259*bis* § 5 CP joint à l'art. 11 § 2, 3° L.R&S). Or il ne dispose pas d'un tel mandat pour la mise en œuvre de méthodes particulières de renseignement. Le Comité recommande que le législateur mène un débat sur la nécessité de permettre certaines méthodes MRD à l'étranger. Le ministre de la Défense a souscrit à l'idée – entre autres aux fins du respect des droits de l'homme et des besoins opérationnels sur le terrain – d'accorder une attention spécifique à cette problématique et l'a assortie d'une évaluation de la Loi MRD.

IX.2.3. DES CONCEPTS UNIVOQUES POUR L'ORGANISATION DE LA BASE DE DONNÉES

Dans son enquête de contrôle sur le suivi de mandataires politiques (II.4), le Comité permanent R a dû constater que les concepts à la base de l'organisation de la banque de données de la VSSE sont à l'origine de problèmes fondamentaux, parce qu'ils ne sont pas interprétés de manière univoque ou appliqués en tant que tels. Aussi le travail de renseignement risque-t-il de perdre en efficacité et en efficience, puisque (tous) les rapports appropriés risquent de ne pas « remonter à la surface » lorsque cela s'avère nécessaire pour le travail d'analyse. Il y a aussi un risque de tirer des conclusions erronées. Le Comité permanent R estime dès lors que la VSSE devrait réexaminer d'urgence ces concepts, particulièrement lorsqu'ils apparaissent dans des documents diffusés en dehors de la VSSE.

Par ailleurs, le Comité permanent R estime qu'un concept manque actuellement à l'appel : l'indication du rôle (supposé) d'une personne citée dans un rapport à l'égard de la menace : s'agit-il d'un « passant », d'une « victime potentielle », d'un « personnage clé », d'un « acteur »… ?

IX.2.4. LA RÉDACTION DES CONCLUSIONS DU TRAVAIL D'ANALYSE[193]

Le Comité recommande que la VSSE clôture toute analyse par une conclusion (qu'elle soit sommaire ou provisoire) en vue d'établir si, comment et avec quelle intensité l'objet de l'analyse (personne, groupement, événement ou phénomène) doit continuer à être suivi.

IX.2.5. LE CONTRÔLE DES SERVICES DE RENSEIGNEMENT ÉTRANGERS

L'élargissement des compétences des services de renseignement en matière de contrôle des services de renseignement étrangers s'est une nouvelle fois avéré nécessaire.[194] Aussi le Comité rappelle-t-il sa recommandation et celle du Sénat visant à inscrire dans la Loi organique des services de renseignement et de sécurité une compétence spécifique en matière de contrôle de la légalité des activités des services de renseignement étrangers sur le territoire belge.[195]

---

193 Cette recommandation découle de l'enquête de contrôle concernant les « faits prétendument répréhensibles d'un service de renseignement étranger et le niveau d'information de la VSSE » (II.6).

194 *Ibid*.

195 COMITÉ PERMANENT R, *Rapport d'activités 2006*, 128.

IX.2.6. PROCÉDURE D'EXTRÊME URGENCE EN CAS D'APPLICATION DE L'ARTICLE 13/1, § 2 L.R&S

L'article 13/1 § 2, alinéa 3 L.R&S octroie à la Commission BIM (dans son ensemble) la possibilité d'autoriser expressément des agents de renseignement à commettre des infractions absolument nécessaires pour assurer l'efficacité d'une méthode MRD ou pour garantir leur propre sécurité ou celle d'autres personnes. La loi n'a toutefois prévu aucune procédure d'extrême urgence en la matière. Le Comité estime que lorsque la méthode particulière peut être mise en œuvre en cas d'extrême urgence, il convient de prévoir également la possibilité que la compétence accessoire découlant de l'article 13/1 § 2, alinéa 3, L.R&S puisse être exercée en cas d'extrême urgence.

IX.3. RECOMMANDATION RELATIVE À L'EFFICACITÉ DU CONTRÔLE : APPLICATION STRICTE DE L'ARTICLE 33, § 2 L.CONTRÔLE

L'article 33, § 2 L.Contrôle stipule que : « *Les services de renseignement, l'Organe de coordination pour l'analyse de la menace et les autres services d'appui transmettent d'initiative au Comité permanent R les règlements et directives internes ainsi que tous les documents réglant le comportement des membres de ces services* ». Ce n'est pas la première fois[196] que le Comité permanent R a dû constater que cette obligation n'est pas strictement respectée, particulièrement en ce qui concerne le SGRS, l'OCAM et les services d'appui. L'application précise de cet article par les services contrôlés constitue une condition *sine qua non* à l'efficacité de l'exécution de la mission du Comité. Aussi le Comité souligne-t-il une nouvelle fois l'importance d'envoyer à temps et d'office toutes les données concernées.

196 Le Comité a déjà mené plusieurs enquêtes à cet égard : COMITÉ PERMANENT R, *Rapport d'activités 1996*, 20-24 (Rapport sur l'application de l'article 33 alinéa 2 L.Contrôle par les services de renseignement) ; *Rapport d'activités 2001,* 206-207 (Les informations indispensables dont le Comité permanent R estime devoir disposer afin d'accomplir sa mission efficacement) ; *Rapport d'activités 2002,* 26-27 (La transmission d'initiative par les services de renseignement de certains documents au Comité permanent R) ; *Rapport d'activités 2006,* 12.

ANNEXES

ANNEXE A.
APERÇU DES PRINCIPALES RÉGLEMENTATIONS RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1ER JANVIER 2013 AU 31 DÉCEMBRE 2013)

Loi 30 juillet 2013 portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *M.B.* 23 août 2013

Loi 31 juillet 2013 modifiant la loi du 28 février 2007 fixant le statut des militaires du cadre actif des Forces armées et modifiant certaines dispositions relatives au statut du personnel militaire, *M.B.* 20 septembre 2013

A.R. 14 janvier 2013 portant exécution de la loi du 4 décembre 2012 modifiant le Code de la nationalité belge afin de rendre l'acquisition de la nationalité belge neutre du point de vue de l'immigration, *M.B.* 21 janvier 2013

A.R. 23 juillet 2013 modifiant l'arrêté royal du 21 juin 1996 portant création d'un Comité ministériel du renseignement et de la sécurité, *M.B.* 30 juillet 2013

A.R. 4 septembre 2013 fixant la composition, le fonctionnement et les attributions du Comité de gestion de l'Autorité nationale de Sécurité, service de l'État à gestion séparée, *M.B.* 7 octobre 2013

A.R. 4 septembre 2013 fixant les montants des rétributions dues pour la délivrance des habilitations de sécurité, des attestations et des avis de sécurité, *M.B.* 7 octobre 2013

A.R. 7 octobre 2013 déterminant l'entrée en vigueur de certaines dispositions de la loi du 15 août 2012 relative à la création et à l'organisation d'un intégrateur de services fédéral, *M.B.* 23 octobre 2013

A.M. 7 janvier 2013 relatif à la constitution des jurys des épreuves linguistiques pour la session de décembre 2012-janvier 2013, *M.B.* 13 février 2013

A.M. 29 mars 2013 portant désignation d'un comité de sélection chargé de l'évaluation des candidatures pour la fonction de directeur adjoint de l'Organe de coordination pour l'analyse de la menace, *M.B.* 8 avril 2013

Comité Permanent de Contrôle des Services de Renseignement et de Sécurité – Directeur du Service d'enquêtes – Nomination, *M.B.* 30 janvier 2013

Circulaire 8 mars 2013 relative à certains aspects de la loi du 4 décembre 2012 modifiant le Code de la nationalité belge afin de rendre l'acquisition de la nationalité belge neutre du point de vue de l'immigration, *M.B.* 14 mars 2013

Nomination de deux membres effectifs, de deux présidents suppléants et de quatre membres suppléants pour le Comité permanent de contrôle des services de renseignements (Comité R), *M.B.* 21 mai 2013

ANNEXE B.
APERÇU DES PRINCIPALES PROPOSITIONS DE LOIS, DES PROJETS DE LOIS, DES RÉSOLUTIONS ET DES DÉBATS PARLEMENTAIRES RELATIFS AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1er JANVIER 2013 AU 31 DÉCEMBRE 2013)

Sénat

Proposition de loi modifiant les articles 137 et 138 du Code pénal visant à renforcer la lutte contre le terrorisme, *Doc. parl.*, Sénat, 2012-2013, nº 5-1655/2 et *Ann. parl.*, Chambre, 2012-2013, 7 février 2013, nº 53-91, p. 17

Projet de loi modifiant le livre II, titre Ier*ter* du Code pénal, *Doc. parl.*, Sénat, 2012-2013, nos 5-1905/2 en 5-1905/3

Proposition de loi complétant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, en vue d'élargir la compétence de contrôle de la Cellule de traitement des informations financières en ce qui concerne l'extrémisme, *Doc. parl.*, Sénat, 2012-2013, nos 5-1873/2 et 5-1873/3 et *Ann. parl.*, Chambre, 2012-2013, 16 mai 2013, nº 53-102, p. 34

Nomination des membres du Comité permanent de contrôle des services de renseignements (Comite R), *Doc. parl.*, Sénat, 2012-2013, nº 5-1956/1

Proposition de loi modifiant diverses lois suite à la réforme du Sénat, *Doc. parl.*, Sénat, 2012-2013, nos 5-1991/1, 5-1991/3 et 5-1991/6 et *Ann. parl.*, Sénat, 2013-2014, 26 novembre 2013, nº 5-125, p. 8

Proposition de budget pour l'année 2013 de la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (Commission BIM – C-BIM), *Doc. parl.*, Sénat, 2012-2013, nos 5-2014/1, 5-2014/2 et 5-2014/3 et *Ann. parl.*, Chambre, 2012-2013, 16 mai 2013, nº 53-102, p. 39

Proposition de loi visant à instituer une commission d'enquête parlementaire chargée d'examiner les cas de mise sous surveillance d'élus politiques par le service de la Sûreté de l'État, *Doc. parl.*, Sénat, 2012-2013, nº 5-2034/1

Proposition visant à modifier l'article 86*bis* du règlement du Sénat, en ce qui concerne la commission permanente chargée du suivi du Comité permanent de contrôle des services de renseignements et de sécurité, *Doc. parl.*, Sénat, 2012-2013, nº 5-2040/1

Nomination de deux membres effectifs, de deux présidents suppléants et de quatre membres suppléants pour le Comité permanent de contrôle des services de renseignements (Comité R), *Ann. parl.*, Chambre, 2012-2013, 2 mai 2013, nº 53-101, p. 42

Proposition de loi modifiant la loi du 18 juillet 1991 organique du contrôle des services de police et de renseignement et de l'Organe de coordination pour l'analyse de la menace, en ce qui concerne la composition de la commission permanente chargée du suivi du Comité permanent de contrôle des services de renseignements et de sécurité, *Doc. parl.*, Sénat, 2012-2013, nº 5-2157/1

Projet de loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *Doc. parl.*, Sénat, 2012-2013, nº 5-2222/3 et *Ann. parl.*, Sénat, 2012-2013, 18 juillet 2013, nº 5-114, p. 39

Comité permanent de contrôle des services de renseignement, rapport d'activités pour 2012, *Ann. parl.*, Sénat, 2013-2014, 10 octobre 2013, nº 5-118, p. 63

Proposition de budget pour l'année 2014 de la Commission administrative chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données par les services de renseignement et de sécurité (Commission BIM – C-BIM), *Doc. parl.*, Sénat, 2013-2014, nºs 5-2312/2 et 5-2312/3

Chambre des Représentants

Examen de l'équilibre linguistique à l'armée, *Doc. parl.*, Chambre, 2012-2013, nº 53-2631/001

Proposition de résolution visant à renforcer le screening des candidats et des membres civils et militaires de la Défense, et à renforcer les moyens du Service général du renseignement et de la sécurité (SGRS), *Doc. parl.*, Chambre, 2012-2013, nº 53-2641/001

Proposition visant à instituer une commission d'enquête parlementaire chargée d'examiner les cas dans lesquels le Service de la Sûreté de l'État surveille des hommes ou femmes politiques élus, *Doc. parl.*, Chambre, 2012-2013, nº 53-2652/001

Proposition de loi modifiant la loi du 27 mars 2003 relative au recrutement des militaires et au statut des musiciens militaires et modifiant diverses lois applicables au personnel de la Défense, *Doc. parl.*, Chambre, 2012-2013, nº 53-2569/002

Auditions sur l'évaluation de la loi du 19 juillet 1991 organisant la profession de détective privé, *Doc. parl.*, Chambre, 2012-2013, nº 53-2711/001

Projet de loi complétant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, en vue d'élargir la compétence de contrôle de la Cellule de traitement des informations financières en ce qui concerne l'extrémisme, *Doc. parl.*, Chambre, 2012-2013, nº 53-2817/001

Projet de loi portant des dispositions urgentes en matière de lutte contre la fraude (2763/1-11), *Ann. parl.*, Chambre, 2012-2013, 29 mai 2013, nº 53-144, p. 19

Proposition de loi visant à punir plus sévèrement les personnes appelant à la haine ou à la violence dans l'intention de porter atteinte aux droits et libertés garantis par l'État, *Doc. parl.*, Chambre, 2012-2013, nº 53-2832/001

Projet de loi modifiant la loi du 5 février 2007 relative à la sûreté maritime, *Doc. parl.*, Chambre, 2012-2013, nºs 53-2897/001 et 53-2897/003

Proposition de résolution visant à instaurer un Centre pour la cybersécurité en Belgique, *Doc. parl.*, Chambre, 2012-2013, nº 53-2918/001

Projet de loi portant modification des articles 2, 126 et 145 de la loi du 13 juin 2005 relative aux communications électroniques et de l'article 90*decies* du Code d'instruction criminelle, *Doc. parl.*, Chambre, 2012-2013, nos 53-2921/001, 53-2921/003, 53-2921/004, 53-2921/005 et 53-2921/006

Projet de loi contenant le budget des Voies et Moyens de l'année budgétaire 2014, projet de loi contenant le budget général de dépenses pour l'année budgétaire 2014, *Doc. parl.*, Chambre, 2013-2014, no 53-3070/007

Projet du budget général des dépenses pour l'année budgétaire 2014, *Doc. parl.*, Chambre, 2013-2014, nos 53-3071/001, 53-3071/008, 53-3071/021, 53-3071/024, 53-3071/027 et 53-3071/036

Justification du budget général des dépenses pour l'année budgétaire 2014, *Doc. parl.*, Chambre, 2013-2014, nos 53-3072/002, 53-3072/003 et 53-3072/008

Note de politique générale, Intérieur, *Doc. parl.*, Chambre, 2013-2014, no 53-3096/010

Projet de loi modifiant la loi sur la fonction de police, la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel et le Code d'instruction et criminelle, *Doc. parl.*, Chambre, 2013-2014,

nos 53-3105/001 à 53-3105/008 et *Ann. parl.*, Chambre, 2013-2014, 28 novembre 2013, n° 53-171, p. 43

Projet de loi modifiant diverses lois suite à la réforme du Sénat, *Doc. parl.*, Chambre, 2013-2014, nos 53-3192/001 et 53-3192/004

Projet de loi modifiant la loi du 10 avril 1990 réglementant la sécurité privée et particulière, *Doc. parl.*, Chambre, 2013-2014, n° 53-3224/001

Cour des comptes, Cour constitutionnelle, Conseil supérieur de la Justice, Comités permanents de contrôle des services de police et de renseignements, Médiateurs fédéraux, Commission pour la protection de la vie privée et Commissions de nomination pour le notariat – comptes de l'année budgétaire 2012 – ajustements du budget 2013 – propositions budgétaires pour l'année 2014, *Doc. parl.*, Chambre, 2013-2014, nos 53-3237/001 et 53-3237/002 et *Ann. parl.*, Chambre, 2013-2014, 17 décembre 2013, n° 53-175, p. 60 et *Ann. parl.*, Chambre, 2013-2014, 18 décembre 2013, n° 53-176, p. 11

Audition de M. Jean-Claude Delepière, président de la Cellule de Traitement des Informations Financières, *Doc. parl.*, Chambre, 2013-2014, n° 53-3269/001

ANNEXE C.
APERÇU DES INTERPELLATIONS, DES DEMANDES D'EXPLICATIONS ET DES QUESTIONS ORALES ET ÉCRITES RELATIVES AUX COMPÉTENCES, AU FONCTIONNEMENT ET AU CONTRÔLE DES SERVICES DE RENSEIGNEMENT ET DE SÉCURITÉ ET DE L'OCAM (1er JANVIER 2013 AU 31 DÉCEMBRE 2013)

Sénat

Question orale d'A. Van dermeersch à la ministre de l'Intérieur sur 'les attentats terroristes possibles du groupe islamique AQMI' (*Ann. parl.*, Sénat, 2012-2013, 17 janvier 2013, n° 5-88, p. 8, Q. n° 5-793)

Question écrite d'Y. Vastersavendts à la ministre de l'Intérieur sur 'l'OCAM – services d'appui – communication – incidents de sécurité' (Sénat, 2012-2013, 18 janvier 2013, Q. n° 5-7802)

Question écrite d'Y. Vastersavendts à la ministre de la Justice sur 'l'Organe de coordination pour l'analyse de la menace (OCAM) – services d'appui – communication – incidents de sécurité' (Sénat, 2012-2013, 18 janvier 2013, Q. n° 5-7803)

Question écrite d'Y. Vastersavendts à la ministre de la Justice sur 'l'Organe de coordination pour l'analyse de la menace (OCAM) – analyse de risques – bâtiment du Conseil européen' (Sénat, 2012-2013, 18 janvier 2013, Q. n° 5-7805)

Question écrite d'Y. Vastersavendts au secrétaire d'État aux Réformes institutionnelles sur 'l'Organe de coordination pour l'analyse de la menace (OCAM) – analyse de risques – bâtiment du Conseil européen' (Sénat, 2012-2013, 18 janvier 2013, Q. n° 5-7806)

Question écrite d'Y. Vastersavendts à la ministre de la Justice sur la 'lutte contre l'extrémisme sur internet – Projet « Clean IT » – obligation de notification – données des clients – contrôles des médias sociaux – participation démocratique au projet – protection de la vie privée – position du gouvernement' (Sénat, 2012-2013, 21 janvier 2013, Q. n° 5-7821)

Question écrite de J. Ceder à la ministre de la Justice sur le 'Baron Benoît de Bonvoisin – dommages et intérêts – note de la Sûreté de l'État – appel' (Sénat, 2012-2013, 23 janvier 2013, Q. n° 5-7917)

Question orale de J. Ceder à la ministre de la Justice sur 'les rapports de la Sûreté de l'État au sujet de parlementaires' (*Ann. parl.*, Sénat, 2012-2013, 7 février 2013, n° 5-91, p. 30, Q. n° 5-834)

Question orale de F. Dewinter à la ministre de la Justice sur 'le suivi des activités des politiques par la Sûreté de l'État' (*Ann. parl.*, Sénat, 2012-2013, 7 février 2013, n° 5-91, p. 30, Q. n° 5-835)

Question orale de R. Torfs à la ministre de la Justice sur 'l'enquête de la Sûreté de l'État sur les organisations sectaires nuisibles' (*Ann. parl.*, Sénat, 2012-2013, 7 février 2013, n° 5-91, p. 30, Q. n° 5-847)

Question orale de B. Anciaux à la ministre de la Justice sur 'l'aide fournie par la Belgique à la CIA lors de la mise en œuvre du programme de détention et d'interrogatoires musclés' (*Ann. parl.*, Sénat, 2012-2013, 7 février 2013, n° 5-91, p. 47, Q. n° 5-839)

Question écrite de K. Vanlouwe au secrétaire d'État à la Fonction publique sur le 'projet de cyberdéfense – cyberstratégie fédérale – relations de coopération – normes de sécurité – Disaster Recovery Plan – personnel – proactivité – Fedict – cyberattaques' (Sénat, 2012-2013, 19 février 2013, Q. n° 5-8183)

Question écrite de K. Vanlouwe au ministre de l'Économie sur le 'projet de cyberdéfense – CERT (Cyber Emergency Team fédérale) – normes de sécurité – Disaster Recovery Plan – relations de coopération – personnel – proactivité – cyberattaques – cyberespionnage industriel' (Sénat, 2012-2013, 19 février 2013, Q. n° 5-8186)

Question écrite de K. Vanlouwe au premier ministre sur le 'projet de cyberdéfense – Coordination fédérale par le premier ministre – personnel – proactivité – cyberattaques – cyberespionnage – plan d'action de l'Union européenne contre les

cyberattaques – Disaster Recovery Plan' (Sénat, 2012-2013, 19 février 2013, Q. n° 5-8212)

Question écrite de K. Vanlouwe au ministre de la Défense sur le 'projet de cyberdéfense – relations de coopération – Disaster Recovery Plan – personnel – proactivité – cyberattaques – CERT – NCIRC – Benelux' (Sénat, 2012-2013, 19 février 2013, Q. n° 5-8213)

Demande d'explications de B. Anciaux à la ministre de l'Intérieur sur 'l'incendie criminel dans un centre culturel kurde à Genk' (*Ann. parl.*, Sénat, 2012-2013, 19 février 2013, n° 5-206, p. 13, Q. n° 5-2944)

Demande d'explications de G. Deprez à la ministre de l'Intérieur sur 'la police et les réseaux sociaux' (*Ann. parl.*, Sénat, 2012-2013, 19 février 2013, n° 5-206, p. 14, Q. n° 5-2931)

Question orale de F. Dewinter à la ministre de la Justice sur 'le suivi des politiques par la Sûreté de l'État et le contrôle de ce service' (*Ann. parl.*, Sénat, 2012-2013, 21 février 2013, n° 5-92, p. 16, Q. n° 5-850)

Question orale de K. Vanlouwe au secrétaire d'État aux Affaires sociales sur 'la cyberattaque MiniDuke visant les ordinateurs des pouvoirs publics' (*Ann. parl.*, Sénat, 2012-2013, 28 février 2013, n° 5-93, p. 19, Q. n° 5-871)

Question orale d'A. De Decker à la ministre de la Justice sur 'les effectifs et les moyens de la Sûreté de l'État' (*Ann. parl.*, Sénat, 2012-2013, 7 mars 2013, n° 5-94, p. 27, Q. n° 5-888)

Question écrite de B. Anciaux à la ministre de la Justice sur 'la Sûreté de l'État – conservation des informations – banque de données – informations inexactes – utilisation – légalité' (Sénat, 2012-2013, 8 mars 2013, Q. n° 5-8421)

Question écrite de M. Taelman à la ministre de la Justice sur 'les prêcheurs de haine – nombre – liste – poursuites et condamnations – jihad – Syrie' (Sénat, 2012-2013, 8 mars 2013, Q. n° 5- 8436)

Question écrite de K. Vanlouwe à la ministre de la Justice sur 'le fonctionnement de la Computer Emergency Response Team' (Sénat, 2012-2013, 14 mars 2013, Q. n° 5-8500)

Question orale de D. Pieters à la ministre de la Justice sur 'la Sûreté de l'État et les politiques' (*Ann. parl.*, Sénat, 2012-2013, 14 mars 2013, n° 5-95, p. 17, Q. n° 5-902)

Question orale de J.-J. De Gucht à la ministre de l'Intérieur sur 'l'augmentation du niveau d'alarme terroriste' (*Ann. parl.*, Sénat, 2012-2013, 21 mars 2013, n° 5-96, p. 27, Q. n° 5-919)

Question orale de F. Dewinter au ministre des Affaires étrangères sur 'les djihadistes « belges » qui se battent en Syrie' (*Ann. parl.*, Sénat, 2012-2013, 21 mars 2013, n° 5-96, p. 27, Q. n° 5-920)

Question orale de B. Laeremans à la ministre de la Justice sur 'les tergiversations de la Justice dans le dossier d'un terroriste bruxellois' (*Ann. parl.*, Sénat, 2012-2013, 28 mars 2013, n° 5-97, p. 31, Q. n° 5-932)

Demande d'explications de R. Miller à la ministre de l'Intérieur sur 'les ressortissants belges combattant en Syrie et le Plan Radicalisme' (*Ann. parl.*, Sénat, 2012-2013, 16 avril 2013, n° 5-216, p. 22, Q. n° 5-3344)

Demande d'explications de B. Anciaux à la ministre de l'Intérieur sur 'les jeunes Belges qui se battent en Syrie et puis retournent en Belgique' (*Ann. parl.*, Sénat, 2012-2013, 16 avril 2013, n° 5-216, p. 22, Q. n° 5-3295)

Question écrite de B. Anciaux à la ministre de l'Intérieur sur 'les conséquences de la cyberattaque MiniDuke sur les ordinateurs des autorités belges' (Sénat, 2012-2013, 19 avril 2013, Q. n° 5-8738)

Question orale de B. Laeremans à la ministre de la Justice sur 'la protection des dirigeants religieux et la garantie de la liberté d'expression' (*Ann. parl.*, Sénat, 2012-2013, 25 avril 2013, n° 5-99, p. 23, Q. n° 5-962)

Question orale de K. Vanlouwe au secrétaire d'État à la Fonction publique sur 'la cyberstratégie et le rôle de Fedict' (*Ann. parl.*, Sénat, 2012-2013, 25 avril 2013, n° 5-99, p. 37, Q. n° 5-957)

Question écrite de N. Lijnen au ministre de la Défense sur les 'cyberguerres – Nations Unies – manuel – utilisation' (Sénat, 2012-2013, 7 mai 2013, Q. n° 5-8972)

Question écrite de M.Taelman à la ministre de l'Intérieur sur la 'vie privée – réclamation de données d'utilisateurs des médias sociaux – Police – Sûreté de l'État – Service général du renseignement et de la sécurité – protection juridique – accords –situation (Sénat, 2012-2013, 23 mai 2013, Q. n° 5-9086)

Demande d'explications de B. Laeremans à la ministre de la Justice sur 'la difficile lutte contre la cybercriminalité' (*Ann. parl.*, Sénat, 2012-2013, 29 mai 2013, n° 5-227, p. 9, Q. n° 5-3508)

Question orale de B. Laeremans à la ministre de la Justice sur 'la radicalisation dans les milieux marocains et le risque accru d'attentats en Belgique' (*Ann. parl.*, Sénat, 2012-2013, 30 mai 2013, n° 5-105, non disponible pour l'instant, Q. n°5-1022)

Question orale de H. Bousetta à la ministre de la Justice sur 'le programme PRISM et la protection de la vie privée' (*Ann. parl.*, Sénat, 2012-2013, 13 juin 2013, n° 5-107, p. 25, Q. n° 5-1042)

Question orale de F. Piryns à la ministre de la Justice sur 'le programme PRISM et la protection de la vie privée' (*Ann. parl.*, Sénat, 2012-2013, 13 juin 2013, n° 5-107, p. 25, Q. n° 5-1049)

Question orale de B. Hellings à la ministre de l'Intérieur sur 'la nouvelle arrestation d'un activiste belge' (*Ann. parl.*, Sénat, 2012-2013, 20 juin 2013, n° 5-108, p. 12, Q. n° 5-1063)

Question orale de G. Deprez à la ministre de l'Intérieur sur 'la banque de données nationale générale' (*Ann. parl.*, Sénat, 2012-2013, 20 juin 2013, n° 5-108, p. 15, Q. n° 5-1066)

Demande d'explications de G. De Padt à la ministre de l'Intérieur sur 'la réforme de la banque de données nationale générale' (*Ann. parl.*, Sénat, 2012-2013, 2 juillet 2013, n° 5-238, p. 7, Q. n°5-3619)

Demande d'explications de K. Vanlouwe à la ministre de la Justice sur 'le projet PRISM des services de sécurité américains et l'espionnage numérique des utilisateurs d'internet' (*Ann. parl.*, Sénat, 2012-2013, 3 juillet 2013, n° 5-239, p. 10, Q. n° 5-3708)

Demande d'explications de K. Vanlouwe au ministre des Affaires étrangères sur 'le projet PRISM des services de sécurité américains et l'espionnage numérique des utilisateurs d'internet' (*Ann. parl.*, Sénat, 2012-2013, 3 juillet 2013, n° 5-239, p. 10, Q. n° 5-3711)

Question écrite de K. Vanlouwe au secrétaire d'État à la Fonction publique sur 'la cybersécurité et la cyberdéfense' (Sénat, 2012-2013, 10 juillet 2013, Q. n° 5-9407)

Question écrite de B. Anciaux à la ministre de la Justice sur le 'terrorisme – liste belge de personnes et d'organisations suspectes – procédure – publicité – liaison avec d'autres listes – protection juridique' (Sénat, 2012-2013, 10 juillet 2013, Q. n° 5-9522)

Question écrite de B. Anciaux à la ministre de la Justice sur 'le rôle de la Sûreté de l'État dans le scandale des écoutes' (Sénat, 2012-2013, 19 juillet 2013, Q. n° 5-9634)

Question écrite de B. De Nijn au ministre des Affaires étrangères sur 'Kenya – Al-Shabaab – Somalie – combattants belges du Jihad – aperçu – confiscation de passeports – groupes de recrutement – retour' (Sénat, 2012-2013, 2 octobre 2013, Q. n° 5-9962)

Question orale de F. Dewinter à la ministre de l'Intérieur sur 'la liste des organisations surveillées' (*Ann. parl.*, Sénat, 2013-2014, 24 octobre 2013, n° 5-121, p. 24, Q. n° 5-1131)

Question écrite de M. Taelman au ministre des Affaires étrangères sur 'l'Agence pour la sécurité nationale (National Security Agency, NSQ) – espionnage industriel – mise sur écoute du personnel de l'entreprise – Sûreté de l'État – mesures' (Sénat, 2013-2014, 31 octobre 2013, Q. n° 5-10260)

Question écrite de M. Taelman au premier ministre sur 'National Security Agency – Belgacom – Swift – écoutes – piratage informatique – aperçu – enquête – mesures' (Sénat, 2013-2014, 31 octobre 2013, Q. n° 5-10284)

Demande d'explications de B. Hellings à la ministre de l'Intérieur sur 'le futur réseau de télécommunications des services de sécurité' (*Ann. parl.*, Sénat, 2013-2014, 5 novembre 2013, n° 5-254, p. 10, Q. n° 5-3895)

Question orale de B. Hellings au ministre de la Défense sur 'l'usage potentiel par le Service général du renseignement et de la sécurité des outils de surveillance de la NSA dans le cadre de la mission de l'armée belge en Afghanistan' (*Ann. parl.*, Sénat, 2013-2014, 14 novembre 2013, n° 5-123, p. 11, Q. n° 5-1164)

Demande d'explications de R. Miller à la ministre de la Justice sur 'le statut juridique des prisonniers' (*Ann. parl.*, Sénat, 2013-2014, 20 novembre 2013, n° 5-159, p. 39, Q. n° 5-4222)

Question orale de F. Dewinter à la ministre de l'Intérieur sur 'la photo diffusée sur internet où la ministre pose avec un salafiste, membre d'Al-Qaida' (*Ann. parl.*, Sénat, 2013-2014, 5 décembre 2013, n° 5-129, p. 12, Q. n° 5-1209)

Chambre des Représentants

Question de M. Doomst à la ministre de la Justice sur 'la cybercriminalité' (*C.R.I.*, Chambre, 2012-2013, 10 janvier 2013, PLEN 124, p. 57, Q. n° 1422)

Questions jointes de B. Schoofs et P. Luykx à la ministre de l'Intérieur sur 'les violences qui ont éclaté à la suite d'une manifestation pro-kurde à Genk' (*C.R.I.*, Chambre, 2012-2013, 24 janvier 2013, PLEN 126, p. 44, Q. n°s 1471 et 1472)

Question de P. Dedecker à la ministre de l'Intérieur sur la 'cybersécurité' (*Q.R.*, Chambre, 2012-2013, 28 janvier 2013, n° 098, p. 46, Q. n° 714)

Question de B. Slegers à la ministre de la Justice sur la 'Sûreté de l'État – moyens budgétaires limités' (*Q.R.*, Chambre, 2012-2013, 28 janvier 2013, n° 098, p. 60, Q. n° 770)

Question de P. Logghe au ministre des Finances sur le 'blanchiment d'argent' (*Q.R.*, Chambre, 2012-2013, 28 janvier 2013, n° 098, p. 104, Q. n° 668)

Question de K. Grosemans au ministre de la Défense sur 'les origines militaires des Special Forces' (*Q.R.*, Chambre, 2012-2013, 28 janvier 2013, n° 098, p. 268, Q. n° 363)

Question de N. Lanjri à la ministre de la Justice sur 'les compétences et l'avenir de l'Exécutif des musulmans de Belgique' (*C.R.I.*, Chambre, 2012-2013, 30 janvier 2013, COM 658, p. 6, Q. n° 15265)

Questions jointes de J. Galant et D. Ducarme à la ministre de la Justice sur 'le contrôle des écoles islamiques implantées en Belgique' (*C.R.I.*, Chambre, 2012-2013, 30 janvier 2013, COM 658, p. 35, Q. nos 15448 et 15518)

Questions jointes de D. Ducarme, A. Ponthier et G. Dallemagne au ministre de la Défense sur 'la présence d'extrémistes au sein de l'armée' (*C.R.I.*, Chambre, 2012-2013, 17 février 2013, PLEN 125, p. 26, Q. nos 1442, 1443 et 1444)

Questions jointes de M. Doomst, P. Logghe, C. Van Cauter, G. Dallemagne, S. Van Hecke, B. Schoofs, K. Degroote en M. Jabour à la ministre de la Justice sur 'la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 7 février 2013, COM 666, p. 1, Q. nos 15667, 15671, 15693, 15705, 15706, 15730, 15739 et 15767)

Question de Z. Génot à la ministre de la Justice sur 'le suivi des recommandations de la commission 'Lumumba'' (*C.R.I.*, Chambre, 2012-2013, 20 février 2013, COM 678, p. 35, Q. no 15688)

Question de G. Dallemagne au premier ministre sur 'le pillage de données et le sabotage d'une entreprise belge par la Chine' (*C.R.I.*, Chambre, 2012-2013, 21 février 2013, PLEN 132, p. 19, Q. no 1534)

Questions jointes de B. Schoofs, K. Degroote et M. Doomst à la ministre de l'Intérieur sur 'le fonctionnement de la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 21 février 2013, PLEN 132, p. 27, Q. nos 1535, 1536 et 1537)

Questions jointes de K. Degroote, M. Doomst, C. Van Cauter, S. Van Hecke, B. Weyts et B. Schoofs à la ministre de la Justice sur 'la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 26 février 2013, COM 682, p. 1, Q. nos 15873, 15876, 15882, 15896, 15934 et 15983)

Questions jointes de K. Lalieux, L. Van Biesen et T. Veys au secrétaire d'État à l'Environnement sur 'la sécurité à l'aéroport de Bruxelles-National' (*C.R.I.*, Chambre, 2012-2013, 13 mars 2013, COM 689, p. 19, Q. nos 16011, 16038 et 16355)

Question de K. Grosemans au ministre de la Défense sur 'la participation au programme MUSIS' (*C.R.I.*, Chambre, 2012-2013, 13 mars 2013, COM 691, p. 4, Q. no 16186)

Questions jointes de B. Valkeniers et D. Ducarme à la ministre de la Justice sur 'de jeunes Belges agissant comme mercenaires pour les intégristes musulmans en Syrie' (*C.R.I.*, Chambre, 2012-2013, 13 mars 2013, COM 698, p. 4, Q. nos 16484, 16485 et 16587)

Questions jointes de B. Slegers, P. Logghe et S. Van Hecke à la ministre de la Justice sur 'la banque de données de la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 13 mars 2013, COM 698, p. 9, Q. nos 16457, 16487 et 16524)

Questions jointes de P. Logghe, B. Somers et B. Weyts à la ministre de l'Intérieur sur 'la participation de jeunes Belges aux combats en Syrie et la menace terroriste dans notre pays' (*C.R.I.*, Chambre, 2012-2013, 14 mars 2013, PLEN 135, p. 5, Q. nos 1601, 1602 et 1603)

Question de P. Logghe à la ministre de la Justice sur 'les terroristes musulmans et la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 20 mars 2013, COM 703, p. 6, Q. no 16711)

Question de J. Van Esbroeck à la ministre de l'Intérieur sur 'l'adaptation du niveau de la menace' (*Q.R.*, Chambre, 2012-2013, 25 mars 2013, n° 106, p. 146, Q. n° 711)

Questions jointes d'O. Maingain et E. Thiébaut à la ministre de l'Intérieur sur 'l'affaire Benladghem' (*C.R.I.*, Chambre, 2012-2013, 28 mars 2013, PLEN 137, p. 32, Q. nos 1660 et 1662)

Question de T. Francken au ministre de la Défense sur 'les officiers généraux qui ne remplissent aucune fonction' (*Q.R.*, Chambre, 2012-2013, 2 avril 2013, n° 107, p. 98, Q. n° 414)

Question de D. Thiéry au secrétaire d'État à la Fonction publique sur 'les mesures prises afin de lutter contre les cybersabotages' (*Q.R.*, Chambre, 2012-2013, 2 avril 2013, n° 107, p. 284, Q. n° 61)

Question de B. Valkeniers au ministre des Affaires étrangères sur le 'monitoring des avis eurocritiques' (*Q.R.*, Chambre, 2012-2013, 12 avril 2013, n° 108, p. 422, Q. n° 424)

Question de P. Dedecker à la ministre de l'Intérieur sur la 'cybersécurité' (*Q.R.*, Chambre, 2012-2013, 12 avril 2013, n° 108, p. 503, Q. n° 714)

Questions jointes de P. Logghe et W.-F. Schiltz à la ministre de l'Intérieur sur 'le vol de diamants à l'aéroport de Zaventem' (*C.R.I.*, Chambre, 2012-2013, 16 avril 2013, COM 713, p. 24, Q. n^{os} 16053 et 16535)

Question et interpellation jointes de Ch. Lacroix et K. Grosemans au ministre de la Défense sur 'les ambitions de l'armée belge en matière d'imagerie satellitaire' (*C.R.I.*, Chambre, 2012-2013, 16 avril 2013, COM 714, p. 6, Q. n^{o} 16482 et 85)

Question de K. Grosemans au ministre de la Défense sur 'la fuite lors d'une audition à huis clos' (*C.R.I.*, Chambre, 2012-2013, 16 avril 2013, COM 714, p. 21, Q. n^{os} 16826)

Questions jointes de D. Ducarme, B. Somers et B. Schoofs à la ministre de la Justice sur 'la persistance d'absence de sanctions légales à l'encontre des Belges recrutés et s'engageant individuellement en vue de participer au conflit syrien' (*C.R.I.*, Chambre, 2012-2013, 17 avril 2013, COM 718, p. 6, Q. n^{os} 16917, 17256 et 17279)

Questions jointes de B. Clerfayt, F. De Man, H. Bonte, L. Devin, B. Slegers, B. Weyts et J. M. Dedecker au premier ministre su 'les jeunes Belges partis combattre en Syrie' (*C.R.I.*, Chambre, 2012-2013, 18 avril 2013, PLEN 138, p. 22, Q. n^{os} 1679 à 1685)

Question de B. Slegers à la ministre de la Justice sur la 'Sûreté de l'État – moyens budgétaires limités' (*Q.R.*, Chambre, 2012-2013, 19 avril 2013, n° 109, p. 203, Q. n° 770)

Question de K. Grosemans au ministre de la Défense sur 'le point de vue de la Défense en ce qui concerne le programme MUSIS' (*C.R.I.*, Chambre, 2012-2013, 24 avril 2013, COM 723, p. 15, Q. n^{o} 17386)

Question de S. Van Hecke à la ministre de la Justice sur 'les conditions de travail à la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 24 avril 2013, COM 725, p. 2, Q. n^{o} 17123)

Question de S. De Wit à la ministre de l'Intérieur sur la 'connaissance des langues au sein des services d'appui de la police' (*Q.R.*, Chambre, 2012-2013, 26 avril 2013, n° 110, p. 131, Q. n° 21)

Questions jointes de T. Francken à la ministre de la Justice sur 'le droit de consultation par le Roi de documents secrets de la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 30 avril 2013, COM 732, p. 17, Q. n^{os} 17559 et 17577)

Questions jointes de D. Ducarme à la ministre de la Justice sur 'Sharia4Belgium, le retour de Belges de Syrie recrutés et engagés dans les combats en Syrie et le transfert d'information au départ de la Justice vers le département des Affaires étrangères' (*C.R.I.*, Chambre, 2012-2013, 30 avril 2013, COM 732, p. 19, Q. n^{os} 17586 et 17587)

Question de K. Grosemans au ministre de la Défense sur la 'détection de logiciels malveillants (malware) dans les systèmes informatiques de la Défense' (*Q.R.*, Chambre, 2012-2013, 6 mai 2013, n° 111, p. 64, Q. n° 441)

Questions jointes de T. Francken, W. De Vriendt, D. Van der Maelen et Ph. Blanchart au ministre de la Défense sur 'l'accord de livraison d'armes conclu par la Défense' (*C.R.I.*, Chambre, 2012-2013, 8 mai 2013, PLEN 141, p. 15, Q. nos 1738, 1739, 1740 et 1741)

Question de D. Ducarme à la ministre de la Justice sur 'le manque de moyens de la Sûreté de l'État' (*C.R.I.*, Chambre, 2012-2013, 8 mai 2013, PLEN 141, p. 15, Q. no 1747)

Question de B. Pas à la ministre de l'Intérieur sur 'les menaces proférées par Sharia4UK' (*C.R.I.*, Chambre, 2012-2013, 16 mai 2013, PLEN 142, p. 20, Q. no 1768)

Questions jointes de D. Ducarme, W. De Vriendt, D. Geerts et A. Ponthier au ministre de la Défense sur 'le contrôle à opérer par la Défense nationale et notre gouvernement sur la revente de matériel militaire' (*C.R.I.*, Chambre, 2012-2013, 21 mai 2013, COM 750, p. 17, Q. nos 17801, 17873, 17898 et 18001)

Question de G. Dallemagne au ministre de la Défense sur 'les cyberattaques' (*C.R.I.*, Chambre, 2012-2013, 21 mai 2013, COM 750, p. 24, Q. no 17925)

Questions jointes de D. Ducarme et P. Logghe à la ministre de l'Intérieur sur 'le retour des ex-djihadistes belges de Syrie' (*C.R.I.*, Chambre, 2012-2013, 23 mai 2013, PLEN 143, p. 13, Q. nos 1784 et 1785)

Question de B. Weyts à la ministre de l'Intérieur sur les 'islamistes radicaux en Syrie' (*Q.R.*, Chambre, 2012-2013, 27 mai 2013, n° 114, p. 48, Q. n° 860)

Question de P. Dedecker au secrétaire d'État à la Fonction publique sur la 'cybersécurité' (*Q.R.*, Chambre, 2012-2013, 27 mai 2013, n° 114, p. 325, Q. n° 125)

Questions jointes de K. Grosemans et A. Ponthier au ministre de la Défense sur 'la critique du Comité R relative au manque de contrôle de l'unité ISTAR' (*C.R.I.*, Chambre, 2012-2013, 29 mai 2013, COM 760, p. 8, Q. nos 18156 et 18164)

Questions jointes de L. Van Biesen, B. Slegers et P. Logghe à la ministre de l'Intérieur sur 'la menace de Sharia4UK' (*C.R.I.*, Chambre, 2012-2013, 29 mai 2013, COM 761, p. 35, Q. nos 17926, 17933, 18007 et 18050)

Question de P. Logghe à la ministre de l'Intérieur sur la 'radicalisation de jeunes musulmans – influence/renseignements en provenance de l'Arabie saoudite, de la Tchétchénie et du Qatar' (*Q.R.*, Chambre, 2012-2013, 3 juin 2013, n° 115, p. 60, Q. n° 891)

Question de D. Ducarme à la ministre de la Justice sur 'le suivi judiciaire produit à l'encontre de Belges de retour de Syrie ayant pris part aux combats' (*C.R.I.*, Chambre, 2012-2013, 11 juin 2013, COM 773, p. 14, Q. no 18227)

Question de D. Ducarme à la ministre de la Justice sur 'les menaces à caractère terroriste proférées par Sharia4UK à l'encontre de la Belgique' (*C.R.I.*, Chambre, 2012-2013, 11 juin 2013, COM 773, p. 15, Q. no 18382)

Questions jointes de J. Van Esbroeck et P. Logghe à la ministre de l'Intérieur sur 'les combattants qui reviennent de Syrie' (*C.R.I.*, Chambre, 2012-2013, 13 juin 2013, PLEN 148, p. 21, Q. nos 1857 et 1858)

Question de I. Emmery au ministre des Affaires étrangères sur 'le programme PRISM des services secrets américains' (*C.R.I.*, Chambre, 2012-2013, 13 juin 2013, PLEN 148, p. 54, Q. no 1861)

Question de P. Logghe à la ministre de l'Intérieur sur 'les combattants musulmans en Syrie et les informations les concernant' (*Q.R.*, Chambre, 2012-2013, 17 juin 2013, n° 117, p. 70, Q. n° 929)

Question de K. Grosemans au ministre de la Défense sur 'les recommandations du Comité R concernant le fonctionnement du SGRS' (*Q.R.*, Chambre, 2012-2013, 17 juin 2013, n° 117, p. 161, Q. n° 474)

Question de F. De Man à la ministre de l'Intérieur sur 'la discrétion entourant les dossiers de djihadistes partis combattre en Syrie' (*C.R.I.*, Chambre, 2012-2013, 20 juin 2013, PLEN 150, p. 10, Q. n° 1880)

Question de G. Dallemagne à la ministre de la Justice sur 'le programme PRISM' (*C.R.I.*, Chambre, 2012-2013, 20 juin 2013, PLEN 150, p. 27, Q. n° 1887)

Question de B. Weyts à la ministre de l'Intérieur sur le 'Centre de Crise – traitement de dossiers de personnes menacées' (*Q.R.*, Chambre, 2012-2013, 24 juin 2013, n° 118, p. 172, Q. n° 824)

Question d'A. Frédéric à la ministre des Affaires sociales sur 'le rapport français relatif aux sectes thérapeutiques' (*Q.R.*, Chambre, 2012-2013, 1er juillet 2013, n° 119, p. 161, Q. n° 1005)

Questions jointes de H. De Croo, T. Francken, J. Fernandez Fernandez et S. Van Hecke à la ministre de l'Intérieur sur 'l'espionnage américain à grande échelle' (*C.R.I.*, Chambre, 2012-2013, 3 juillet 2013, COM 795, p. 2, Q. nos 18510, 18525, 18693, 19037, 19071 et 19075)

Questions jointes de T. Francken à la ministre de la Justice sur 'l'enquête judiciaire sur les éventuels actes de terrorisme commis par des personnes provenant du milieu anarchiste bruxellois' (*C.R.I.*, Chambre, 2012-2013, 3 juillet 2013, COM 795, p. 38, Q. nos 18734 et 18735)

Questions jointes de P. Logghe à la ministre de l'Intérieur sur 'les flux financiers internationaux dans le cadre du terrorisme' (*C.R.I.*, Chambre, 2012-2013, 3 juillet 2013, COM 795, p. 42, Q. nos 18756 et 18918)

Questions jointes de B. Schoofs à la ministre de la Justice sur 'les avis émis par le Conseil des Théologues de l'Exécutif des musulmans' (*C.R.I.*, Chambre, 2012-2013, 3 juillet 2013, COM 795, p. 45, Q. nos 18760 et 18785)

Questions jointes d'O. Henry, H. De Croo et D. Van der Maelen au ministre des Affaires étrangères sur 'le programme PRISM' (*C.R.I.*, Chambre, 2012-2013, 4 juillet 2013, PLEN 154, p. 8, Q. nos 1925, 1935 et 1926)

Questions jointes de P. Logghe et J. Van Esbroeck à la ministre de l'Intérieur sur 'le nombre d'intégristes musulmans dans notre pays' (*C.R.I.*, Chambre, 2012-2013, 9 juillet 2013, COM 800, p. 25, Q. nos 18161 et 18215)

Questions jointes de J. Van Esbroeck, B. Slegers, P. Logghe et D. Ducarme à la ministre de l'Intérieur sur 'les divergences dans le cadre de la task force Syrie' (*C.R.I.*, Chambre, 2012-2013, 9 juillet 2013, COM 800, p. 44, Q. nos 18699, 18942, 19030 et 19073)

Questions jointes de K. Grosemans, Ch. Lacroix et T. Francken au ministre de la Défense sur 'le programme PRISM' (*C.R.I.*, Chambre, 2012-2013, 9 juillet 2013, COM 801, p. 16, Q. nos 18527, 18588 et 19070)

Interpellation de F. De Man au ministre de la Défense sur 'l'information selon laquelle un fondamentaliste musulman, formé par l'armée belge, aurait été tué en Syrie' (*C.R.I.*, Chambre, 2012-2013, 9 juillet 2013, COM 801, p. 31, Q. n° 99)

Question de P. Dedecker au secrétaire d'État à la Fonction publique sur 'l'espionnage d'entreprises IT par le gouvernement américain' (*Q.R.*, Chambre, 2012-2013, 22 juillet 2013, n° 122, p. 228, Q. n° 159)

Question de B. Schoofs à la ministre de la Justice sur 'les activités de la Sûreté de l'État' (*Q.R.*, Chambre, 2012-2013, 29 juillet 2013, n° 123, p. 182, Q. n° 841)

Question de G. Dallemagne au Premier ministre sur 'les cyberattaques chinoises' (*Q.R.*, Chambre, 2012-2013, 19 août 2013, n° 124, p. 389 Q. n° 95)

Question de S. Van Hecke à la ministre de la Justice sur 'la cybersécurité' (*C.R.I.*, Chambre, 2012-2013, 24 septembre 2013, COM 816, p. 6, Q. n° 19749)

Question de S. Van Hecke à la ministre de la Justice sur 'le suivi du programme PRISM' (*C.R.I.*, Chambre, 2012-2013, 24 septembre 2013, COM 817, p. 47, Q. n° 19643)

Questions jointes d'O. Maingain et M. Senecaut à la ministre de la Justice sur 'la plainte déposée par la société Belgacom à la suite de l'accès non autorisé à son système informatique interne' (*C.R.I.*, Chambre, 2012-2013, 2 octobre 2013, COM 824, p. 11, Q. n^{os} 19703 et 19716)

Question de P. Logghe à la ministre de l'Intérieur sur 'les djihadistes belges' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 309, Q. n° 684)

Question de J. Galant à la ministre de l'Intérieur sur 'la fusillade mortelle sur l'autoroute A8 – la découverte d'un arsenal de guerre au domicile du gangster abattu – le niveau d'alerte pour menace terroriste' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 317, Q. n° 889)

Question de P. Logge à la ministre de l'Intérieur sur la 'radicalisation de jeunes musulmans – influence/renseignements en provenance de l'Arabie saoudite, de la Tchétchénie et du Qatar' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 322, Q. n° 891)

Question de B. Slegers à la ministre de l'Intérieur sur la 'lutte contre le terrorisme – Discussions avec les autorités américaines' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 345, Q. n° 973)

Question de Ph. Blanchart à la ministre de l'Intérieur sur 'l'agence de renseignements de l'Union européenne (SitCen)' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 351, Q. n° 1118)

Question de D. Bacquelaine à la ministre de la Justice sur 'la suppression de postes de provinces de la Sûreté de l'État – le manque de moyens financiers ainsi que de personnel' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 382, Q. n° 1047)

Question d'I. De Meulenmeester au ministre des Entreprises publiques sur 'la visite de M. Labille au Rwanda en juin 2013' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 464, Q. n° 584)

Question de J. Van den Bergh au secrétaire d'État à l'Environnement sur 'les véhicules prioritaires' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 582, Q. n° 150)

Question de K. Calvo au secrétaire d'État à l'Environnement sur 'le contrôle de l'utilisateur final après exportations nucléaires au sein de l'Union européenne' (*Q.R.*, Chambre, 2012-2013, 4 octobre 2013, n° 130, p. 588, Q. n° 158)

Question de K. Grosemans au ministre de la Défense sur 'le contrôle du bataillon ISTAR' (*C.R.I.*, Chambre, 2013-2014, 9 octobre 2013, COM 826, p. 7, Q. n° 19436)

Questions jointes de K. Grosemans et Ch. Lacroix au ministre de la Défense sur 'les menaces d'attentats adressées par courrier électronique contre des militaires' (*C.R.I.*, Chambre, 2013-2014, 9 octobre 2013, COM 826, p. 9, Q. n^{os} 19449 et 19595)

Questions jointes de J. Galant, J. Van Esbroeck et B. Slegers à la ministre de l'Intérieur sur 'le contexte de sécurité renforcée et le rapport du Comité P fustigeant la gestion

des données concernant le terrorisme, le radicalisme et l'extrémisme' (*C.R.I.*, Chambre, 2013-2014, 9 octobre 2013, COM 830, p. 7, Q. nos 19452, 19473 et 19763)

Questions jointes de P. Dedecker, S. Van Hecke, R. Deseyn S. Lahaye-Battheu et T. Veys au ministre des Entreprises publiques sur 'l'espionnage chez Belgacom' (*C.R.I.*, Chambre, 2013-2014, 9 octobre 2013, COM 831, p. 29, Q. nos 19670, 105, 108, 20082, 20083, 20084, 20142 et 20154)

Question d'A. Frédéric à la ministre de l'Intérieur sur 'le rapport confidentiel de la Sûreté de l'État concernant les tentatives d'approche de l'Église de Scientologie auprès de nos politiciens' (*C.R.I.*, Chambre, 2013-2014, 23 octobre 2013, COM 839, p. 4, Q. no 19591)

Question de P. Logghe à la ministre de l'Intérieur sur 'les compétences accordées aux sociétés privées de gardiennage' (*C.R.I.*, Chambre, 2013-2014, 23 octobre 2013, COM 839, p. 10, Q. no 19679)

Questions jointes de D. Ducarme, B. Somers et P. Logghe à la ministre de l'Intérieur sur 'les camps d'entraînement djihadistes en Ardennes' (*C.R.I.*, Chambre, 2013-2014, 24 octobre 2013, PLEN 165, p. 4, Q. nos 2000, 2001 et 2002)

Questions jointes de H. De Croo, G. Dallemagne, R. Deseyn, P. Dedecker et P. Logghe à la ministre de l'Intérieur sur 'les pratiques d'écoutes' (*C.R.I.*, Chambre, 2013-2014, 24 octobre 2013, PLEN 165, p. 17, Q. nos 2010, 2011, 2012, 2013 et 2014)

Question de J. Van Esbroeck à la ministre de l'Intérieur sur 'les coûts engendrés par Sharia4Belgium' (*Q.R.*, Chambre, 2013-2014, 4 novembre 2013, n° 134, p. 148, Q. n° 700)

Question de K. Grosemans à la ministre de l'Intérieur sur la 'participation du SGRS à la visite de travail de la ministre en Turquie' (*Q.R.*, Chambre, 2013-2014, 4 novembre 2013, n° 134, p. 155, Q. n° 974)

Question de R. Deseyn à la ministre de l'Intérieur sur 'le système PRISM' (*Q.R.*, Chambre, 2013-2014, 4 novembre 2013, n° 134, p. 165, Q. n° 1012)

Question de H. Bonte au ministre de la Justice sur 'les risques inhérents à la lenteur de la Justice' (*C.R.I.*, Chambre, 2013-2014, 6 novembre 2013, COM 846, p. 24, Q. no 20597)

Questions jointes de J. De Potter, D. Bacquelaine, P. Logghe et J. Van Esbroeck à la ministre de l'Intérieur sur 'la radicalisation des jeunes et les mesures prises à cet égard' (*C.R.I.*, Chambre, 2013-2014, 12 novembre 2013, COM 850, p. 46, Q. nos 20399, 20410, 20412 et 20433)

Questions jointes de D. Thiéry, Ch. Lacroix et D. Ducarme au ministre de la Défense sur 'la collaboration des services de renseignement américains dans notre cyberdéfense militaire' (*C.R.I.*, Chambre, 2013-2014, 13 novembre 2013, COM 851, p. 1, Q. nos 19438, 19875, 20643 et 20749)

Question de P. Logghe à la ministre de de l'Intérieur sur 'des ressortissants belges dans les rangs d'Al-Shabaab' (*Q.R.*, Chambre, 2013-2014, 18 novembre 2013, n° 136, p. 78, Q. n° 1186)

Question de G. D'haeseleer à la ministre de la Justice sur 'les rémunérations ou indemnités supplémentaires perçues par les délégués syndicaux dans les comités de gestion et autres conseils/ commissions' (*Q.R.*, Chambre, 2013-2014, 18 novembre 2013, n° 136, p. 112, Q. n° 1020)

Question de Ch. Brotcorne à la ministre de la Justice sur 'la présence d'un recruteur à la prison de Mons – islam radical' (*Q.R.*, Chambre, 2013-2014, 18 novembre 2013, n° 136, p. 127, Q. n° 1059)

Questions jointes de P. Logghe et J. Van Esbroeck à la ministre de la Justice sur 'les déclarations d'un prédicateur salafiste' (*C.R.I.*, Chambre, 2013-2014, 4 décembre 2013, COM 879, p. 1, Q. n^{os} 20784 et 20807)

Questions jointes de J. Van Esbroeck et P. Logghe à la ministre de la Justice sur 'le retour de Syrie de combattants mineurs' (*C.R.I.*, Chambre, 2013-2014, 4 décembre 2013, COM 879, p. 5, Q. n^{os} 20805, 20833 et 21065)

Question de R. Deseyn au ministre de la Défense sur 'le système PRISM' (*Q.R.*, Chambre, 2013-2014, 9 décembre 2013, n° 139, p. 71, Q. n° 614)

Question de E. Brems au ministre des Affaires étrangères sur 'l'accueil de détenus de Guantanamo' (*Q.R.*, Chambre, 2013-2014, 9 décembre 2013, n° 139, p. 92, Q. n° 574)

Question de E. Brems au ministre des Affaires étrangères sur 'l'espion belgo-iranien' (*Q.R.*, Chambre, 2013-2014, 9 décembre 2013, n° 139, p. 132, Q. n° 650)

Question de P. Logghe à la ministre de l'Intérieur sur 'le départ de mineurs vers la Syrie' (*Q.R.*, Chambre, 2013-2014, 16 décembre 2013, n° 140, p. 146, Q. n° 930)

Question de P. Logghe à la ministre de la Justice sur la 'radicalisation de jeunes musulmans – influence/renseignements en provenance de l'Arabie saoudite, de la Tchétchénie et du Qatar' (*Q.R.*, Chambre, 2013-2014, 16 décembre 2013, n° 140, p. 244, Q. n° 1114)

Question de T. Francken à la ministre de la Justice sur 'le personnel de la Sûreté de l'État affecté à la protection du Roi et de son entourage' (*Q.R.*, Chambre, 2013-2014, 16 décembre 2013, n° 140, p. 271, Q. n° 1175)

Question de T. Francken au ministre de la Défense sur 'le personnel du service de sécurité militaire SGRS affecté à la protection du Roi et de son entourage' (*Q.R.*, Chambre, 2013-2014, 16 décembre 2013, n° 141, p. 194, Q. n° 621)

ANNEXE D.
PREMIER RAPPORT INTERMÉDIAIRE DE L'ENQUÊTE DE CONTRÔLE RELATIVE À LA POSITION D'INFORMATION DES SERVICES DE RENSEIGNEMENT BELGES CONCERNANT LES CAPACITÉS DE RÉCOLTE MASSIVE ET L'EXPLORATION DE MÉTA-DATA PAR CERTAINS ÉTATS ET LA MANIÈRE DONT CES ÉTATS PRATIQUERAIENT L'ESPIONNAGE POLITIQUE DE SOI-DISANT 'ÉTATS-AMIS' (PRISM)

I. INTRODUCTION

Le 6 juin 2013, *The Guardian*[197] et *The Washington Post*[198] publiaient pour la première fois des informations issues des dizaines de milliers de documents (classifiés) qui ont été divulgués par Edward Snowden, qui a rempli diverses fonctions dans ou pour des services de renseignement américains. Depuis lors, de nouvelles révélations se succèdent avec une régularité de métronome.

Les communications donnaient une vue sur des programmes extrêmement secrets, principalement de la NSA. Elles révélaient notamment l'existence du programme appelé PRISM, au travers duquel la NSA récoltait massivement des (méta)données de télécommunications, et dévoilaient que les services américains, mais aussi britanniques, ont monté des opérations de renseignement visant certaines institutions internationales et structures de coopération (UN, UE et G20), où des 'pays amis' étaient également ciblés.

Ces révélations ont constitué le point de départ de nombreuses enquêtes (parlementaires, judiciaires et de renseignement).[199] En Belgique aussi. Ainsi, le 1er juillet 2013, la Commission de suivi du Sénat a demandé au Comité permanent R '*[…] een update van de bestaande informatie over de praktijken op het vlak van datamining. Niet alleen de Amerikaanse inlichtingendienst NSA zou dit doen, maar ook het Verenigd Koninkrijk zou massaal gegevens onderscheppen en analyseren. In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, een van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden*

197 G. GREENWALD et E. MACASKILL, *The Guardian*, 6 juin 2013 («NSA Taps in to Internet Giant's Systems to Mine User Data, Secret files Reveals»).

198 B. GELLMAN et L. POITRAS, *The Washington Post*, 6 juin 2013 («US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program»).

199 Ainsi, par exemple, au Parlement européen, où le Sénateur et membre de la Commission de suivi Armand De Decker et le président du Comité permanent R ont été auditionnés par la *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens* sur 'The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance' (voir à ce propos : http://www.europarl.europa.eu/committees/en/libe/events.html) et au sein des Nations Unies (J. KASTRENAKES, *The Verge*, 3 décembre 2013 («United Nations Counterterrorisms Official Lauches Investigation into NSA Surveillance»).

getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen.'[200]

Le Comité permanent R a dès lors ouvert trois enquêtes de contrôle qui sont évidemment imbriquées. Cela vaut aussi pour une quatrième enquête, qui a été initiée à la suite d'une plainte du président de l'Ordre néerlandophone des avocats du Barreau du Bruxelles.

La **première enquête de contrôle**, dont le présent rapport est le premier résultat intermédiaire, entend apporter une réponse aux questions suivantes :

- De quels moyens les grandes puissances telles que les États-Unis et la Grande-Bretagne disposent-elles pour intercepter et exploiter à grande échelle des données de personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique, et de quelles données s'agit-il (quantitativement *et* qualitativement) ?
- Dans quelle mesure les services de renseignement belges étaient-ils au courant des moyens dont disposent ces grandes puissances (ou dans quelle mesure devaient-ils être au courant au regard de leurs missions légales) ? Des renseignements ont-ils été recueillis à ce sujet ou cela n'a-t-il pas été jugé souhaitable ? Nos services offrent-ils une protection suffisante en la matière ?
- Quelle est la signification/valeur de la notion d''État ami',
- Dans le contexte des services de renseignement, et dans quelle mesure cette notion détermine-t-elle la position de nos propres services de renseignement ? Bien que cet aspect des révélations (c'est-à-dire certaines opérations des services de renseignement de soi-disant 'pays amis' à l'égard d'institutions internationales ou supranationales dans lesquelles la Belgique est représentée ou à l'égard d'intérêts belges) n'était pas repris explicitement dans la liste de questions de la Commission de suivi, le Comité permanent R décide d'y accorder aussi son attention, et ce vu l'intérêt intrinsèque de cette question.

La première enquête de contrôle se décline en trois volets :

- Un aperçu, réalisé au moyen de sources ouvertes par un expert externe (Mathias Vermeulen, doctorant, VUB et *European University Institute* de Florence), des différents types de 'données' qui pourraient concerner ou provenir de personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique, et qui sont captées et enregistrées à grande échelle par des services publics ou des firmes privées pour le compte des autorités américaines et britanniques, et ce en vue d'être exploitées (éventuellement par la suite) par leurs services de renseignement.[201]

---

200 '*[…] une mise à jour des informations existantes sur les pratiques en matière de* datamining *[exploration de données]. Le service de renseignement américain ne serait pas le seul à le pratiquer, la Grande-Bretagne intercepterait et analyserait aussi massivement des données. En second lieu, la commission de suivi veut que le Comité examine quelles sont les conséquences pour la protection du potentiel scientifique et économique de notre pays, une des missions légales de nos services de renseignement. Enfin, la commission de suivi souhaite que le Comité R étudie comment de telles pratiques sont évaluées au regard des règles de droit nationales et internationales qui protègent la vie privée des citoyens.*' (traduction libre).

201 Le projet de rapport de M. Vermeulen a fait l'objet d'une lecture critique par un groupe de travail constitué au sein du Comité permanent R. À la demande de ce groupe de travail, des clarifications ont été apportées, et des éléments ont été ajoutés. En outre, il a été demandé à

- Une analyse des informations qui sont actuellement disponibles au Comité, entre autres sur la base des dossiers MRD et des enquêtes de contrôle clôturées (telles que les enquêtes Echelon, Swift, Echelon bis, les activités de renseignement du SGRS à l'étranger…). En outre, des tiers, susceptibles de détenir des informations pertinentes, ont été interrogés.
- Une évaluation de la position de renseignement de la Sûreté de l'État (VSSE) et du Service général du renseignement et de la sécurité (SGRS) : que savaient-ils ou qu'ont-ils entendu dire ? Comment ont-ils géré les informations et les connaissances ? En ce qui concerne ce volet, les deux services de renseignement ont déjà été interrogés de manière approfondie à deux reprises. L'analyse de toutes les réponses a contraint le Comité permanent R à soumettre les services à une troisième série de questions.

La **deuxième enquête de contrôle**[202] traite des règles de droit en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle des données relatives à des personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique. Quant aux règles internationales, une attention sera naturellement portée à l'article 8 CEDH (où sont développés tant l''effet horizontal' de ces dispositions que les éventuelles 'obligations positives' qui en découlent pour un État), à l'article 17 de la Convention internationale relative aux droits civils et politiques (D.C.P), à la Directive 95/46/EC du 24 octobre 1995 (avec une attention pour l'exception en matière de données relatives à la sécurité nationale et pour les récentes négociations en vue de renforcer la Directive), au Traité n° 108 du 28 janvier 1981 du Conseil de l'Europe et aux articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Des règles plus spécifiques entreront aussi en ligne de compte : les règles relatives au *Passenger Name Record*, Swift, *Safe Harbour…* Enfin, les règles de droit internes relatives à la protection de la vie privée et à la protection des données, seront développées : l'article 10 de la Constitution, la Loi relative à la protection de la vie privée et son arrêté d'exécution ainsi que les dispositions spécifiques au fonctionnement des services de renseignement (p. ex. les limites fixées pour l'échange de données au niveau international).

En outre, cette deuxième enquête de contrôle doit offrir une vue sur les possibilités en termes juridiques dont disposent les États, les citoyens et les entreprises pour entreprendre une action contre d'éventuelles infractions aux droits fondamentaux. Dans ce volet, une attention sera notamment accordée à 'l'utilisabilité' des informations qui sont recueillies légalement à l'étranger, mais qui n'auraient jamais pu l'être de cette manière en Belgique.

Pour cette deuxième enquête aussi, il a été fait appel à un expert. Il s'agit du Professeur Annemie Schaus.

---

l'expert, dans le cadre d'une mission complémentaire, de mettre à jour le rapport, de rédiger un glossaire et de dresser l'inventaire de 'liens' (éventuels) avec la Belgique.

202 Enquête de contrôle sur les règles en vigueur en Belgique en matière de protection de la vie privée eu égard aux moyens autorisant l'interception et l'exploitation à grande échelle de données relatives à des personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique).

De plus, la VSSE et le SGRS ont été interrogés sur les règles précitées et les possibilités juridiques susmentionnées dont disposent les États, les citoyens et les entreprises. Enfin, des informations sont échangées avec la Commission de la protection de la vie privée.

La **troisième enquête de contrôle**[203] traite des implications éventuelles de datamining pour la protection du potentiel scientifique et économique du pays. Cette enquête a pour objectif de vérifier si les services de renseignement belges :

- ont prêté attention à ce phénomène ;
- ont détecté une menace réelle ou éventuelle pour le potentiel scientifique et économique belge ;
- en ont informé les autorités compétentes et proposé des mesures de protection ; et
- disposent des moyens suffisants et adéquats pour suivre cette problématique.

II. PRÉAMBULE AU RAPPORT DE L'EXPERT (VOIR ANNEXE 1)

Depuis la divulgation des premiers *slides* relatifs à la NSA et depuis l'ouverture de l'enquête de contrôle, de nouvelles données extrêmement sensibles font constamment l'objet de révélations. Celles-ci mettent en lumière la captation massive de données et l'espionnage politique et économique de et dans des pays amis. De plus, il ne s'agit plus seulement, et ce depuis longtemps, de PRISM, TEMPORA ou de l'espionnage du G20. Le rapport de l'expert ne fera que confirmer cette évidence.

Il convient naturellement de lire ce rapport avec toute la réserve qui s'impose. Celui-ci se base presque exclusivement sur des sources ouvertes. Toutefois, l'expert a effectué un travail très critique, et les pistes de réflexion ou les théories trop spéculatives n'ont pas été reprises. Le Comité tient d'ores et déjà à souligner qu'il n'a pas encore trouvé d'indications fondées mettant en doute l'authenticité des *slides* de Snowden. Au contraire, des enquêtes déjà menées, le Comité estime pouvoir conclure que les révélations, certainement 'dans les grandes lignes' sont véridiques.[204] En outre – aussi en raison du caractère fragmentaire des révélations[205] – le fait il n'y ait aucune certitude sur la véracité de *chaque* aspect technique de l'affaire, ne change en rien cette constatation. À ce propos, il convient également de tenir compte du fait que le rapport de l'expert a été clôturé le 23 octobre 2013. De nouvelles informations ou les contestations au niveau officiel relatives à des données précédemment commentées (voir II.4) n'exclut pas une autre lecture de certains aspects du dossier.

---

203 Enquête de contrôle sur l'attention que les services de renseignement belges portent (ou non) sur les menaces que peuvent représenter pour le potentiel scientifique et économique de la Belgique des programmes de surveillance électroniques sur les systèmes de communication et d'information mis en œuvre à grande échelle par des puissances et/ou des services de renseignement étrangers.

204 Il convient de tenir compte aussi du fait que ni les autorités américaines ni les autorités britanniques n'ont jusqu'à présent mis en doute l'authenticité des documents divulgués. Tout au plus, l'interprétation qui en a parfois été faite dans les sources ouvertes a été contestée.

205 *The Guardian* n'aurait jusqu'à présent publié qu'un pourcent de tous les documents qu'il a reçus de Snowden (X., *De Standaard*, 3 décembre 2013 («Amper 1 procent van informatie Snowden gepubliceerd»).

Au préalable, le Comité permanent R tient encore à brièvement expliquer quelques éléments. Ceux-ci doivent d'une part permettre une lecture plus fluide du rapport de l'expert, élaboré et technique, et d'autre part présenter utilement le contexte au sein duquel ce rapport doit être compris.

II.1. LA NSA ET LE GCHQ. ENTRE AUTRES…

Le rapport traite seulement de la captation massive de données par la National Security Agency américaine et le Government Communications Headquarters (GCHQ) britannique. Il est probable que, dans ces pays, d'autres services font de la captation massive de données. Et naturellement, les États-Unis et la Grande-Bretagne ne sont pas les seules grandes puissances à procéder de la sorte.

En marge des révélations de Snowden, les activités des services de renseignement, entre autres, français[206], allemands[207] et suédois[208] sont abordées. Et bien entendu il y a aussi les moyens susceptibles d'être déployés par, à titre d'exemple, la Russie[209] et la Chine.[210] Mais, ce qui est au moins aussi important dans ce cadre, ce sont les accords de coopération en matière de *Signal Intelligence* (SIGINT) qui existent (ou existeraient) entre certains pays. Le plus connu est le dénommé FIVE EYES qui, outre les États-Unis et la Grande-Bretagne, compte le Canada, l'Australie et la Nouvelle-Zélande. Ces pays collaborent très étroitement depuis des décennies et les communications de données captées seraient échangées de manière pratiquement illimitée. De plus, la presse, par exemple, a également mentionné les NINE EYES et les FOURTEEN EYES, desquels, selon les sources ouvertes, la Belgique ferait également partie.[211]

Enfin, les autorités n'ont pas le monopole de la captation et de l'exploitation massive de données. De grands acteurs privés disposent parfois de moyens similaires, même si la finalité de leurs activités diffère la plupart du temps. Pour des raisons évidentes, cette

---

206 *Le Monde* a par exemple affirmé que la DGSE française conserve systématiquement, dans son quartier général et '*depuis des années*', les métadonnées de téléphone, fax et communications internet entre un numéro français et un numéro étranger. Six autres services ont accès à cette base de données (J. FOLLOROU et F. JOHANNES, *Le Monde*, 4 juillet 2013 («Révélations sur le Big Brother français»)).

207 A. REIβMANN, *Der Spiegel*, 13 novembre 2013 (« Uberwachung : BND soll weitgehenden Zugriff auf Internetverkehr in Deutschland haben »).

208 T.T., *The Local*, 6 septembre 2013 (« Sweden 'a close partner' in NSA surveillance »). Voir aussi : « Snowden papers unmask close technical cooperation and loose alliance between British, German, French, Spanish and Swedish spy agencies», dans : J. BOGER, *The Guardian*, 1er novembre 2013 (« GCHQ and European Spy Agencies Worked together on Mass Surveillance »).

209 Voir dans ce cadre les allégations relatives à 'SORM' : S. WALKER, *The Guardian*, 6 octobre 2013 («Russia to monitor 'all communications' at Winter Olympics in Sochi»).

210 X., *www.sophos.com*, 7 mai 2008 («Belgium accuses Chinese government of cyber-espionage»).

211 « *Beyond that, the NSA has other coalitions, although intelligence-sharing is more restricted for the additional partners : the 9-Eyes, which adds Denmark, France, The Netherlands and Norway; the 14-Eyes, including Germany, Belgium, Italy, Spain and Sweden […].* » (E. MACASKILL en J. BALL, *The Observer*, 2 novembre 2013 («Portrait of the NSA : no detail too small in quest for total surveillance»).

problématique n'a pas été reprise dans les enquêtes de contrôle du Comité : elles se situent en dehors de sa sphère de compétences.

II.2. PRISM ET TEMPORA. ENTRE AUTRES…

Les premières révélations concernaient surtout – en ce qui concerne les Américains – le programme PRISM et – en ce qui concerne les Britanniques – TEMPORA. Il s'avère que ces deux programmes de renseignement sont une source très importante d'informations, mais elles ne sont pas les seules. Un peu schématiquement, l'on pourrait distinguer cinq[212] formes ou techniques de captation massive de données ou 'interception non ciblée' de (télé)communications (II.2.1). En outre, il existe divers moyens pour conserver et exploiter cette masse de données (II.2.2).

II.2.1. Cinq formes de captation massive de données

L'enquête de contrôle du Comité se limite essentiellement aux programmes ou techniques de renseignements par lesquels le recueil est principalement 'non ciblé' (aussi appelée *phishing expedition*). Un gigantesque filet à mailles fines est, pour ainsi dire, lancé. Ce n'est que par la suite que ce qui peut être pertinent et utile est examiné manuellement ou au moyen de processus automatisés. Cela ne concerne donc *pas* la mise sur écoute du trafic téléphonique d'une personne ou d'une instance (bien qu'il puisse s'agir de données nombreuses et sensibles). Une forme pure de captation 'non ciblée' est par exemple l'extraction et la conservation de *toutes* les informations qui passent par un câble internet international, pour ensuite effectuer des recherches numériques (datamining). Un autre exemple est la captation de tous les signaux GSM dans une région déterminée.

Il ressort du rapport de l'expert que la captation, par exemple, des câbles en fibre optique, est opérée avec ce que l'on appelle des *selectors* : un numéro de GSM, une adresse IP ou un terme déterminé (p. ex. 'attaque'). Cela signifie que toutes les données qui passent par le câble sont, il est vrai, scannées sur la base de paramètres dictés au préalable, mais seules les informations qui répondent à un ou plusieurs critère(s) de sélection sont effectivement extraites et conservées. Dans ce cas, l'appréciation du fait que la captation est 'ciblée' ou 'non ciblée' dépend en grande partie de la quantité et de la description des *selectors*. Lorsque les *selectors* restent principalement limités à des numéros de GSM ou adresses IP bien déterminés, le recueil de renseignement semble alors plutôt 'ciblé' (en supposant évidemment qu'un nombre limité de numéros et d'adresses soient introduits). En revanche, si des critères de sélection très larges sont utilisés (tels que l'usage de certains termes, un nom de domaine (p. ex. '@comiteri.be'), l'utilisation de certains termes sur des moteurs de recherche ou l'utilisation de certaines applications (par exemple les techniques VPN ou TOR), nous ne pouvons alors pas ignorer que les données sont récoltées de manière non ciblée. Bien que toute la lumière ne soit pas (encore) faite à ce sujet, tout indique de façon probante que des captations non ciblées et massives ont lieu.

---

212 Il y a bien entendu d'autres propositions tout aussi valables, où l'on distinguerait plus ou moins de formes de captation massive de données.

Au préalable, nous tenons encore à faire remarquer que les 'techniques' reprises ci-après peuvent à la fois se compléter (par exemple, parce qu'un e-mail ne peut éventuellement pas être lu via un câble surveillé, il peut être utile de collecter le message complet chez le fournisseur de service) et se chevaucher (une conversation GSM peut être directement extraite des ondes et aussi être extraite d'un câble).

II.2.1.1. Recueil en amont (upstream)

Le recueil en amont (*upstream*)[213] est le nom donné à la 'saisie' du trafic internet ou téléphonique qui passe par des câbles (en fibre optique) (internationaux), par exemple en plaçant un appareil à des points centraux qui sont exploités par de grands opérateurs télécoms ou en surveillant directement le câble. Cela peut se faire – comme pour la plupart des techniques – à l'insu ou non de l'opérateur/exploitant du câble.

TEMPORA est, selon les *slides* de Snowden, le nom de code du programme britannique de cette forme de captation.

Selon toute vraisemblance, étant donné qu'une quantité énorme de données passent par de tels câbles, des 'filtres' ou des 'sélecteurs' (*selectors*) sont placés (voir II.2.1), de telle sorte que seules des informations susceptibles d'être pertinentes sont enregistrées et traitées.

II.2.1.2. Recueil en aval (downstream)

Une autre possibilité pour capter massivement des données est de les collecter ou – par la contrainte ou non – de les demander directement aux opérateurs télécoms. Cette forme d'acquisition de données est connue sous le nom de recueil en aval (*downstream*).[214] L'exemple le plus connu est le programme PRISM, où neuf grandes entreprises de technologie américaines étaient prêtes et/ou étaient/sont obligées de fournir des données d'utilisateurs de manière structurée. Il s'agit de Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL et Apple. Bien que PRISM opère également sur la base de *selectors* (voir II.2.1), il ressort du rapport de l'expert que sur la base de ce programme, une quantité colossale de données ont été transmises à la NSA.

II.2.1.3. Interception de communications sans fil

De très nombreuses communications nationales et internationales se font en partie via des ondes électromagnétiques : de signaux radio classiques à une technologie GSM plus moderne qui passent ou peuvent passer par des antennes émettrices et des satellites.

L'interception discrète et massive de ces signaux est techniquement tout à fait possible et permet d'écouter des conversations en temps réel. FORNSAT serait le nom de code d'un

---

213 *Upstream* ou 'en amont' à l'égard du destinataire de la communication. Un exemple : lorsqu'une personne utilise un webmail (c'est-à-dire qu'il se logue à partir de son ordinateur à un fournisseur de services de webmail, tel que l'*outlook* de Microsoft), il opère alors sur le serveur de ce fournisseur de service. Sa boîte mail ne se trouve pas sur son propre ordinateur mais bien ailleurs, sur un serveur (très souvent aux États-Unis). Le message qui est envoyé peut donc être intercepté entre la personne concernée et le serveur.

214 *Downstream* of 'en aval' à l'égard du destinataire de la communication. Ici, les informations sont extraites directement du serveur du fournisseur de service, par exemple, par un accès à la boîte mail sur ce serveur ou en demandant les informations.

des programmes qui vise une telle captation de communications qui se fait via des satellites. Mais aussi l'interception de communications à partir de dizaines de postes diplomatiques et consulaires américains répartis aux quatre coins du monde (F6 SITES), peut être placée sous ce dénominateur.

II.2.1.4. Piratage (hacking) de système IT

Un autre moyen pour recueillir massivement des données jugées intéressantes est l'intrusion dans le système IT d'un opérateur, par exemple, afin d'extraire, sans être vu, toutes les informations utiles. Ce fut le cas avec BICS, une filiale de Belgacom, qui est responsable du *roaming* de télécommunication dans de grandes zones du globe. Via l'OPERATION SOCIALIST[215] (*sic*), les Britanniques seraient parvenus à installer un *malware* (logiciel malveillant) techniquement très élaboré, avec la collaboration de la NSA, et ainsi, selon toute vraisemblance, extraire une quantité énorme de données. Mais BICS n'est probablement pas la seule. De récentes révélations parlent de dizaines de milliers de systèmes informatiques qui auraient été infectés à travers le monde par le *malware* de la NSA.[216]

II.2.1.5. Coopération et échange de données

Une dernière 'méthode' est l'échange d'informations en vrac entre services partenaires. Cet échange se produit tantôt 'spontanément', tantôt dans le cadre d'un accord de coopération, aux termes duquel chaque service concerné se charge du *monitoring* d'un aspect déterminé de la (télé)communication et transmet ensuite les informations récoltées. Comme cela ressort d'ailleurs des sources ouvertes, le danger existe évidemment que le service A fasse ce que le service B n'est pas autorisé à faire en vertu de sa législation nationale et inversement, et que les données soient échangées, si bien que les restrictions légales sont *de facto* contournées.[217]

La structure de coopération la plus connue est le FIVE EYES. Les pays qui la composent partagent par exemple les informations qu'ils extraient chacun séparément des câbles en fibre optique qui passent par leur territoire. Mais d'autres pays transmettent aussi massivement des données récoltées en vrac. Ainsi, par exemple, les Norvégiens, les Français et les Néerlandais auraient passé plusieurs millions de données sur une période d'un mois.[218]

---

215 X., *Der Spiegel*, 20 septembre 2013 («Belgacom Attack: Britain's GCQH tracked Belgian Telecoms Firm»).

216 S. DERIX et H. MODDERKOLK, *NRC Handelsblad*, 23 novembre 2013 («De hackers van de NSA dringen overal binnen»).

217 «*De Amerikaanse inlichtingendienst bespioneerde volgens The Gardian sinds 2007 in ruime mate de gegevens van Britse burgers – en dat met gedoging van Londen.*» (X., De Morgen, 22 novembre 2013 («Britse burgers massaal bespioneerd»).

218 Cela a été admis publiquement, entre autres, par le service de renseignement norvégien et par des responsables de la NSA qui se sentaient obligés de rectifier une lecture prétendument erronée qu'on faite certains journalistes des *slides* de Snowden. Les journalistes étaient en effet d'avis que dans chacun de ces pays, il s'agissait de communications mises sur écoute par la NSA (VHN, *De Standaard*, 27 novembre 2013 («Noorse inlichtingendienst betwist claims over NSA-spionage»)).

II.2.2. Conservation et exploitation d'une masse d'informations

Il est naturellement inutile de capter massivement des données – selon *The Washington Post* la NSA intercepte quotidiennement 1,7 milliard d'e-mails et d'autres formes de communications – si ces données ne peuvent être ni conservées ni exploitées. Vu les quantités énormes de données générées par l'ensemble des programmes, un *hardware* gigantesque est non seulement nécessaire pour stocker ces données, mais il faut aussi un *software* performant qui permette de trouver l'aiguille dans la botte de foin. XKEYSCORE permet notamment aux analystes de la NSA de traiter des informations en amont. Une partie de l'analyse se fait sans aucun doute de manière automatisée: des algorithmes recherchent au préalable certains 'modèles' et certaines 'anomalies' dans les données. Mais il est aussi possible de transmettre une masse de données à des pays ou à des services partenaires en vue d'une analyse ultérieure.

II.3. QUEL GENRE DE DONNÉES SONT CAPTÉES VIA LE SIGINT AMÉRICAIN ET BRITANNIQUE ?

Bien qu'au départ, il n'y avait aucune certitude sur la question, il est vite devenu clair que les différents programmes captaient non seulement les métadonnées (telles que, par exemple, l'adresse d'expéditeurs et de destinataires, l'identification de connexion, l'heure et la durée, le moyen technique utilisé, la taille d'un fichier…), mais aussi le contenu même des messages, si ceux-ci sont envoyés par GSM, téléphone, boîte vocale interne, messageries instantanées, messages de forums online, clouding, annexes d'e-mails, Skype…

Les autorités américaines prétendent depuis longtemps que seuls les messages en rapport avec le terrorisme ont été interceptés. Mais ici aussi, les sources ouvertes démontrent de manière convaincante que l'intérêt et la sphère de compétences de la NSA, par exemple, sont nettement plus larges: il s'avère que les informations à caractère économique et politique constituent également des cibles.

II.4. QU'EN EST-IL DES DONNÉES À CARACTÈRE PERSONNEL, ÉCONOMIQUE OU POLITIQUE DE ET SUR DES BELGES ET LA BELGIQUE ?

Les incessantes révélations laissent supposer des capacités de traitement de plusieurs pétaoctets par jour ou de milliards de métadonnées sur de plus longues périodes. Il semble dès lors prouvé que le filet virtuel lancé par les grands services de renseignement sur le monde numérique permet une captation inédite.

Il va toutefois de soi que le Comité permanent R est principalement intéressé par l'éventuelle interception de données qui concernent ou proviennent de personnes, organisations, entreprises ou instances établies en Belgique ou qui ont un lien avec la Belgique. Jusqu'à présent, peu d'éléments spécifiques sont connus à cet égard.

Il serait cependant naïf de conclure que la Belgique peut être un des pays resté hors d'atteinte, certainement en raison de la présence d'organisations internationales

importantes sur son territoire. De nouvelles révélations à ce propos pourraient nous éclairer davantage.

Indépendamment de cela, le rapport de l'expert comporte toute une série d'éléments qui permettent de conclure que des 'données belges' ont nécessairement été interceptées à grande échelle.

La manière avec laquelle la NSA recueille certaines données d'utilisateurs, par exemple, implique à elle seule, par définition, que des données de Belges ont aussi pu être captées.

En effet, de nombreux concitoyens utilisent quotidiennement les services des neuf entreprises américaines reprises dans le programme PRISM (Microsoft, Google, Yahoo !, Facebook, PalTalk, YouTube, Skype, AOL et Apple).

Mais les données belges ne sont pas non plus immunisées contre le recueil en amont (*upstream*). Des e-mails ou des messageries instantanées peuvent déclencher certains *selectors* lorsque par exemple – ce qui est souvent le cas – ils passent par un câble qui transite par le territoire américain. De plus, il est important de savoir qu'un message électronique (ou une partie de celui-ci) qui part de la Belgique vers un autre pays transite souvent par les États-Unis. Le chemin emprunté par un message (ou une partie du message) dépend de la densité du trafic ou du coût à un moment donné sur un trajet donné, et donc pas du chemin le plus court d'un point de vue géographique. Un nombre considérable d'informations sur Internet passent par les États-Unis parce que ce pays possède la plus grande capacité de transport de et vers les autres pays du monde, même si les messages doivent faire un 'détour' de milliers de kilomètres. Et ce qui a échappé aux Américains, les Britanniques peuvent l'intercepter via les moyens dont ils disposent pour 'surveiller' des câbles en fibre optique. Dans le même contexte, l'on peut mentionner le fait que le GCHQ mettrait sur écoute des données passant par des câbles en fibre optique entre les centres de données de Google. Il convient en outre de signaler qu'un des centres de données les plus importants de Google se trouve en Belgique.

Par ailleurs, des métadonnées de 'conversations belges' sont recueilles si des Belges communiquent directement avec un Américain qui est considéré comme une cible par la NSA, mais aussi s'ils communiquent avec un 'contact' de cette personne.

Un tout autre exemple est la révélation selon laquelle la division de la NSA qui est responsable de la 'sécurité internationale', se concentre notamment sur 'la politique étrangère et les relations commerciales de la Belgique'.[219]

Enfin, il y a évidemment le *hacking* de BICS/Belgacom. Bien qu'ici, selon toute vraisemblance, peu de données 'purement' belges ont été collectées, nous ne pouvons bien entendu pas ignorer que cette entreprise publique fait partie de l'infrastructure critique belge.

III. EN CONCLUSION

Que certaines grandes puissances – telles que les États-Unis – disposent depuis assez longtemps de moyens et de programmes très avancés pour procéder à une captation

219 X., *De Tijd*, 4 septembre 2013 («Staatsveiligheid onderzoekt spionage door NSA»).

massive de données est de notoriété publique. A titre d'exemple, nous pouvons faire référence ici aux révélations relatives au réseau Echelon et à l'affaire Swift.[220]

Mais aujourd'hui, nous sommes confrontés à deux éléments nouveaux.

Tout d'abord, il y a le fait que l'espionnage électronique, global et massif, est réalisé à partir de centaines de SIGADS (points de recueil de données) répartis à travers le monde, et ce avec les *hardwares* et *softwares* les plus en pointe et des moyens humains et financiers colossaux. Peu de moyens de communication ou de messages semblent pouvoir échapper à une éventuelle interception. Que cela se produise dans le contexte du renseignement n'est pas si surprenant. Par exemple, la technologie de l'Internet, y compris toutes les formes de communications qui passent par Internet, offre une source rêvée de données détaillées qui étaient auparavant inaccessibles. Avec la numérisation, une nouvelle ère s'est ouverte pour le monde du renseignement, ce dont chacun doit avoir conscience.

Le second élément nouveau est qu'aujourd'hui, avec une quasi-certitude, des éléments prouvant l'existence et l'ampleur de ces captations sont disponibles, sous la forme de documents administratifs internes et officiels, notamment les *slides* divulgués.

220 Ce qui est moins connu est le fait qu'avant Snowden, d'autres lanceurs d'alerte avaient déjà dénoncé certaines pratiques de la NSA. Ainsi, par exemple, William Binney, Thomas Andrew Drake et Thomas Tamm, d'anciens collaborateurs de la NSA, avaient révélé certains programmes de collecte dès le début des années 2000.

LES RÉVÉLATIONS DE SNOWDEN, INTERCEPTION MASSIVE DE DONNÉES ET ESPIONNAGE POLITIQUE

Étude des sources ouvertes[221]

INTRODUCTION

1. Le présent rapport présente un aperçu, au moyen de sources ouvertes[222], des types de données susceptibles de porter sur des (ou d'émaner de) personnes, organisations, entreprises ou instances établies en Belgique (ou qui ont un lien avec la Belgique) et qui sont interceptées et enregistrées à grande échelle par la NSA (National Security Agency) américaine, le GCHQ britannique (Government Communications Headquarters), ou des sociétés privées opérant pour le compte de ces services, et ce en vue d'une (éventuelle) exploitation (ultérieure) par leurs services de renseignement. Parallèlement, ce rapport présente des cas dont il ressort que ces services (parmi d'autres) ont mis sur pied, ces dernières décennies, des opérations d'espionnage politique à l'égard de « pays alliés ». Les sources ouvertes consultées aux fins du présent rapport sont de qualité variable. Nous avons autant que possible utilisé des sources primaires (*slides*, documents officiels) qui ont été publiées ces derniers mois par des journalistes d'investigation. L'interprétation critique de ces éléments (incomplets) d'information s'est appuyée sur la consultation d'autres experts. Nous n'avons pas retenu les analyses de presse trop spéculatives, où nous n'avons trouvé aucune information complémentaire venant étayer une piste de réflexion. Une liste explicative des abréviations figure en annexe.

2. Toutefois, pour mieux comprendre les mécanismes spécifiques de recueil qui ont été dévoilés depuis juin 2013, il convient au préalable de décrire brièvement le contexte légal dans lequel opèrent la NSA et le GCHQ, car il éclaire également le mandat et les mesures de précaution qui s'appliquent ou non à l'exercice de ce mandat. Nous avons aussi tenté de faire dans tous les cas la lumière sur l'ampleur du recueil de données et sur la période d'activité de ces mécanismes de recueil.

---

221 Le Comité permanent R a confié la présente étude des sources ouvertes aux bons soins du Dr Mathias Vermeulen, chercheur à l'Institut universitaire européen de Florence et au sein du groupe de recherche LSTS (Law, Science, Technology and Society) de la VUB. De 2008 à 2011, le Dr Mathias Vermeulen a travaillé en tant que chercheur aux côtés du Rapporteur spécial des Nations unies sur la promotion et la protection des droits de l'homme et la lutte contre le terrorisme. Il s'est également penché, pour le compte du Parlement européen, sur le contrôle parlementaire des services de sécurité et de renseignement au sein de l'Union européenne ('Parliamentary oversight of security and intelligence agencies in the European Union'). http://www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf.

222 Toutefois, l'expert a effectué un travail très critique, et les pistes de réflexion ou les théories trop spéculatives n'ont pas été reprises. De nouvelles informations ou les contestations au niveau officiel relatives à des données précédemment commentées n'excluent pas une autre lecture de certains aspects du dossier.

3. L'expérience relative aux documents de Snowden nous apprend à ce stade que les documents confidentiels qui n'ont pas encore été publiés, et qui le seront probablement à l'avenir, auront un impact sur l'interprétation de documents et d'informations déjà publiés à propos des révélations. La présente note n'est donc qu'un instantané de la situation au 23 octobre 2013.

I. LA NATIONAL SECURITY AGENCY (NSA) AMÉRICAINE

4. La NSA est un service de renseignement militaire dirigé par le Général Keith B. Alexander. Alexander rend compte à l'Under Secretary of Defense for Intelligence, Michael G. Vickers, le principal conseiller en renseignement du ministre américain de la Défense, Chuck Hagel. La NSA fait également partie de l'*Intelligence Community* américaine, dirigée par James Clapper. En vertu de l'EO 12333, le directeur de la NSA (DIRNSA) a notamment pour mission de recueillir, de traiter, d'analyser, de produire et de diffuser des *signals intelligence* (SIGINT[223]) (y compris par des moyens clandestins) à des fins de *foreign intelligence* et de *counterintelligence*[224] ainsi qu'en appui d'opérations militaires.[225] Le recueil de SIGINT par la NSA est régi par deux documents majeurs : l'Executive Order 12333 (EO 12333)[226] et le Foreign Intelligence Surveillance Act (FISA).

I.1. LE CADRE LÉGAL DU RECUEIL D'INFORMATIONS SUR DES CIBLES ÉTRANGÈRES

I.1.1. Executive Order 12333

5. L'EO 12333 définit le concept de *foreign intelligence* comme désignant toutes les informations relatives aux capacités, aux intentions ou aux activités de puissances, d'organisations ou de personnes étrangères.[227] Le recueil de SIGINT peut se fonder purement et simplement sur cet *executive order*, sans qu'il faille pour autant suivre les

---

223 Les SIGINT sont des renseignements (*intelligence*) créés par des signaux et systèmes électromagnétiques, tels que des systèmes de communication, des radars, des satellites ou des systèmes d'armement. Voir à cet égard, par exemple, http://www.nsa.gov/sigint/.

224 Executive Order 12333 – United States intelligence activities, 4 décembre 1981, section 1.7(c)(1). L'EO 12333 a été amendé par les Executive Orders 13284 (2003), 13355 (2004) et 13470 (2008). La version consolidée de l'EO 12333 est disponible à l'adresse https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf. Il convient de noter que l'EO 12333 régit les activités de tous les membres de l'US Intelligence Community, et donc pas seulement de la NSA.

225 *Idem*, section 1.7(c)(3) et (5).

226 Avant l'EO 12333, il y avait déjà l'EO 12139 (Exercise of Certain Authority Respecting Electronic Surveillance), qui fut amendé par l'EO 12333, l'EO 13383 et l'EO 13475.

227 *Idem*, section 3.5(e). L'EO 12333 stipule clairement que la *foreign intelligence* peut être acquise par d'autres moyens que SIGINT, à savoir en ayant recours à d'autres éléments de l'*intelligence community* par le biais de la surveillance physique (voir p.ex. section 2.4(d) "*Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means*").

procédures FISA plus élaborées.[228] Par exemple, l'EO 12333 constitue la base légale pour l'acquisition de quantités colossales de métadonnées en dehors du territoire américain[229], ainsi que pour le recueil des listes de contacts ou des carnets d'adresses de logiciels de messagerie électronique et de conversation instantanée.[230] En effet, ce type d'information ne relève pas de la définition d'*electronic surveillance* telle qu'utilisée par le FISA.[231] L'EO 12333 semble également offrir une base légale aux activités les plus controversées de la NSA, et ce particulièrement celles de ses subdivisions, telles que l'Office of Tailored Access Operations (TAO) et le Special Collection Service (SCS), comme le contournement des systèmes de cryptage commerciaux[232], le piratage d'ordinateurs étrangers[233] ou l'espionnage de dirigeants étrangers à partir d'ambassades américaines.[234] L'US Senate Intelligence Committee exerce un contrôle limité sur ces activités.[235]

I.1.2. Foreign Intelligence Surveillance Act

6. Une grande partie de la « surveillance électronique » est régie par le Foreign Intelligence Surveillance Act (FISA) datant de 1978. Le FISA a été codifié au titre 50 de l'U.S.C. § 1801 *et seq*., puis s'est vu compléter de manière plus significative par de nouvelles dispositions du Patriot Act[236], qui régissent entre autres l'installation et l'utilisation des *pen registers* [237] et des *trap and trace devices* [238], ainsi que la production

---

228 N.S.A., The National Security Agency : Missions, Authorities, Oversight and partnerships, 9 août 2013 (http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 2).

229 Foreign Intelligence Surveillance Court, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13 – 109, 29 août 2013, 10, n° 10. ("*The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders*"). Voir également paragraphe 15.

230 Voir paragraphes 25-27.

231 US Code Title 50 – War and National Defence, 50 USC 1801(f).

232 Voir paragraphes 45-48.

233 Voir par exemple paragraphes 29, 47 et 48.

234 Voir par exemple paragraphe 19.

235 Un membre du Committee a indiqué ce qui suit : "*In general, the committee is far less aware of operations conducted under 12333 (…). I believe the NSA would answer questions if we asked them, and if we knew to ask them, but it would not routinely report these things, and, in general, they would not fall within the focus of the committee*". http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html.

236 Voir 50 U.S.C. §1841 *et seq.*

237 Le titre 18 de l'U.S.C. §3127(3) définit un *pen register* comme "*a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business*".

238 Le titre 18 de l'U.S.C. §3127(4) définit un *trap and trace device* comme "*a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the*

d''éléments tangibles'.[239] Le FISA a été amendé pour la dernière fois en 2008 par le biais du FISA Amendments Act (FAA).[240] En décembre 2012, le Sénat américain a prolongé les effets du FISA Amendments Act jusqu'au 31 décembre 2017 inclus. Selon la NSA, la principale application du FAA réside dans le recueil des communications de ressortissants étrangers qui utilisent des fournisseurs américains de services de communication.[241] Plusieurs propositions législatives visant à restreindre la collecte par les États-Unis d'informations relatives à des « nationaux »[242] sont actuellement sur la table, mais jusqu'à présent aucune initiative semblable ne cherche à limiter le recueil d'informations relatives à des « étrangers ».[243] Le présent rapport se penchera uniquement sur le récent FISA-Amendments Act, qui vient en complément du titre 50 de l'U.S.C. § 1802. En vertu du titre 50 de l'U.S.C. § 1802, le procureur général américain (*Attorney-General*) peut mandater une surveillance électronique pour une période d'un an si cette surveillance est exclusivement destinée à (1) acquérir le contenu des communications transmises par des moyens de communication uniquement utilisés par ou entre des « puissances étrangères »[244] ou (2) acquérir la *technical intelligence* de lieux qui se trouvent sous le contrôle ouvert et exclusif d'une « puissance étrangère ».

7. Le FISA Amendments Act confère à l'AG et au DNI la compétence de mandater, pour une période d'un an, la surveillance électronique de personnes dont il peut être raisonnablement admis qu'elles se trouvent en dehors des États-Unis, et ce dans le but spécifique de recueillir des « renseignements étrangers ».[245] Ces « renseignements étrangers » font l'objet d'une définition très large :

> « *(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–*

---

source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication".

239 Voir 50 U.S.C. §1861. Il s'agit, par exemple, de la base légale pour la banque de données MAINWAY. Voir paragraphe 37.

240 Voir H.R. 6404, FISA Amendments Act of 2008' sur http://www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf. La section 702 "Procedures for targeting certain persons outside the United States other than United States persons", souvent citée, a été consolidée dans l'U.S Code sous le titre 50 USC §1881a, disponible à l'adresse http://www.law.cornell.edu/uscode/text/50/chapter-36. Auparavant, le FISA avait déjà fait l'objet de modifications majeures par le biais du Patriot Act en 2001.

241 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 août 2013. http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 4.

242 Pour un aperçu des principales initiatives, voir J. GRANICK, "A tale of two surveillance reform bills. Centre for Internet and Society", 29 octobre 2013. https://cyberlaw.stanford.edu/blog/2013/10/tale-two-surveillance-reform-bills.

243 Voir par exemple D. POKEMPNER, "Dispatchers: Taming the NSA – Reform bills fall short. Human Rights Watch", 30 octobre 2013. http://www.hrw.org/news/2013/10/30/dispatches-taming-nsa-reform-bills-fall-short.

244 Voir définition au paragraphe 8.

245 Il convient de noter que le verbe '*acquire*' n'a pas la même signification que le verbe '*collect*'. Voir par exemple Department of Defense, DoD 5240 1-R, Procedures governing the activities of DoD intelligence components that affect United States persons. December 1982, 15. "*Data*

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States. »[246]

8. C'est cette dernière catégorie qui permet le recueil en principe illimité d'informations, d'autant plus que la définition de « puissance étrangère » est elle aussi étendue. Ce terme ne désigne pas seulement des gouvernements ou parlementaires étrangers ou des organisations internationales, mais aussi « *une organisation politique à l'étranger, qui n'est pas essentiellement composée de citoyens américains* »[247] et « *une entité dirigée et contrôlée par un ou des gouvernements étrangers* ».[248] En théorie, ces deux catégories pourraient par exemple aussi inclure respectivement des ONG qui organisent des manifestations anti-américaines ou des entreprises publiques.

9. La Foreign Intelligence Surveillance Court (FISC) vérifie si le mandat de l'AG et du DNI (voir paragraphe 7) satisfait à un certain nombre de conditions procédurales. L'AG et le DNI joignent un certificat écrit au mandat qui atteste du respect de ces conditions procédurales. Ces conditions visent principalement à limiter autant que possible le recueil intentionnel de données concernant des citoyens américains.[249] Aucune loi ou réglementation américaine ne prévoit de telles « procédures de minimisation » censées éviter le recueil et l'enregistrement de données étrangères « innocentes ». Ce certificat doit également mentionner les installations, lieux ou propriétés spécifiques qui sont précisément la cible de la collecte SIGINT.[250] Les autorités américaines ont déclassifié un document datant du 31 octobre 2011, qui décrivait les « procédures de minimisation » appliquées par la NSA pour recueillir des informations de type *foreign intelligence*. Il s'est avéré que les communications émanant de ou relatives à des citoyens américains qui

---

acquired by electronic means is "collected" only when it has been processed into intelligible form". La section 1881a s'intitule : "Procedures for targeting certain persons outside the United States other than United States persons ". Le '*targeting*' n'est toutefois pas défini au titre 50 de l'USC §1881. Le titre 50 de l'U.S.C. §1801 définit l'"*electronic surveillance*' comme "*the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes* ". Une interprétation pourrait donc être que le '*targeting*' vise uniquement les données recueillies *intentionnellement*. Les informations recueillies accidentellement ne sont pas considérées comme du '*targeting*'.

246 50 USC §1801(e).

247 50 USC §1801(a)(5).

248 50 USC §1801(a)(6).

249 50 USC §1801(g).

250 50 USC §1801(g)(2)(4).

n'ont pas été recueillies intentionnellement pouvaient être conservées jusqu'à cinq ans[251] et pouvaient être partagées avec des autorités étrangères.[252]

10. Si la FISC marque son accord, l'AG et le DNI peuvent transmettre, sur la base d'un certificat d'une telle portée, des *identifiers* (par exemple, des adresses e-mail ou des numéros de téléphone)[253] à une entreprise américaine, qui est alors obligée de fournir immédiatement toutes les « informations, facilités ou autre assistance » nécessaires à la réussite de ce recueil SIGINT.[254] En échange, ces entreprises bénéficient d'une compensation financière et ne peuvent être tenues pour responsables de la fourniture de telles informations « *devant aucun tribunal* ».[255] Une entreprise peut introduire un recours contre une telle demande (par exemple, parce que la demande est trop vaste)[256], à la suite de quoi la FISC peut rejeter la demande ou prononcer une ordonnance définitive de collaboration.[257]

I.1.3. SAFE HARBOUR

11. Les entreprises américaines peuvent dès lors être obligées de transmettre des données à la NSA, y compris des données émanant et concernant des clients belges. Cette exigence en vertu du droit américain peut se heurter aux principes de l'accord « Sphère de sécurité » (ou *Safe Harbour*) que les États-Unis et l'Union européenne ont conclu en 2000 et qui permet aux entreprises américaines de se conformer volontairement aux principes de cet accord. Par exemple, les entreprises sont censées informer leurs clients que leurs données personnelles ont été transmises à une tierce partie.[258] La Federal Trade Commission (FTC) veille au respect de cet accord. Il peut être dérogé à ces principes au nom de la sécurité nationale ou parce que le maintien de l'ordre public le requiert. Cependant, en raison de la grande ampleur avec laquelle des données personnelles

---

251 Exhibit B, Minimization Procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf), s.3(b)(1).

252 *Idem*, (s.8(a)).

253 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 août 2013, (http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf), 4.

254 50 USC §1802, (a)(4) ; 50 USC §1881a(1) et (2).

255 50 USC §1881a (h)(3).

256 En 2007, Yahoo a reçu un tel « ordre » de fournir des données et l'a contesté auprès de la Foreign Intelligence Surveillance Court of Review. Le tribunal a toutefois rejeté les objections de Yahoo. Cette décision n'a été divulguée que récemment. https://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.

257 50 USC §1881a (h)(4).

258 2000/520/CE : Décision de la Commission du 26 juillet 2000 conformément à la Directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (notifiée sous le numéro de document C(2000) 2441) (Texte présentant de l'intérêt pour l'EEE). Voir également http://export.gov/safeharbor/eu/eg_main_018493.asp.

d'utilisateurs européens d'entreprises américaines ont été envoyées à la NSA dans le cadre du programme PRISM (voir paragraphes 32-38), la Commission européenne examine actuellement une éventuelle révision de l'accord *Safe Harbour.*[259]

12. Le 22 octobre 2013, le Parlement européen a voté en faveur de l'ajout d'une clause dite « anti-FISA », qui ne permettrait pas aux entreprises de transmettre, sans l'autorisation d'une *supervisory authority,* des données personnelles de résidents européens à un pays tiers à la demande d'un tribunal ou d'une autre autorité de ce pays. Cette *supervisory authority* doit d'abord vérifier si ce transfert est nécessaire et conforme à la nouvelle législation européenne en matière de protection des données. Reste à savoir si cet article survivra aux négociations avec le Conseil.[260]

I.2. NATURE ET AMPLEUR DU RECUEIL SIGINT PAR LA NSA

13. Il est difficile de dresser l'inventaire de la totalité du recueil SIGINT de la NSA. Quelques chiffres donnent toutefois déjà une idée de son ampleur. *The Guardian* cite un rapport de 2007 de la NSA qui estimait qu'à l'époque, les différentes bases de données de la NSA contenaient environ 850 milliards de *call events* non définis et environ 150 milliards d'*internet records* non définis. D'après le document, un à deux milliards de *records* viennent s'ajouter chaque jour.[261] Un article du journal *The Washington Post* mentionnait en 2010 que la NSA conservait, par jour, le contenu et les métadonnées de 1,7 milliards d'e-mails, de conversations téléphoniques et d'autres formes de communications, et qu'une fraction était stockée dans quelque 70 bases de données distinctes.[262]

14. Depuis lors, cette capacité a connu une croissance exponentielle. Des *slides* du programme interne Boundless Informant[263] de la NSA, qui ont été publiés par *The Guardian*, montrent qu'en un mois (mars 2013), la division Global Access Operations

---

259 Commissaire Reding : "*The Safe Harbor agreement may not be so safe after all (.) It could be a loophole for data transfers because it allows data transfers from EU to U.S. companies-although U.S. data protection standards are lower than our European ones. (…) I have informed ministers that the commission is working on a solid assessment of the Safe Harbor Agreement, which we will present before the end of the year* ", European Commission, Memo/13/710, 19/07/2013, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm.

260 Voir article 43a de la "unofficial consolidated version of the European Data Protection Regulation after the LIBE Committee vote provided by the rapporteur, 22 October 2013". http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf. Voir également Caspar Bowden, The US surveillance programmes and their impact on EU citizens' fundamental rights. European Parliament, Directorate General for Internal Policies, 2013, 28.

261 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

262 D. PRIEST, W. M. ARKIN, *The Washington Post* ("Secret America : A Hidden World, Growing Beyond Control"). http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/.

263 Pour en savoir plus, voir : NSA, Boundless Informant – Frequently Asked Questions, 09-06-2012. http://www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text.

(GAO)[264] de la NSA a recueilli 97 milliards de métadonnées de communications internet (e-mails, conversations instantanées…) et près de 125 milliards de métadonnées de conversations téléphoniques provenant de plus de 504 SIGINT Activity Designator (SIGADS).[265] Il ressort du *slide* que la Belgique faisait partie des pays pour lesquels le recueil de métadonnées était le moins important en chiffres absolus.[266] Le *slide* ne révèle rien de la quantité de métadonnées concernée, mais le code couleur de la Belgique indique que la quantité de métadonnées recueillies en Belgique est moindre que celles recueillies aux Pays-Bas, par exemple.

15. En août 2013, *Der Spiegel* publiait des *slides* supplémentaires du programme qui indiquaient clairement qu'en décembre 2012, environ 1,8 million de métadonnées issues de conversations téléphoniques émanant des Pays-Bas ont été recueillies.[267] Durant cette même période, 70 millions de métadonnées ont été recueillies à partir de communications téléphoniques depuis la France[268], 60 millions depuis l'Espagne et 47 millions depuis l'Italie.[269]

16. Durant la même période, plus de 500 millions de métadonnées ont été recueillies depuis l'Allemagne. Ce nombre est bien plus important puisqu'il s'agit de métadonnées Internet. Il ressort d'un document que plus de 471 millions de métadonnées proviennent de SIGAD US-987LA.[270] Selon *Der Spiegel,* le Bundesnachrichtendienst (BND) pense

---

264 La collecte de métadonnées d'autres divisions de la NSA, telles que TAO ou SSO, n'est donc pas concernée.

265 Signals activity/address designators – peuvent faire référence à une plateforme de collecte physique spécifique (comme une base de l'armée américaine à l'étranger, une ambassade, un navire…), une plateforme virtuelle de traitement de données (par exemple, PRISM est connu sous le SIGAD US-984XN) ou un satellite spatial.

266 http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#.

267 Http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html.

268 Http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html En octobre, *Le Monde* a publié davantage de détails dont il ressort que 62,5 millions de métadonnées issues de communications mobiles ont été recueillies sous le nom de code DRTBOX et 7,8 millions de métadonnées de conversations du réseau téléphonique public (PSTN – Public switched telephone network) sous le nom de code WHITEBOX. Parmi les cibles figuraient tant des personnes qui ont été associées à des activités terroristes que des personnes issues du monde des affaires, de la politique française ou du monde des affaires français. http://www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-cross hair-phone-networks-under-surveillance_3499741_651865.html. Plusieurs médias ont annoncé que 70 millions de communications téléphoniques françaises ont été écoutées. Il s'agit là certainement d'une interprétation erronée des documents de Snowden. Voir également "DNI Statement on Inaccurate and Misleading Information in Recent Le Monde Article", 22 octobre 2013, (http://icontherecord.tumblr.com).: "*The allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data " is false. (…) While we are not going to discuss the details of our activities, we have repeatedly made it clear that the United States gathers intelligence of the type gathered by all nations.*"

269 Http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-5.html.

270 Http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-4.html.

qu'il est ainsi fait référence au site Bad Aibling, qui était exploité par la NSA jusqu'en 2004, puis a été repris par le BND. Depuis ce site, le BND collecte des SIGINT étrangers, principalement en provenance d'Afghanistan et du Moyen-Orient. Ces données sont alors transmises à la NSA.[271]

17. Selon la NSA, Internet transporte chaque jour 1,826 pétaoctet de données. Sur l'ensemble de ces données, la NSA ne « touche » qu'à 1,6 %, soit environ 29 millions de gigaoctets par jour.[272] Sur ce 1,6 %, 0,025 % est sélectionné en vue d'une évaluation. Selon la NSA, « elle examine donc à peine 0,00004 % de tout le trafic Internet par jour ».[273] Un simple calcul suggérerait que ce chiffre est dix fois plus élevé, et la NSA examinerait dès lors 0,0004 % du trafic Internet, mais selon la NSA, le chiffre initial est correct.[274]Ce qui semble peu, mais représente toutefois une quantité colossale lorsqu'on sait que par exemple, seulement 2,9 % de tout le trafic Internet aux États-Unis sont des communications.[275]

18. *The Guardian* a décrit un document datant du 26 décembre 2012, dans lequel la division « Special Source Operations » (SSO) annonçait l'acquisition d'une nouvelle capacité (nom de code EVILOLIVE) afin de recueillir encore davantage de métadonnées de communications dont une partie n'est pas américaine (One-End Foreign (1EF) solution). La NSA pourrait à présent stocker dans ses propres bases de données plus de la moitié de toutes les métadonnées recueillies via ses SIGADS.[276] Un autre document non publié évoque une autre capacité d'acquisition de métadonnées baptisée SHELLTRUMPET, à propos de laquelle un responsable de la SSO a déclaré le 31 décembre 2012 que ce programme venait de traiter sa trillionième métadonnée. La moitié de ces traitements ont eu lieu en 2012. Deux autres programmes de métadonnées

---

271 Selon *Der Spiegel*, pas moins de 62.000 e-mails sont interceptés chaque jour rien qu'à partir du site Bad Aibling. http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

272 Le terme '*touch*' n'est pas défini par la loi, mais implique que la NSA consulte effectivement ces informations (et ne se contente pas de les recueillir). *The Wall Street Journal*: "*One U.S. official says the agency doesn't itself "access" all the traffic within the surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering*". http://online.wsj.com/article_email/SB10001424127887324108204579022874091732470-lMyQjAxMTAzMDIwMDEyNDAyWj.html.

273 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships". 9 août 2013, 6.

274 V. VINES, porte-parole de la NSA: "*Our figure is valid; the classified information that goes into the number is more complicated than what's in your calculation*". http://www.thewire.com/politics/2013/08/nsa-better-data-collection-math/68490/.

275 Par exemple, aux États-Unis, le divertissement en temps réel ('*real time entertainment*') (sites de diffusion en continu tels que Netflix) représente 62 % du trafic Internet et le partage de fichiers *peer-to-peer* (via des sites tels que Bittorrent, par exemple) 10,5 %. J. JARVIS, *Buzzmachine*, 10 août 2013, ("NSA by the numbers"), http://buzzmachine.com/2013/08/10/nsa-by-the-numbers/.

276 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection "*This new system, SSO stated in December, enables vastly increased collection by the NSA of internet traffic. (…) The 1EF solution is allowing more than 75 % of the traffic to pass through the filter," the SSO December document reads. "This milestone not only opened the aperture of the access but allowed the possibility for more traffic to be identified, selected and forwarded to NSA repositories*".

(MOONLIGHTPAD et SPINNERET) devaient devenir opérationnels en septembre 2013.[277]

19. Un jugement prononcé par la FISC en 2011 et récemment publié suggère que 91 % des données Internet collectées par la NSA sont issues du programme PRISM.[278] Les 9 % restants proviennent du traitement de données en amont (*upstream*) et de missions clandestines dans le cadre du programme SRP (Specialized Reconnaissance Program) qui peuvent être menées en collaboration avec la CIA. *The Washington Post* a divulgué le budget de la US intelligence community en 2013 et il s'est avéré que 2 % du budget total est réservé à deux programmes conjoints CIA-NSA. Le premier, baptisé CLANSIG (*clandestine signals collection*), couvre une multitude de *black bag jobs* ou d'opérations *off-net*. Il s'agit d'opérations clandestines très risquées au travers desquelles l'on cherche à accéder, par exemple, à des radiofréquences et une infrastructure télécom critique d'un pays, mais aussi à obtenir un accès spécifique aux e-mails et ordinateurs de cibles *high interest*, telles que des gouvernements étrangers, des systèmes de communication militaire et d'éminentes multinationales. Cette dernière décennie, plus de cent *black bag jobs* de ce type ont été menés. Par exemple, durant ces opérations, des *spyware* sont installés sur des ordinateurs, ou la CIA fait en sorte que des lignes téléphoniques, routeurs, câbles en fibre optique, centres de commutation de données et autres systèmes protégés puissent être mis sur écoute pour permettre à la NSA d'accéder à ces données. De telles opérations ont surtout lieu au Moyen-Orient et en Asie, principalement en Chine.[279] La deuxième initiative conjointe de la NSA et la CIA est le « Special Collection Service » (SCS). Il utilise des bâtiments américains officiels, tels que des ambassades et des consulats, comme point de départ pour l'interception de communications secrètes, entre autres du trafic diplomatique (chiffré) dans le pays où est établi le consulat ou l'ambassade.[280] Le personnel du SCS jouit du statut diplomatique.[281] Leurs opérations se déroulent souvent depuis une Secure Compartmented Intelligence Facility (SCIF), situé au dernier étage d'une ambassade. La plupart des diplomates d'une ambassade semblent

---

277 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

278 Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), 3 octobre 2011, 71. http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa – partie 8.

279 Exemple : "*In another more recent case, CIA case officers broke into a home in Western Europe and surreptitiously loaded Agency-developed spyware into the personal computer of a man suspected of being a major recruiter for individuals wishing to fight with the militant group al-Nusra Front in Syria, allowing CIA operatives to read all of his email traffic and monitor his Skype calls on his computer*". http://www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation.

280 US Intelligence 2013 budget http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/#document/p13/a117314 Foreign Policy : "*For example, virtually every U.S. embassy in the Middle East now hosts a SCS SIGINT station that monitors, twenty-four hours a day, the complete spectrum of electronic communications traffic within a one hundred mile radius of the embassy site*". http://www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation?page=0,1).

281 Voir également note 99.

ignorer ce qui se passe dans ces *staterooms*.[282] Selon *Der Spiegel*, le SCS est actif dans 80 pays, dont 19 en Europe.[283] Les documents et *slides* divulgués jusqu'à présent semblent suggérer que le SCS n'est pas actif en Belgique.[284] C'est le SCS qui est soupçonné d'avoir mis le téléphone portable d'Angela Merkel sur écoute.[285]

I.3. RECUEIL EN AMONT (UPSTREAM) AUX ÉTATS-UNIS

20. Plus de 80 % du trafic Internet et téléphonique mondial passe par des câbles en fibre optique, par des points centraux aux États-Unis qui sont exploités par les trois principaux opérateurs télécoms américains (AT&T, Verizon et Sprint). Ce trafic inclut par définition le trafic de données en provenance et à destination de la Belgique. La division « Special Source Operations » de la NSA contrôle l'équipement placé sur ces points de sorte que toutes les données passant par ces points peuvent être copiées et filtrées sur la base des paramètres définis par la NSA.[286] Le principal filtre est le filtre « légal » : en théorie, seules les communications dont au moins un participant n'est pas américain ou ne se trouve pas aux États-Unis peuvent être transmises à la NSA. D'autres filtres doivent veiller à ce que seules les données ayant une valeur en matière de *foreign intelligence* soient transférées à la NSA. Grâce à des programmes tels que XKEYSCORE, les analystes de la NSA sont en mesure d'explorer ces données en amont (*upstream data)* sur la base de *strong selectors* (par exemple : un numéro de téléphone, une adresse e-mail ou un groupe d'adresses IP qui appartiennent à une organisation à laquelle s'intéresse la NSA), de *soft*

---

282 http://www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079-6.html.

283 http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from- berlin-embassy-a-930205.html.

284 http://cpunks.files.wordpress.com/2013/10/20131027-191221.jpg?w=545. L'auteur a vérifié l'origine du *slide*.

285 http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205-2.html.

286 "*There are two common methods used, according to people familiar with the system. In one, a fiber-optic line is split at a junction, and traffic is copied to a processing system that interacts with the NSA's systems, sifting through information based on NSA parameters. In another, companies program their routers to do initial filtering based on metadata from Internet "packets" and send copied data along. This data flow goes to a processing system that uses NSA parameters to narrow down the data further*". http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html.
En ensuite : " *According to a U.S. official, lawyers at telecom companies serve as checks on what the NSA receives. "The providers are independently deciding what would be responsive," the official says. Lawyers for at least one major provider have taken the view that they will provide access only to "clearly foreign" streams of data – for example, ones involving connections to ISPs in, say, Mexico, according to the person familiar with the legal process. The complexities of Internet routing mean it isn't always easy to isolate foreign traffic, but the goal is "to prevent traffic from Kansas City to San Francisco from ending up" with the NSA, the person says.*", S. GORMAN et J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 août 2013 ("New Details Show Broader NSA Surveillance Reach"). L'existence de ce type d'activités a déjà été en partie révélée en 2006 par Mark Klein, lanceur d'alerte de AT&T (Declaration of Mark Klein in support of plaintiffs' motion for preliminary injunction. United States District Court, Northern District of California, 8 June 2006).

selectors (comme des mots clés), ou des *selectors* qui détectent un type de trafic crypté (par exemple au moyen de Tor[287] ou d'un réseau VPN (Virtual Private Network)[288]).[289] Pour prendre cette décision, la NSA peut dès lors examiner le contenu *et* les métadonnées d'une communication.[290] XKEYSCORE est détaillé aux paragraphes 28-31.

21. Un document divulgué et publié par *The Washington Post* mentionne que FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251) et SILVERZEPHYR (US-3273) sont tous des *special source operations* qui acquièrent des données issues du trafic passant par les États-Unis, mais dont ni le destinataire ni l'émetteur ne sont américains.[291] Un autre *slide* cite FAIRVIEW, STORMBREW, BLARNEY et OAKSTAR en tant que *upstream* SIGADS.[292] Selon *The Wall Street Journal*, LITHIUM fait également partie de ce *cluster.*[293]

22. BLARNEY (US-984) est le SIGAD qui faisait initialement référence aux *upstream data* que la NSA obtenait par l'intermédiaire d'AT&T[294], mais il semble avoir été étendu par la suite à plusieurs entreprises.[295] Selon *The Washington Post*, des données provenant de BLARNEY sont toujours traitées.[296] Un *slide* d'une présentation de la NSA, vu l'émission télévisée brésilienne Fantastico, suggérait que BLARNEY assure la '*collection against DNR and DNI FISA Court Order authorized communications*'. DNR est l'acronyme de 'Dial Number Recognition', tandis que DNI signifie « Digital Network Intelligence'. Il est également mentionné dans le *slide* que BLARNEY cible principalement les éléments suivants : « *diplomatic establishment, counterterrorism, counter proliferation, foreign government, economic, military en political/intention of nations* ».[297] Selon un autre *slide*, BLARNEY a commencé à accéder aux communications de « *foreign*

---

287 Tor est un réseau de serveurs qui permettent aux utilisateurs de surfer anonymement. Voir à ce propos https://www.torproject.org/.

288 Souvent utilisé par des entreprises pour permettre à leurs collaborateurs d'accéder à leur réseau depuis leur domicile via un 'tunnel' crypté.

289 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

290 Pour une analyse technique de XKeyscore, voir http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/.

291 http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/#document/p2/a114809.

292 http://www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?wprss=rss_national
The Washington Post avait précédemment censuré les noms STORMBREW et OAKSTAR.

293 http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html.

294 S. GORMAN et J. VALENTINO -DEVRIES, *The Wall Street Journal*, 20 août 2013 ("New Details Show Broader NSA Surveillance Reach").

295 "*BLARNEY's top-secret program summary describes it as "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks*". http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html.

296 *Idem.*

297 http://leaksource.files.wordpress.com/2013/09/blarney.jpg. *Der Spiegel* a précédemment écrit que "*NSA technicians working for the Blarney program have managed to decrypt the UN's internal video teleconferencing (VTC) system*".

establishments, agents of foreign powers and terrorists » dès 1978.[298] *Der Spiegel* a précédemment mentionné que les techniciens de la NSA qui travaillaient pour le programme BLARNEY étaient parvenus à exploiter le système de vidéoconférence (VTC) interne de l'ONU.[299] Selon ce même *slide*, les informations recueillies dans le cadre de BLARNEY ont été envoyées à des « clients externes », dont : US Department of State, CIA, US UN Mission, Joint Chiefs of Staff, Department of Homeland Security, DNI, 2nd parties to Five eyes, National Counterterorrism Center, White House, Defense Intelligence Agency, NATO, Office of Secretary of Defense, ainsi que des commandements militaires (Army, EUCOM).[300] Le programme ressemble beaucoup au programme de la NSA décrit dans l'affaire opposant Jewel à la NSA.[301]

I.4. RECUEIL EN AMONT (UPSTREAM) EN DEHORS DES ÉTATS-UNIS

23. Les informations qui circulent sur les câbles en fibre optique et passent par le territoire d'un des partenaires secondaires des États-Unis (Royaume-Uni, Canada, Australie et Nouvelle-Zélande) sont également partagées avec les États-Unis.[302] Selon Duncan Campbell, l'agence SIGINT suédoise *'Försvarets radioanstalt' (*FRA) partage aussi les données en amont (*upstream data*) qu'elle acquiert via la fibre optique avec « Five Eyes ». Les données ainsi obtenues seraient connues sous le nom de code SARDINE.[303] Campbell affirme que le '*Forsvarets Efterretningstjeneste*' (Danish Defence Intelligence Service) partage aussi des informations avec la NSA. Les données ainsi obtenues seraient connues sous le nom de code DYNAMO.[304] La NSA a également conclu des accords de coopération avec des sociétés de télécoms étrangères « *principalement en Europe et au Moyen-Orient* », selon une source anonyme dans *The Wall Street Journal*.[305] D'après

---

298 Capture d'écran d'un segment montré sur le site http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html ; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large.

299 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

300 Capture d'écran du segment montré sur le site http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html ; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large.

301 https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf. Selon Thomas Drake, ancien collaborateur de la NSA, BLARNEY est "*a key access program facilitated by these commercial arrangements that exploits the Internet data at these junctions. (…) BLARNEY is to the international Internet space as PRISM is to the domestic*". http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

302 http://apps.washingtonpost.com/g/page/world/how-the-nsa-tried-to-collect-less/518/.

303 Témoignage de Duncan Campbell : http://www.youtube.com/watch?v=ZX1tmizZLpc. Ce qui n'a rien de surprenant à la lumière de la « loi FRA » adoptée par la Suède en 2008. http://news.bbc.co.uk/2/hi/europe/7463333.stm.

304 Duncan Campbell testimony to the Council of Europe, 1er octobre 2013. http://www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf, 19.

305 S. GORMAN et J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 août 2013 ("New Details Show Broader NSA Surveillance Reach"). http://online.wsj.com/article_email/SB10001424127887324108204579022874091732470-lMyQjAxMTAzMDIwMDEyNDAyWj.html.

Glenn Greenwald, la NSA ne conclut pas d'accords de coopération directement avec des entreprises étrangères, mais utilise l'accès d'une grande société de télécommunications américaine – jusqu'à présent inconnue – qui collabore avec de telles entreprises étrangères. La société américaine en question a un accès direct à l'infrastructure de télécommunications de son partenaire, qui – à son insu – octroie également un accès à la NSA. Selon Greenwald, ces informations aboutissent dans le programme FAIRVIEW.[306] D'autres câbles en fibre optique sont des cibles légitimes pour les États-Unis dans le cadre de l'interception clandestine du trafic Internet et téléphonique en vertu de l'EO 12333.

24. Le programme *upstream* a également permis l'interception automatique d'e-mails de sociétés de télécommunications françaises tels qu'Alcatel-Lucent. On ne sait pas exactement si le contenu de tous les e-mails de ces adresses a été conservé automatiquement ou si seuls les e-mails contenant certains mots clés et/ou les métadonnées de ce trafic d'e-mails étaient concernés.[307] D'après les fonctions et les opérations effectuées par ces deux sociétés, il ne serait pas impossible que des e-mails similaires d'employés de BICS, Belgacom ou Tecteo aient été interceptés de la même manière.[308]

25. Parmi les données collectées par la division SSO de la NSA via ce recueil en amont, figurent des millions de listes de contacts ou de carnets d'adresses de programmes de messagerie électronique et de conversation instantanée, ainsi que des captures d'écran de toute une boîte de réception électronique. Les listes de contacts de programmes de conversation instantanée peuvent parfois inclure le contenu d'un message, et la boîte de réception d'une personne affiche souvent la première ligne du message.[309] Une présentation PowerPoint de la NSA mentionne que le 10 janvier 2012, 444 743 carnets d'adresses de Yahoo ont été recueillis en une seule journée, 105.068 de Hotmail, 82 857 de Facebook, 33 697 de Gmail et 22 881 d'autres fournisseurs. Les sociétés américaines en question n'ont – selon leurs dires – absolument pas connaissance de la collecte de ces informations.[310] Ce qui signifie que, sur une année, ce sont plus de 250 millions de carnets d'adresses qui sont collectés.

---

306 http://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Par le passé, l'ancien collaborateur de la NSA, Thomas DRAKE, a décrit FAIRVIEW comme un programme-cadre (*umbrella programma*) dont dépendent beaucoup d'autres programmes. http://www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

307 http://www.lemonde.fr/technologies/article/2013/10/21/les-services-secrets-americains-tres-interesses-par-wanadoo-et-alcatel-lucent_3499762_651865.html).

308 Alcatel Lucent fournit entre autres une infrastructure essentielle pour les câbles en fibre optique sous-marins. Voir par exemple http://www.alcatel-lucent.com/solutions/submarine-networks).

309 http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/.

310 Le nombre élevé de carnets d'adresses Yahoo peut s'expliquer par le fait que Yahoo ne crypte pas automatiquement ses données via SSL – contrairement aux autres fournisseurs. En partie en réponse à ces révélations, Yahoo a annoncé qu'il proposerait également le protocole de sécurité SSL par défaut (*by default*) dès janvier 2014. http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_2.html.

26. La NSA admet que nombre de ces carnets d'adresses ne présentent aucune *foreign intelligence value*, d'autant plus que dans 22 % des cas, le propriétaire de la liste d'adresses est inconnu.[311] Or une analyse de ces données permet à la NSA de voir les « connexions secrètes » et les relations d'un groupe beaucoup plus restreint de cibles du type *foreign intelligence*. Ces listes sont stockées dans plusieurs bases de données de la NSA, telles que MARINA, MAINWAY, PINWALE et CLOUDs. Selon une source *intelligence* de *The Washington Post*, un analyste NSA n'est pas autorisé à explorer ces bases de données ni à diffuser les informations qu'elles contiennent, sauf s'il peut démontrer qu'une cible *foreign intelligence* valide se trouve dans ces données.[312]

27. Depuis novembre 2010, les métadonnées collectées en vertu de l'Executive Order 12333 peuvent être utilisées pour établir un *contact chaining* afin d'identifier les relations entre les *foreign intelligence targets* et les habitants des « Five Eyes ».[313] En outre, les données peuvent être complétées par des *enrichment data,* c'est-à-dire des données émanant essentiellement de sources publiques et commerciales, telles que des listes de passagers, des profils Facebook, des codes bancaires, des registres d'électeurs, des données GPS de TomTom et des données fiscales américaines.[314] Étant donné que selon la NSA, il s'agit ici purement de métadonnées et de sources ouvertes, aucun contrôle de la FISC n'est nécessaire pour créer de tels profils.[315]

I.5. CLASSEMENT ET ANALYSE DES DONNÉES (EN AMONT) AVEC XKEYSCORE

28. Une présentation divulguée et datant de février 2008 décrit XKEYSCORE (également connu sous le nom de CrossKeyScore ou XKS) comme étant un *DNI exploitation system/analytic Framework* ».[316] Durant trois à cinq jours[317], XKEYSCORE

---

311 http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/.

312 http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html.

313 http://www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html.

314 "*A top-secret document titled "Better Person Centric Analysis" describes how the agency looks for 94 "entity types", including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A. correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs". (…) A 2009 PowerPoint presentation provided more examples of data sources available in the "enrichment" process, including location-based services like GPS and TomTom, online social networks, billing records and bank codes for transactions in the United States and overseas*". http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

315 *Idem*.

316 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

317 Il arrive que ce type de données ne soit conservé qu'une seule journée. "*One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours*". http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

consigne les données Internet non filtrées *full take*), et durant 30 jours, les métadonnées qui sont recueillies auprès de 150 SIGADS aux quatre coins du monde.[318] Il ne s'agit pas seulement de recueillir des informations en amont (*upstream*), par exemple par le biais de câbles sous-marins, mais aussi des informations émanant de satellites (Fornsat[319]) et de missions diplomatiques et consulaires des États-Unis partout dans le monde (sites F6).[320] En 2012, XKEYSCORE contenait, sur une période de 30 jours, en moyenne 41 milliards d'enregistrements.[321] D'après le *slide*, un tel *full-take* permet à un analyste de trouver dans les métadonnées des cibles qui n'étaient pas encore connues.[322] Un analyste doit d'abord prouver qu'il est sûr à 51 % que sa recherche porte sur une cible étrangère. Les analystes peuvent ensuite explorer XKEYSCORE en temps réel[323] et envoyer des données vers d'autres bases de données, telles que PINWALE, MARINA ou TRAFFICTHIEF[324], où ces informations brutes sont stockées pendant une plus longue période.

29. Les exemples cités dans les *slides* démontrent qu'un analyste peut analyser un très grand volume de données via XKEYSCORE. XKEYSCORE peut lire le contenu de toute activité http, c'est-à-dire tous les e-mails et toutes les pièces jointes, toutes les conversations instantanées[325], toutes les métadonnées d'une communication internet,

---

318 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 6. L'expert de la NSA, Marc AMBINDER, qui a écrit pour les documents de Snowden, décrit Xkeyscore comme suit : " *(it's) not a thing that DOES collecting; it's a series of user interfaces, backend databases, servers and software that selects certain types of metadata that the NSA has ALREADY collected using other methods".* http://theweek.com/article/index/247684/whats-xkeyscore.

319 Selon Duncan CAMPBELL, qui a dévoilé l'existence du GCHQ en 1976, il s'agit du successeur d'Echelon. Ce programme existe toujours, mais a perdu de son intérêt, car les données téléphoniques se déplacent aujourd'hui en grande partie via les câbles en fibre optique. Témoignage de Duncan CAMPBELL au Parlement européen, à visionner sur http://www.youtube.com/watch?v=ZX1tmizZLpc.

320 Présentation de Xkeyscore, divulguée sur http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 5. Selon AMBINDER, d'un point de vue technique, « F6 » renvoie au quartier général du Special Collection Service (SCS) à Beltsville, Maryland, qui recueille des informations à partir d'au moins 75 sites F6, principalement implantés dans des pays où il est impossible d'envoyer des informations à la NSA par le biais des câbles téléphoniques ou en fibre optique ordinaires, puisque les États-Unis ne sont pas techniquement censés y être présents. La NSA ne reconnaît pas l'existence du SCS parce que la plupart des membres du personnel travaillent comme responsables du State Department. http://theweek.com/article/index/247684/whats-xkeyscore et http://theweek.com/article/index/247761/5-nsa-terms-you-must-know.

321 ???

322 Présentation de Xkeyscore, divulguée sur http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

323 *Idem*. Pour de plus amples informations sur ce processus (ainsi que d'autres *slides* originaux), voir http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

324 *Idem*.

325 Xkeyscore permet également d'effectuer des recherches en demandant, par exemple, « *affiche-moi toutes les feuilles de calcul Excel provenant d'Irak et contenant des Media Access Control Addresses* » (23) ou « *affiche-moi tous les documents Word qui mentionnent l'AIEA ou Oussama Ben Laden* » (26), http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation,.

tout l'historique de navigation et toutes les recherches qu'une personne effectue en ligne.[326] En outre, il peut détecter l'utilisation d'une technologie de cryptage ou VPN donnée[327] ou vérifier la langue utilisée par une personne en ligne.[328] XKEYSCORE peut également contrôler les adresses IP de toutes les personnes qui consultent un site web défini par l'analyste.[329] En outre, XKEYSCORE permet de vérifier qui est l'auteur d'un document envoyé en ligne.[330] Au moyen des « profils de vulnérabilité » fournis par les Tailored Access Operations (TAO) de la NSA, XKEYSCORE peut également être utilisé pour trouver des « machines exploitables » dans un pays donné.[331] Un analyste peut également recourir au programme DNI PRESENTER pour lire dans XKEYSCORE le contenu des e-mails et des conversations ou messages privés Facebook stockés.[332]

30. Les *slides*, qui datent de 2008, indiquent qu'à l'époque, XKEYSCORE ne pouvait pas encore intercepter le protocole VoIP (Voice over Internet Protocol)[333], mais que l'on s'attendait à ce qu'il intercepte à l'avenir davantage de métadonnées telles que les *exif tags*.[334]

31. La NSA a reconnu l'existence de XKEYSCORE comme composante de son *lawful foreign signals intelligence collection system*, mais a souligné que l'accès à XKEYSCORE est restreint et que toutes les recherches sont *fully auditable* par un analyste. La NSA insiste sur le fait que plus de 300 terroristes ont été arrêtés sur la base des renseignements issus de XKEYSCORE.[335]

---

326 Xkeyscore enregistre toutes les recherches ainsi que l'utilisation de Google Maps, par exemple. http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 20.

327 Par exemple, XKeyscore permet d'afficher « *tous les documents Word cryptés provenant d'Iran ou toutes les utilisations de PGP en Iran* ». http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 16). Un analyste peut également demander à Xkeyscore de détecter l'utilisation de certaines technologies, par exemple en demandant : « *affiche-moi tous les démarrages VPN dans le pays X et donne-moi les données pour que je puisse identifier les utilisateurs de ce service* ». http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (17).

328 Xkeyscore permet également un suivi des langues (*language tracking*) au moyen du plugin « http activity », qui suit les balises HTML de langue (*HTML language tags*). http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (p.19).

329 *Idem*. Par exemple : tous les Belges qui consultent un site web extrémiste X.

330 http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 21.

331 Pour une analyse technique, voir http://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/.

332 http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

333 Fait référence à des services tels que Skype et Facetime d'Apple.

334 Présentation de Xkeyscore, divulguée sur http://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 32. L'« *exchangeable image file format* » (exif) est une norme technique qui enregistre les métadonnées d'appareils photo numériques, comme la date et l'heure auxquelles une photo numérique a été prise.

335 http://www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml.

I.6. PRISM : RECUEIL EN AVAL DE SIGINT

32. En partie parce qu'un nombre sans cesse croissant d'étrangers ont commencé à faire appel aux services d'entreprises américaines, et en partie parce que ces entreprises ont commencé à crypter leurs communications à l'aide du protocole SSL[336], la NSA a décidé de conclure un accord de coopération avec les plus éminentes de ces entreprises afin qu'elles lui transmettent les données d'utilisateurs d'une manière efficace et rationalisée.[337] Ces négociations ont donné naissance au programme PRISM, qui a permis à la NSA – contrairement à la collecte en amont (*upstream*) – de réceptionner d'une manière structurée des données en aval de neuf grandes sociétés technologiques : Microsoft, Google, Yahoo !, Facebook, PalTalk, YouTube, Skype, AOL et Apple.[338]

33. Tous les fournisseurs PRISM se sont vu octroyer un code. P1 : Microsoft[339], P2 : Yahoo, P3 : Google[340], P4 : Facebook, P5 : PalTalk, P6 : YouTube, P7 : Skype[341], P8 : AOL, PA : Apple.[342]

---

336 Protocole de cryptage utilisé pour sécuriser les communications sur Internet.

337 C.C. MILLER, *The New York Times*, 7 juin 2013 (*"Tech companies concede to surveillance programme"*).

338 Les *slides* les plus complets de PRISM ont été publiés en octobre par le journal *Le Monde*. http://www.lemonde.fr/technologies/article/2013/10/21/espionnage-de-la-nsa-tous-les-documents-publies-par-le-monde_3499986_651865.html.

339 *The Guardian* a en outre décrit des documents de la SSO, qui démontraient que Microsoft et le FBI ont permis que la NSA puisse contourner aisément le cryptage de conversations instantanées d'outlook.com. Un autre document démontre que la NSA a accès aux e-mails de Hotmail, de Windows Live et d'Outlook.com avant qu'ils soient cryptés. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

340 La NSA a ainsi accès à Gmail, aux appels audio et vidéo de Google, aux fichiers Google Drive, au service photo Picasa Web de Google et à la surveillance (en temps réel) des termes de recherche qu'une personne introduit dans Google. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html.

341 *"According to a separate "User's Guide for PRISM Skype Collection", that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of "audio, video, chat, and file transfers" when Skype users connect by computer alone."* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html. Un autre document mentionnait que *"Prism monitoring of Skype video production has roughly tripled since a new capability was added on 14 July 2012. (…) The audio portions of these sessions have been processed correctly all along, but without the accompanying video. Now, analysts will have the complete 'picture', it says"*. http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

342 Les fournisseurs ont commencé à participer au programme PRISM à des moments différents. Microsoft : 11/09/2007, Yahoo : 12/3/2008, Google : 14/01/2009, Facebook : 3/6/2009, PalTalk : 7/12/2009, Youtube : 24/9/2010, Skype : 6/2/2011, AOL : 31/3/2011, Apple : octobre 2012. PRISM a donc seulement démarré après l'adoption du Protect America Act en 2007. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#
En avril 2013, ce journal titrait que l'ajout de Dropbox était imminent. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html.

34. Neuf grands types de données sont recueillis par l'intermédiaire de PRISM et se sont eux aussi vu attribuer un code. A = communications enregistrées (p. ex. les messages privés sur les sites de réseaux sociaux, l'historique des conversations, les e-mails…), B = Instant Messaging (messagerie instantanée), C = RTN-EDC (notification en temps réel du nom d'utilisateur d'un compte et d'un message envoyé), D = RTN-IM (notification en temps réel de la connexion ou déconnexion à une conversation), E = e-mail, F = VoIP (services tels que Skype, y compris la vidéoconférence), G = Full (forum web), H = OSN ('Online Social Networking' – photos, publications sur le mur, activités sur les sites de médias sociaux…) I = informations OSN fournies lors de l'inscription à un service OSN. J = vidéos.[343]

35. Le système semble fonctionner comme suit: un analyste de la NSA peut saisir des *selectors* (adresse e-mail, numéro de téléphone, nom, mais aussi termes de recherche) dans un *Unified Targeting Tool*.[344] Ces *selectors* sont examinés par un supérieur, qui vérifie s'il y a 51 % de chance qu'il s'agisse d'une cible étrangère.[345] Si la NSA souhaite consulter les données enregistrées (par exemple les e-mails dans une boîte de réception), le FBI doit vérifier qu'aucun Américain n'est espionné. Si la NSA souhaite procéder à une surveillance en temps réel, cette vérification supplémentaire du FBI n'est pas nécessaire. Dans les deux cas, l'unité DITU (Data Intercept Technology Unit) du FBI utilise du matériel (*government equipment*) d'une des entreprises participant au programme PRISM pour obtenir des informations sur ces cibles. Le FBI transmet ensuite ce matériel à la CIA ou à la NSA.[346]

36. Le recueil d'informations à propos d'une cible peut également impliquer le recueil des informations relatives à toutes les personnes avec lesquelles la cible a communiqué jusqu'au second degré. Un simple exemple hypothétique démontre que le recueil d'informations à propos d'une cible signifie dans la pratique que les données d'un très grand nombre de personnes peuvent être potentiellement collectées. Lorsqu'une cible a communiqué avec 700 personnes via Facebook ou par e-mail et que ces personnes ont à leur tour communiqué chacune avec 700 personnes, la NSA peut recueillir des données concernant 490 000 personnes.[347]

---

343 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#.

344 " *In another classified report obtained by The Post, the arrangement is described as allowing "collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations", rather than directly to company servers.*" http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

345 Notons que chaque année, la FISC examine uniquement les certificats (voir paragraphe 9), et pas les termes de recherche individuels.

346 "*The information the NSA collects from Prism is routinely shared with both the FBI and CIA. A 3 August 2012 newsletter describes how the NSA has recently expanded sharing with the other two agencies. The NSA, the entry reveals, has even automated the sharing of aspects of Prism, using software that "enables our partners to see which selectors [search terms] the National Security Agency has tasked to Prism". The document continues: "The FBI and CIA then can request a copy of Prism collection of any selector…"* http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

347 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#

37. La NSA trie à son tour les données obtenues en fonction de leur type, puis les soumet à un filtre pour vérifier qu'aucune donnée américaine n'est examinée. Le contenu DNI[348] et les vidéos sont envoyés vers la base de données PINWALE.[349] Les métadonnées des *internet records* sont envoyées vers MARINA[350] et les métadonnées des conversations téléphoniques, vers MAINWAY.[351] Un bulletin interne de la NSA indiquait qu'en 2011, MAINWAY avait réceptionné quotidiennement les métadonnées issues de 700 millions de communications téléphoniques. À partir d'août 2011, 1,1 milliard de métadonnées de conversations téléphoniques est venu s'ajouter chaque jour.[352]

38. Le 5 avril 2013, la *counterterrorism database* de Prism contenait 117 675 cibles de surveillance active.[353] Selon les *slides* divulgués, PRISM est le SIGAD dont sont issues la plupart des informations brutes utilisées pour tous les rapports de la NSA.[354] En 2012,

---

The Washington Post fait également remarquer ceci : "*it is true that the PRISM program is not a dragnet, exactly. From inside a company's data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all*". http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html Et d'ajouter plus loin : "*To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially.*" http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html.

348 Par exemple : des publications sur des forums, des conversations, des e-mails… Bref, du contenu Internet (*internet content*).

349 Pinwale conserve le contenu des communications pendant cinq ans. Le flux de ces informations semble se fonder sur des *dictionary tasked terms* prédéfinis et émaner entre autres des programmes Xkeyscore et PRISM. http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

350 Un *slide* Xkeyscore décrivait Marina comme contenant les "*user activity meta-data with front end full take feeds and back-end selected feeds*". http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu *The Guardian* cite un document qui décrit l'application Marina : "*The Marina metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target," the analysts' guide explains. "This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development." (…) "Of the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of DNI metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection*". http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

351 http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#.

352 http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

353 En comparaison : en décembre 2011, la liste *Terrorist Identities Datamart Environment* (TIDE) du gouvernement américain comptait 740.000 enregistrements (*records*), où une même personne peut apparaître plusieurs fois si son nom est mal orthographié. http://www.dni.gov/files/Tide_Fact_Sheet.pdf.

354 Ce qu'a également confirmé la FISC, voir paragraphe 19. "*According to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relies on PRISM" as its leading source of raw material, accounting for nearly 1 in 7 intelligence reports*". http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-com

des données PRISM sont apparues dans 1 477 éléments du Daily Intelligence Brief du Président américain.[355] Le directeur Clapper de la DNI a confirmé l'existence de PRISM (sans citer nommément le programme) et en a parlé comme étant l'*« une des principales sources »* de la NSA.[356]

I.7. DONNÉES FINANCIÈRES

39. Selon des documents que *Der Spiegel* a pu consulter, la NSA dispose d'une branche *'Follow the money'*, qui surveille les flux monétaires internationaux, surtout en Afrique et au Moyen-Orient. Ces informations atterrissent dans une base de données, baptisée TRACFIN. En 2011, cette base contenait déjà 180 millions d'ensembles de données (*datasets*) concernant des transferts bancaires, des transactions de cartes de crédit et des transferts de fonds. Selon *Der Spiegel*, la NSA conserve ce type de données durant cinq ans.[357]

40. Toujours selon *Der Spiegel*, la NSA connaît en détail les processus internes de sociétés telles que Visa et MasterCard (par exemple, les *payment authorisation processes* et les communications internes chiffrées[358]) et surveille également des modes de paiement alternatifs tels que Bitcoin. Selon *Der Spiegel*, la NSA recueille, via le programme DISHFIRE, des informations relatives à des transactions exécutées à l'aide des cartes de crédit de plus de 70 banques dans le monde – surtout dans les 'territoires en crise' et y compris dans des pays tels que l'Italie, l'Espagne et la Grèce. DISHFIRE est actif depuis le printemps 2009. Les transactions de clients Visa en Europe, au Moyen-Orient et en Afrique ont également été analysées dans le but de mettre au jour des associations financières.[359] Grâce à ces connaissances, plusieurs banques arabes ont été mises sur la *blacklist* du Trésor américain.[360]

---

panies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

355 http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

356 http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa.

357 http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html.

358 "*According to the presentation, the NSA was previously only able to decrypt payment transactions by bank customers, but now they have access to the internal encrypted communication of the company's branch offices. This "provides a new stream of financial data and potentially encrypted internal communications" from the financial service provider, the analysts concluded with satisfaction. This bank data comes from countries that are of "high interest." It's interesting to note that the targeted company is also one of the many SWIFT service partners*". http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html.

359 "*Furthermore, the author concluded, thanks to network analyses and the use of the XKeyscore spying program, NSA analysts had stumbled across the encrypted traffic of a large financial network operator in the Middle East*". http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html.

360 "*In one case, the NSA provided proof that a bank was involved in illegal arms trading -- in another case, a financial institution was providing support to an authoritarian African regime*".

41. D'autres documents démontrent que la division Tailored Access Operations (TAO) de la NSA a acquis, depuis 2006, un accès clandestin au trafic de données interne de SWIFT (Society for Worldwide Interbank Financial Telecommunication).[361] Ce qui est remarquable, étant donné que les États-Unis ont un accord avec l'UE visant à partager les données SWIFT, mais cet accord n'autorise pas l'envoi de données en vrac (*bulk data*).[362] Après ces révélations, le Parlement européen a voté la suspension du 'Terrorist Finance Tracking Program' (TFTP Agreement) le 23 octobre 2013.[363] Dans une déclaration, le Commissaire Malmström a fait savoir que l'accord TFTP ne serait pas suspendu.[364]

I.8. MÉTADONNÉES DE CONVERSATIONS TÉLÉPHONIQUES AMÉRICAINES

42. Aux États-Unis, le débat relatif à la NSA porte surtout sur le recueil de données téléphoniques américaines par la NSA, entre autres sur la base de la section 215 *business records* introduite par le Patriot Act dans le FISA.[365] En vertu de cette section, les États-Unis ont pu contraindre les principaux opérateurs télécoms américains à mettre à la disposition de la NSA toutes les métadonnées des conversations téléphoniques au départ ou à destination des États-Unis. Selon la NSA, ces données peuvent uniquement être consultées aux fins de la lutte contre le terrorisme. La consultation peut uniquement commencer par un numéro de téléphone ayant été précédemment associé à une organisation terroriste étrangère (*a seed*).[366]

I.9. DONNÉES DE SMARTPHONES

43. Selon *Der Spiegel*, la NSA dispose de la capacité requise pour obtenir un large éventail de données de smartphones émanant de *high interest targets*.[367] La NSA avait accès aux listes de contacts, journaux d'appels, trafic SMS, brouillons de SMS et données de localisation de plateformes mobiles d'Apple (IOS), de Google (Android) et de

---

http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html.

361 http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html "Since then, it has been possible to read the 'SWIFT printer traffic from numerous banks'".

362 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0005:0014:EN:PDF.

363 European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)) http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//EN.

364 European Commission, Memo, 23 octobre. http://europa.eu/rapid/press-release_MEMO-13-928_en.htm.

365 Voir paragraphe 6.

366 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships. 9 août 2013.

367 Voir aussi paragraphe 19.

BlackBerry.[368] Par exemple, la NSA a accès à 38 applications iPhone, telles que l'utilisation de la fonction de cartographie intégrée, la messagerie vocale et les photos, Google Earth, Yahoo et Facebook Messenger.[369]

I.10. DONNÉES PNR

44. Par le biais de l'accord Passenger Name Records (PNR) de 2012, le ministère américain de la Sécurité intérieure (US Department of Homeland Security (DHS)) obtient les données PNR des passagers qui prennent l'avion sur le territoire de l'UE à destination des États-Unis. Ces données se composent des informations qu'un passager a fournies à la compagnie aérienne, par exemple : le nom du passager et des personnes qui l'accompagnent éventuellement, leurs adresses et numéros de téléphone, les dates de voyage, la destination finale, les détails du billet, le mode de paiement, le numéro de carte de crédit, les détails des bagages… La liste exhaustive figure en annexe à l'accord.[370] Le DHS peut partager ces données avec des services nationaux[371] et des pays tiers.[372] Ces données sont utilisées à des fins de prévention, de recherche et de jugement de crimes terroristes et autres crimes transfrontaliers graves.[373] Après six mois, toutes les données personnelles sont masquées et après cinq ans, les données sont stockées dans une base de données 'passive'. Les données peuvent être utilisées pendant dix ans à des fins de prévention de crimes transfrontaliers et pendant quinze ans dans le cadre de la lutte contre le terrorisme.[374]

I.11. EFFORTS DE LA NSA CONTRE LE CRYPTAGE

45. *The New York Times* a publié une *briefing sheet* que la NSA a portée à l'attention du GCHQ en 2010 à propos d'un programme intitulé BULLRUN. Dans ce briefing, la NSA suggère qu'elle peut décrypter ou contourner les protocoles de cryptage les plus utilisés pour la sécurisation du commerce mondial, des systèmes bancaires, des données médicales et de l'utilisation d'Internet (comme l'envoi d'e-mails, les recherches en ligne, les conversations instantanées et les conversations téléphoniques en ligne). Sont

368 "*The presentation notes that the acquisition of encrypted BES (Blackberry Services) communications requires a "sustained" operation by the NSA's Tailored Access Operation department in order to "fully prosecute your target. (…) The alleged telecommunications surveillance has been a targeted activity that was performed without the smartphone makers' knowledge*". M. ROSENBACH, L. POITRAS et H. STRAK, *Der Spiegel,* 9 septembre 2013, ("iSpy : How the NSA Accesses Smartphone Data").

369 *Idem*.

370 http://register.consilium.europa.eu/pdf/en/11/st17/st17434.en11.pdf,36.

371 *Idem*, article 16.

372 *Idem*, article 17.

373 *Idem*, article 4.

374 *Idem*, article 8.

concernés les protocoles suivants : TLS/SSL[375], HTTPS[376], SSH[377], VPN[378], ainsi que les conversations instantanées[379] et les communications VOIP[380] cryptées. Jusqu'à présent, les détails techniques de ce qui a été précisément piraté n'ont pas été divulgués.[381, 382] L'existence de ces moyens de décryptage ainsi que l'utilisation de toutes les données exploitées (tant sous la forme de *plaintext* que de métadonnées) qui en sont issues ont été classifiées comme 'Exceptionally Controlled Information' (ECI), un niveau (*level*) supérieur à 'Top Secret'.[383]

46. Une demande de budget datant de 2012 a également révélé l'existence du projet Sigint Enabling Project, qui vise à influencer en secret des sociétés Internet américaines et étrangères à adapter la conception de leurs produits de manière à permettre leur exploitation. Le programme englobe toute une série d'activités : (1) Collaborer avec des entreprises en vue d'installer des 'portes dérobées' dans des systèmes de décryptage commerciaux, des systèmes informatiques, des réseaux et des terminaux de communication (*endpoint communication devices)* qui sont utilisés par des 'cibles'.[384] Cette collaboration peut être volontaire[385] ou imposée en vertu du FISA.[386] (2) Influencer des normes et spécifications techniques en matière de technologies commerciales à clé

---

375 Transport Layer Security/Secure Sockets Layer. Protocole le plus utilisé pour l'envoi d'informations sur Internet et sur des serveurs internes. La sécurisation du protocole HTTPS consiste à appliquer le cryptage TLS/SSL à un site web.

376 Hypertext Transfer Protocol Secure. Méthode permettant d'envoyer en toute sécurité des informations financières et des mots de passe d'un ordinateur à un réseau. Des sites tels que Facebook, Twitter et Gmail utilisent souvent le HTTPS par défaut. Cette sécurisation est reconnaissable au verrou qui s'affiche avant « https » dans la barre d'adresse du navigateur web.

377 Secure Shell. Permet aux utilisateurs Linux et Mac d'accéder à un ordinateur à distance.

378 Virtual Private Network. Souvent utilisé par des entreprises pour permettre à leurs collaborateurs d'accéder à leur réseau depuis leur domicile via un 'tunnel' crypté.

379 Par exemple, le programme Adium permet un cryptage de bout en bout (*end to end*) et les données ne peuvent être décryptées à aucun stade du transfert.

380 Fait référence à des services tels que Skype et Facetime d'Apple.

381 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us Des experts ont remarqué que les documents ne montrent pas quels systèmes la NSA a décryptés au moyen de simples formules mathématiques et lesquels l'ont été au moyen d'un piratage ou d'une collaboration avec des développeurs. Un système tel que PGP (Pretty Good Privacy) fonctionnerait toujours. Pour de plus amples informations, voir (les liens) : http://www.washingtonmonthly.com/political-animal-a/2013_09/the_nsa_is_mostly_not_breaking046760.php ou http://www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html.

382 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

383 http://www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-crypt analysis.

384 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

385 *"In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a back door into the product before it was shipped, someone familiar with the request told The Times"*. http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

386 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

publique (*commercial public key technologies)*, y compris la norme de 2006 du National Institute of Standards and Technology.[387] (3) Poursuivre la collaboration avec d'éminents opérateurs de télécommunications (*telecommunications carriers).*[388] La méthode la plus controversée consiste toutefois à dérober subrepticement des clés de cryptage. Des documents de la NSA démontrent que la NSA possède une base de données interne (Key Provisioning Service), qui contient les clés de cryptage de produits commerciaux spécifiques. Lorsqu'une clé donnée ne figure pas dans la base, une demande est adressée au Key Recovery Service, dont on affirme qu'il acquiert des clés en piratant les serveurs des entreprises qui ont créé lesdites clés. Pour que cette méthode reste secrète, la NSA ne partagerait que des messages décryptés avec d'autres services lorsque les clés ont été obtenues par des moyens légaux.[389]

47. Le 4 octobre 2013, *The Guardian* et *The Washington Post* ont révélé comment la NSA a tenté, depuis 2006, d'identifier et d'espionner des utilisateurs du réseau Tor.[390] Il s'agit d'un réseau de serveurs qui permet aux utilisateurs de surfer anonymement.[391] Les utilisateurs peuvent utiliser ce réseau à l'aide d'un logiciel spécial et complexe. Une autre méthode plus simple consiste à télécharger le Tor Browser Bundle (TBB), une version de Firefox qui transfère automatiquement des données sur le réseau Tor. Il ressort des documents qu'en 2007, la NSA a pu distinguer des utilisateurs TBB de simples utilisateurs Firefox[392], mais que, cette même année, elle n'était pas encore parvenue à pirater le réseau Tor. Une présentation de la NSA datant de juin 2012 mentionne que la NSA ne sera jamais en mesure de désanonymiser simultanément tous les utilisateurs Tor et qu'elle ne possède pas de technique permettant de désanonymiser un utilisateur donné sur demande. Une analyse manuelle permet toutefois de désanonymiser un 'très petit nombre' d'utilisateurs Tor.[393] Les *slides* de la division Tailored Access Operations (TAO) de la NSA décrivent comment la NSA a exploité les vulnérabilités de JavaScript dans Firefox à l'aide des programmes EGOTISTICALGOAT et EGOTISTICALGIRAFFE.[394] Ces vulnérabilités auraient disparu avec la dernière mise à jour de Firefox en

---

387 *Idem*.

388 http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

389 http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

390 *The Washington Post* a mis en ligne un document de 49 pages datant de 2006, qui décrit les méthodes qui permettraient la désanonymisation potentielle à grande échelle d'utilisateurs Tor. http://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/. Déclaration de J. CLAPPER à propos des révélations : http://icontherecord.tumblr.com/post/63103784923/dni-statement-why-the-intelligence-community.

391 http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.

392 http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/#document/p5/a124608.

393 http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document?utm_source=hootsuite&utm_campaign=hootsuite.

394 http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.

janvier 2013[395], mais on ne sait pas très bien si la NSA est parvenue à contourner ce problème entre-temps.[396]

48. Sous le nom de code Quantum, la NSA a placé des serveurs Quantum secrets à des emplacements importants de l'infrastructure Internet afin de pouvoir mener une attaque de type 'homme du milieu' (*man in the middle*) sur des utilisateurs Tor.[397] Ce qui signifie que ces serveurs peuvent réagir plus rapidement que d'autres sites Internet et peuvent envoyer l'utilisateur vers une imitation infectée du site Internet demandé qui se trouve sur un serveur FoxAcid. Les serveurs de ce système FoxAcid sont exploités par la TAO et peuvent contaminer des ordinateurs de différentes façons et pour de longues périodes.[398] La consultation de la page d'accueil d'un serveur FoxAcid n'engendrerait pas directement la contamination, car il faut pour cela une URL spécifique créée par la TAO. Cette URL permettrait au serveur FoxAcid de savoir exactement quelle cible visite le serveur FoxAcid.[399] FoxAcid est un système CNE général utilisé pour plusieurs formes de cyberattaques. Il ne sert donc pas seulement à identifier des utilisateurs Tor, loin de là. Des documents émanant de *Der Spiegel* suggèrent, par exemple, que des serveurs Quantum seraient (en partie) à l'origine de l'attaque de Belgacom.[400]

II. LE GOVERNMENT COMMUNICATIONS HEADQUARTERS (GQHQ) BRITANNIQUE

II.1. LE CADRE LÉGAL BRITANNIQUE DU RECUEIL D'INFORMATIONS SUR DES CIBLES ÉTRANGÈRES

49. En 1994, l'Intelligence Services Act a défini pour la première fois les fonctions du Government Communications Headquarters (GCHQ). L'agence SIGINT britannique a notamment pour mandat de surveiller ou de perturber « *les émissions électromagnétiques,*

---

395 http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

396 "*In anticipation of a new release of Firefox, one agency official wrote in January that a new exploit was under development: 'I'm confident we can have it ready when they release something new, or very soon after'*". http://www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story_2.html.

397 B. SCHNEIER: " *More specifically, they are examples of "man-on-the-side" attacks* ". http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

398 "*After identifying an individual Tor user on the internet, the NSA uses its network of secret internet servers to redirect those users to another set of secret internet servers, with the codename FoxAcid, to infect the user's computer. FoxAcid is an NSA system designed to act as a matchmaker between potential targets and attacks developed by the NSA, giving the agency opportunity to launch prepared attacks against their systems. Once the computer is successfully attacked, it secretly calls back to a FoxAcid server, which then performs additional attacks on the target computer to ensure that it remains compromised long-term, and continues to provide eavesdropping information back to the NSA*". http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

399 *Idem.*

400 http://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

acoustiques et autres, ainsi que tout dispositif produisant de telles émissions ».[401] L'agence doit transmettre des informations sur ces émissions à l'armée britannique, au gouvernement et à d'autres services[402] lorsque le requièrent la sécurité nationale du Royaume-Uni (avec une référence spécifique à la politique de défense et étrangère du Royaume-Uni) et le bien-être économique du Royaume-Uni (eu égard aux actes et intentions de personnes en dehors des Iles britanniques), ainsi qu'à des fins de prévention et de recherches de crimes graves.[403]

50. Le Royaume-Uni ne dispose d'aucune législation spécifique régissant exclusivement l'utilisation de *foreign intelligence*, mais le Regulation of Investigatory Powers Act (RIPA) opère une distinction entre la surveillance 'interne' et 'externe', où cette dernière catégorie renvoie à la surveillance de communications dont au moins une extrémité se trouve au Royaume-Uni.[404] Dans ces cas-là, le GCHQ ne doit demander aucune réquisition visant une personne ou un endroit spécifique[405], mais peut demander une réquisition pour, par exemple, intercepter des données d'une liaison externe de télécommunications (comme un câble en fibre optique spécifique qui court entre le Royaume-Uni et le continent européen).[406] À titre d'exemple, tous les câbles en fibre optique qui arrivent en Belgique sont reliés à un point d'atterrissement au Royaume-Uni. Le câble Tangerine relie Broadstairs à Ostende ; Concerto relie Zeebruges à Sizewell et Thorpeness, et le Pan-European Crossing relie Bredene à Dumpton Gap. Le grand câble SeaMeWe-3, qui est en partie détenu par Belgacom, relie Ostende à Goonhilly Downs au Royaume-Uni, mais compte de nombreux autres points d'atterrissement en Arabie saoudite, en Malaisie et en Chine.

51. Une réquisition à si large portée est délivrée par le Secretary of State, qui décrit dans un 'certificat' quel élément requiert précisément un examen[407] dans l'intérêt de la sécurité nationale du Royaume-Uni, pour prévenir ou rechercher des crimes graves ou pour préserver le bien-être économique du Royaume-Uni.[408] Le contenu des certificats

---

401 Intelligence Services Act 1994, Chapter 13, s3, (1)(a).

402 Intelligence Services Act 1994, Chapter 13, s3, (1)(b).

403 Intelligence Services Act 1994, Chapter 13, s3, (2).

404 RIPA, s20.

405 RIPA, s.8.4. L'interception est définie de la manière suivante à la section s.2.2 : "*A person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he- (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of the system, or (c) monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication. .*"

406 "*Lawyers at GCHQ speak of having 10 basic certificates, including a "global" one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus. Other certificates have been used for "special source accesses" – a reference, perhaps, to the cables carrying web traffic. All certificates have to be renewed by the foreign secretary every six months*". http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

407 RIPA, s8.4(b).

408 RIPA, s.5(3)a-c. *The Guardian* cite un document du GCHQ comme suit : "*The certificate is issued with the warrant and signed by the secretary of state and sets out [the] class of work we can do under it … cannot list numbers or individuals as this would be an infinite list which we*

est secret, mais selon des documents consultés par *The Guardian*, la formulation utilisée est très large et permet d'intercepter des éléments sur des thèmes vastes, tels que les intentions politiques de gouvernements étrangers, la situation militaire d'autres pays, le terrorisme, le trafic de drogues international et la fraude. Selon *The Guardian*, il existe au moins dix certificats de ce type.[409] Selon le RIPA, un tel mandat est initialement valable trois mois[410], mais peut être renouvelé tous les six mois.[411] Des sociétés de télécommunications peuvent être obligées de collaborer à l'interception de ces communications.[412]

52. Il convient de souligner que le contenu de la réquisition et du certificat n'est pas clairement précisé. La loi n'est pas non plus très claire à ce sujet. L'Intelligence Security Committee (ISC), qui contrôle le GCHQ, a annoncé que *« des directives et procédures plus détaillées seront élaborées afin que le GCHQ respecte le Human Rights Act de 1998 »*. L'ISC va désormais examiner l'interaction complexe entre l'ISA, le Human Rights Act et le RIPA, et les procédures qui les régissent.[413]

53. La loi permet également au GCHQ de pirater à distance des systèmes informatiques dans le but d'obtenir des données.[414] En vertu de la section 7 de l'ISA, toute action du GCHQ en dehors du Royaume-Uni est exemptée de toute responsabilité civile ou pénale si elle s'appuie sur une autorisation du Secretary of State.

II.2. NATURE ET AMPLEUR DU RECUEIL DE DONNÉES BRITANNIQUE

54. Selon *The Guardian*, le GCHQ a entamé les préparatifs du projet Mastering the Internet (MTI) à la base de Bude début 2007.[415] L'objectif était de recueillir des données étrangères en amont (*upstream*), en plaçant du matériel *deep packet inspection* sur les

---

couldn't manage". http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

409 http://www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world. *The Guardian* cite un mémo interne au GCHQ datant d'octobre 2011 : "*[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors*". http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

410 RIPA, s9.6.c.

411 RIPA, s9.6.b. Pour de plus amples informations sur les *s(8)4 warrants*, voir UK Home Office, Interception of Communications Code of Practice. TSO, London, p.22-27, disponible à l'adresse https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf.

412 RIPA, s.12.

413 Intelligence and Security Committee of Parliament, Statement on GCHQ's alleged interception of communications under the US PRISM Programme. 17 juillet 2013, disponible à l'adresse http://isc.independent.gov.uk/news-archive/17july2013.

414 Voir Computer Misuse Act 1990, s.10 ; RIPA, s32 et ISA, s.5.

415 Outre le projet MTI, il convient également de citer un autre programme, baptisé *Global Telecoms Exploitation*, dont l'objectif n'est pas clair. http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

câbles sous-marins à leur arrivée sur les côtes britanniques.[416] En mai 2009, *The Register* et *The Sunday Times* ont annoncé que le financement du MTI avait été approuvé en octobre 2007. Plus d'un milliard de livres sterling seraient affectées à cette collecte en amont (*upstream*) pour les trois années suivantes.[417] Le GCHQ a reconnu l'existence du projet MTI, mais a souligné qu'il n'était pas en train d'élaborer une technologie capable de surveiller toutes les utilisations d'Internet et du téléphone *au Royaume-Uni*.[418]

55. À un moment indéterminé entre 2010 et 2011, le GCHQ a atteint son objectif et a commencé à contraindre par mandat les exploitants de câbles commerciaux en fibre optique de collaborer en tant qu'*intercept partners*. Ce processus de collaboration forcée porte le nom de *special source exploitation,* et les *intercept partners* sont indemnisés pour les coûts générés.[419] Plus tard, le *Suddeütsche Zeitung* divulguait le nom des entreprises participantes. Elles étaient toutes les sept connues sous un autre nom de code : BT (Remedy), Verizon Business (Dacron), Vodafone Cable (Gerontic), Global Crossing (Pinnage), Level 3 (Little), Viatel (Vitreous) et Interoute (Streetcar).[420] Les câbles en fibre optique qui arrivent en Belgique (voir paragraphe 50) sont tous exploités par une de ces entreprises.

56. Ces informations en amont (*upstream*) sont d'abord filtrées via le programme TEMPORA afin d'exclure le trafic Internet qui occupe un volume important (comme les téléchargements de films ou de musique) et d'ainsi réduire le volume d'environ 30 %.[421] Le reste des informations en amont (*upstream*) est filtré sur la base de *hard selectors* (comme des numéros de téléphone et des adresses e-mail) et de *soft selectors* (comme des critères de recherche). Selon *The Guardian*, 40 000 de ces sélecteurs ont été choisis par le GCHQ et 31 000 par la NSA.[422] Les certificats élaborés déterminent le choix de ces *selectors*. Les données non filtrées sont jetées, les métadonnées restantes sont conservées durant trente jours et le contenu, durant trois jours.[423] Une source du journal *The Guardian* semble suggérer que toutes les données 'filtrées' sont conservées et peuvent être consultées par l'Interception Commissioner britannique, sans savoir précisément s'il s'agit de toutes les informations stockées après filtrage des *selectors* ou uniquement des

---

416 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Un premier projet expérimental connu sous le nom de *Cheltenham Processing Centre* (CPC) poursuivait le même objectif. À partir de mars 2010, il est fait référence à ce projet en tant qu'initiative conjointe GCHQ/NSA baptisée TINT.

417 Selon ces articles, Lockheed Martin et Detica collaboreraient au projet MTI. Depuis 2008, ces sociétés ont effectivement publié des offres d'emploi relatives au contrat MTI. http://www.theregister.co.uk/2009/05/03/gchq_mti/ ; http://www.timesonline.co.uk/tol/news/politics/article6211101.ece.

418 (impression de l'auteur) http://www.telegraph.co.uk/technology/news/5271796/Government-not-planning-to-monitor-all-web-use.html.

419 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

420 http://www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.

421 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

422 *Idem*.

423 http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work Il est intéressant de noter que dans certains cas, le GCHQ considère même des mots de passe comme des métadonnées.

données effectivement utilisées.[424] Ces données peuvent ensuite être – entre autres – examinées rétroactivement dans le cadre de la recherche de suspects encore inconnus des services de renseignement britanniques ou américains.[425]

57. Pour le reste, le recueil porte également sur toutes les informations en amont (*upstream*) qui sont également recueillies par la NSA dans le cadre de sa collecte en amont (voir paragraphe 29) : contenu des e-mails, historique de navigation, messages Facebook, documents ajoutés en pièces jointes… Il convient de remarquer ici que des analystes peuvent également décider de recueillir toutes les métadonnées et tout le contenu des contacts d'une cible s'ils l'estiment proportionnel.[426] Au moins 300 analystes du GCHQ et 250 de la NSA ont un accès direct aux données de TEMPORA.[427] Nombre de métadonnées sont stockées par la NSA.[428] En février 2011, la NSA indiquait dans un document que le GCHQ « *traitait plus de données* » que la NSA.[429] En 2012, le GCHQ est parvenu à traiter 600 millions d' 'événements téléphoniques' par jour, écouter 200 câbles en fibre optique et traiter des données de 46 de ces câbles simultanément. *The Guardian* a estimé que le GCHQ a ainsi accès en théorie à 21,6 pétaoctets par jour, soit 192 fois le contenu de tous les livres de la British Library ou du Congress.[430]

II.3. LOGICIEL MALVEILLANT CHEZ BELGACOM

58. Le 21 juin 2013, Belgacom trouve un logiciel malveillant (*malware)* dans son système informatique interne. Après l'aide infructueuse de sous-traitants tels que Microsoft et HP, Belgacom demande à la société néerlandaise Fox-IT d'examiner ce logiciel malveillant.[431] Après un examen approfondi par Fox-IT, Belgacom dépose, le 19 juillet 2013, une plainte contre X auprès du parquet fédéral pour accès frauduleux à ses systèmes informatiques internes. L'enquête est dirigée par la police judiciaire de Bruxelles (Regional Computer

---

424 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

425 http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

426 "*If analysts believe it is proportional, they can look at all the traffic – content and metadata – relating to all of the target's contact*". http://www.theguardian.com/uk/2013/jun/23/mi5-feared-gchq-went-too-far.

427 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

428 http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

429 http://www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

430 http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa ?CMP=twt_fd Et *The Guardian* d'ajouter : "*The system seems to operate by allowing GCHQ to survey internet traffic flowing through different cables at regular intervals, and then automatically detecting which are most interesting, and harvesting the information from those. The documents suggest GCHQ was able to survey about 1,500 of the 1,600 or so high-capacity cables in and out of the UK at any one time, and aspired to harvest information from 400 or so at once – a quarter of all traffic. As of last year, the agency had gone halfway, attaching probes to 200 fibre-optic cables, each with a capacity of 10 gigabits per second. In theory, that gave GCHQ access to a flow of 21.6 petabytes in a day, equivalent to 192 times the British Library's entire book collection*". http://www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

431 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Voir http://www.youtube.com/watch ?v=ayR6CAuNE4w.

Crime Unit) avec le soutien (technique) de la Federal Computer Crime Unit (FCCU) et du Service général du renseignement et de la sécurité (SGRS).[432] En septembre, le président de la Commission de la protection de la vie privée décide d'ouvrir une enquête distincte, en collaboration avec Belgacom et l'Institut belge des services postaux et des télécommunications (IBPT), afin de déterminer les circonstances exactes de cet incident. Dans un communiqué de presse du 16 septembre 2013, Belgacom annonce avoir supprimé « *un virus inconnu* » durant le week-end des 14 et 15 septembre. Selon Belgacom, « *au stade actuel, il n'y a aucune indication d'impact pour les clients ou leurs données* ».[433] Le coût de l'opération de nettoyage est alors estimé à cinq millions d'euros.[434]

59. D'après un communiqué de presse du parquet, vu l'engagement de moyens financiers et logistiques considérables par les intrus et sa complexité technique, l'attaque pointe dans la direction d'une opération d'espionnage étatique visant le recueil d'informations stratégiques.[435] Par la suite, Belgacom confirme que 124 des 26 600 appareils[436] connectés au système Windows interne de Belgacom ont été compromis[437] par ce que les experts appellent une *advanced persistent threat* (menace persistante avancée).[438] La description des symptômes de ce *malware* relève du secret de l'instruction, mais la FCCU a autorisé la divulgation du *malware*, dans la mesure du possible, afin que d'autres institutions (belges et européennes) puissent vérifier si elles ont été infectées. Les informations sont entre autres partagées avec la Computer Emergency Response Team (CERT-EU) de l'Union européenne.

60. *De Standaard* mentionne, en s'appuyant sur des sources proches du dossier et évoluant dans les milieux des services de sécurité, que la NSA se cache derrière cette attaque et que la NSA visait particulièrement les activités de BICS (Belgacom International Carrier Services), une filiale de Belgacom.[439] Belgacom détient 57,6 % de BICS, Swisscom 22,4 % et l'opérateur sud-africain MTN 20 %. BICS fournit des services à différents opérateurs de télécommunications dans différents pays et exploite entre autres – avec un groupe d'autres entreprises – les câbles sous-marins en fibre optique TAT-14, SEA-ME-WE3 et SEA-ME-WE4 (voir également paragraphe 50). Ce qui permettrait, par exemple, d'intercepter le trafic Internet et téléphonique en provenance de la Syrie, du

---

432 M. EECKHAUT, P. DE LOBEL, *De Standaard*, 17 septembre 2013 ("Natuurlijk zat de NSA hier achter").

433 Belgacom, Belgacom prend action dans le cadre de sa sécurisation IT. 16 septembre 2013. http://www.belgacom.com/be-fr/newsdetail/ND_20130916_Belgacom.page.

434 P. DE LOBEL, N. VANHECKE, *De Standaard*, 21 septembre 2013, ("Op het randje van de catastrofe").

435 M. EECKHAUT, P. DE LOBEL, *De Standaard*, 17 septembre 2013 ("Natuurlijk zat de NSA hier achter").

436 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. http://www.youtube.com/watch?v=ayR6CAuNE4w.

437 X., *De Standaard*, 16 septembre 2013 («Bellens : 'Geen aanwijzing dat Belgacomklanten zijn getroffen'"). http://www.standaard.be/cnt/dmf20130916_00743534.

438 DOD, *De Standaard*, 17 septembre 2013 ("Zeg nooit 'virus' tegen advanced persistent attack"). http://www.standaard.be/cnt/dmf20130916_00745157. Pour de plus amples informations, voir par exemple https://www.damballa.com/knowledge/advanced-persistent-threats.php.

439 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 septembre 2013 ("NSA verdacht van hacken Belgacom"). Voir http://www.standaard.be/cnt/dmf20130915_00743233.

Yémen et de l'Afghanistan. C'était une des raisons de l'attaque que *De Standaard* a citées dans son premier article.[440] Dans un communiqué, BICS affirme le 16 septembre 2013 que « *nous n'avons aucune indication permettant de dire que notre réseau télécoms, par lequel le trafic de communication est acheminé, a été touché par ces opérations d'espionnage. C'est notre système informatique interne, qui est intégré avec celui de Belgacom, qui est concerné par le hacking* ».[441]

61. Le 20 septembre 2013, *Der Spiegel* a publié des *slides* non datés issus des documents de Snowden, dans lesquels le 'Network Analyses Centre' du GCHQ évoque les réussites obtenues dans le cadre de l''Operation Socialist'. Dans cette opération, Belgacom était connue sous le nom de Merion Zeta. Il semble que des employés qui occupent des fonctions-clés au sein de BICS ont été dirigés, via des serveurs Quantum contrôlés par la NSA, vers un autre serveur contrôlé par la NSA (serveur Fox Acid), lequel a utilisé à son tour une vulnérabilité du navigateur de la cible pour installer un logiciel malveillant sur l'ordinateur de la victime (voir aussi paragraphe 48). D'après les *slides* de *Der Spiegel*, le but ultime de l''Operation Socialist' était d'exploiter le principal routeur GRX de Belgacom afin de pouvoir mener à partir de là des attaques *man in the middle* sur des cibles qui utilisent les services itinérants (*roaming*) depuis leur smartphone à l'étranger.[442] Selon les *slides*, le GCHQ était très proche du but.[443] BICS est connu dans le monde entier en tant que fournisseur de services 3GRX. Ces services doivent entre autres permettre à un opérateur téléphonique local d'assurer le roaming des appels de ses clients dans plus de 190 pays.[444] Les connexions VPN de BICS et MyBICS, application en ligne utilisée pour le contact avec les clients, ont également été considérées comme des cibles intéressantes.

62. Après les révélations parues dans *Der Spiegel*, *De Standaard* a cité des sources proches de l'instruction judiciaire qui restent convaincues que l'attaque provient des États-Unis étant donné la signature du logiciel malveillant et surtout l'endroit vers lequel mènent les pistes. Selon les enquêteurs, les États-Unis sont la principale destination, et les pistes ne conduisent que « *dans une mesure très restreinte* » au Royaume-Uni.[445] À la demande du Premier ministre Di Rupo, la Sûreté de l'État belge a officiellement demandé des explications à son homologue britannique.[446]

---

440 M. EECKHAUT, P. DE LOBEL, *De Standaard*, 17 septembre 2013 ("Natuurlijk zat de NSA hierachter").

441 G. QUOISTIAUX, *Trends*, 16 septembre 2013 («Découvrez BICS, la filiale de Belgacom qui serait visée par la NSA"). http://trends.levif.be/economie/actualite/decouvrez-bics-la-filiale-de-belgacom-qui-serait-visee-par-la-nsa/article-4000400052938.htm.

442 http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html. Pour de plus amples détails techniques, voir https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Langlois_Attacking_GRX.pdf.

443 http://www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663-3.html.

444 http://www.bics.com/sites/default/files/mosaic/3GRX_web.pdf.

445 N. VANHECKE, *De Standaard*, 21 septembre 2013 ("Operatie socialist : succes !").

446 K. VAN DE PERRE, *De Morgen*, 4 octobre 2013 («België vraag uitleg aan Britten over Belgacom-hacking").

63. En s'appuyant sur 'diverses sources', la chaîne néerlandaise NOS indique le 3 octobre que fin 2011, une équipe du GCHQ a attaqué le cœur de Belgacom par le biais de canaux nommés (*named pipes)*, méthode sophistiquée utilisée pour envoyer une communication presque invisible sur un réseau. Selon la chaîne NOS, des données de conservation (*loggegevens*) confirment qu'il s'agit de l'Angleterre: les activités d'espionnage sont clairement moins nombreuses pendant les jours fériés et le temps de midi anglais.[447] NOS affirme qu'une fois le réseau piraté, les Britanniques ont eu un accès presque illimité au réseau Belgacom.[448] Avant cela, une autre source a révélé au journal *De Standaard* que celui qui faisait cela pouvait faire tout ce que le gestionnaire réseau le plus haut placé de Belgacom peut faire et possédait toutes les clés, tous les mots de passe et tout le contrôle.[449] NOS affirme également qu'une autre équipe a ensuite cherché des informations spécifiques. Informations qui ont par la suite été partagées avec la NSA.[450] Selon des «*sources proches de l'enquête*», les responsables ont regardé un peu partout et ont pris ce qu'ils pouvaient.[451] Selon *De Standaard*, BICS fournit des services que de nombreux clients importants peuvent utiliser: Swift, Electrabel, bpost, Belgocontrol, l'OTAN à Evere, la Commission européenne et le Parlement européen à Bruxelles et Strasbourg, le SHAPE (Supreme Headquarters Allied Powers Europe) à Mons, mais aussi le quartier général du Commandement aérien allié de l'OTAN à Ramstein.[452] Lors d'une audition au Parlement européen, deux hauts responsables de Belgacom ont nié que le service secret britannique aurait eu accès aux réseaux téléphoniques d'institutions européennes. Selon Belgacom, il n'y a eu aucun débordement via leur système vers des systèmes de clients. Et donc pas non plus vers des systèmes d'instances européennes.[453]

64. À l'heure actuelle, il est cependant impossible de dire avec certitude quelles données ont été précisément interceptées. Tant Belgacom[454], la FCCU[455], que Frank Robben[456], co-rapporteur du rapport Belgacom de la Commission de la protection de la vie privée, ont déclaré que le virus proprement dit utilisait des techniques de cryptage pour masquer les données compromises. Selon la chaîne NOS, il n'est plus possible de déterminer qui a été précisément concerné par les écoutes et quelles informations ont été exactement obtenues. Pour le savoir, il fallait plus de temps. Or ce n'était pas possible, parce que Belgacom voulait que son réseau soit de nouveau opérationnel le plus vite

447 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html.

448 NOS Journaal, 3 octobre 2013, 20h CET. http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html.

449 P. DE LOBEL, N. VANHECKE, *De Standaard*, 21 septembre 2013 ("Op het randje van de catastrofe").

450 NOS Journaal, 3 octobre 2013, 20h CET. http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html.

451 P. DE LOBEL, N. VANHECKE, *De Standaard*, 21 septembre 2013 ("Op het randje van de catastrofe").

452 *Idem*.

453 http://nos.nl/artikel/558285-spionage-belgacom-omvangrijker.html.

454 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. http://www.youtube.com/watch?v=ayR6CAuNE4w.

455 N. VANHECKE, *De Standaard*, 20 septembre 2013 ("Info over malware Belgacom verspreid").

456 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. http://www.youtube.com/watch?v=ayR6CAuNE4w.

possible.[457] On ne sait pas non plus exactement pendant combien de temps le virus est resté sur le réseau. Lors d'une conférence de presse le 16 septembre 2013, le responsable de Belgacom a affirmé n'avoir aucune idée du moment où le virus s'est retrouvé sur le réseau de Belgacom. Selon *Der Spiegel,* il ressort d'un document (jusqu'à présent non publié) que l'accès était possible depuis 2010.[458] Selon *De Standaard* et la chaîne NOS, le virus était déjà présent depuis 2011.[459]

65. Le 18 octobre 2013, Belgacom signale que des contrôles poussés ont mis au jour de nouvelles irrégularités sur un routeur de BICS. « *Les premières analyses indiquent que des modifications ont été réalisées dans le logiciel du router, ce qui a pu avoir lieu pendant la récente intrusion digitale.* »[460] Belgacom n'exclut plus le piratage des données de ses clients. « *L'enquête en cours devra évaluer s'il y a un impact sur les données des clients* », a déclaré Belgacom dans *Le Soir.*[461] Le 23 octobre, Belga annonce que Tecteo a également été victime d'une cyberattaque similaire à celle perpétrée contre les opérateurs de télécommunications Belgacom, France-Telecom et Wanadoo. C'est ce qu'affirme la société. À l'heure actuelle, il est encore trop tôt pour dire si des informations ont été piratées au sein du groupe ou des filiales VOO ou RESA.[462]

II.4. EFFORTS BRITANNIQUES CONTRE LE CRYPTAGE

66. L'équivalent britannique du programme BULLRUN (voir paragraphe 45) a été baptisé EDGEHILL. Des documents que *The Guardian* a pu consulter suggèrent que le Royaume-Uni n'est pas aussi loin que les États-Unis et n'a pu décrypter des informations qu'au cas par cas. L'objectif initial d'EDGEHILL était de déchiffrer le trafic Internet crypté de trois grandes sociétés Internet et de 30 types de VPN. D'ici 2015, le GCHQ espérait avoir décrypté le trafic Internet chiffré de 15 grandes sociétés Internet et 300 types de VPN.[463] Un autre programme, appelé CHEESY NAME, a été mis sur pied pour pirater certaines clés de cryptage (connues sous le nom de *certificates*) à l'aide de

---

457 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html.

458 http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

459 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 septembre 2013 ("NSA verdacht van hacken Belgacom"). http://www.standaard.be/cnt/dmf20130915_00743233.

460 http://www.belgacom.com/be-fr/newsdetail/ND_20131017_Belgacom.page.

461 X., *Belga*, 19 octobre 2013 («Belgacom n'exclut plus le piratage des données de ses clients").

462 X., *Belga*, 23 octobre 2013 ("Tecteo a également été victime de la vague d'espionnage informatique").

463 "*GCHQ's phrasing of beating "30" then "300" VPNs suggest it's done on a case-by-case basis, rather than a blanket capability. It's also worth noting that just because the NSA can, say, beat SSL in some (or many, or most) cases, it doesn't mean they can do it all the time, especially as they often seem to circumvent rather than directly beat security*". http://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat. *The Guardian* mentionne également : "*Analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project. A quarterly update from 2012 notes the project's team "continue to work on understanding" the big four communication providers, named in the document as Hotmail, Google, Yahoo and Facebook, adding "work has predominantly been focused this quarter on Google due to new access*

superordinateurs du GCHQ.[464] Le GCHQ a également créé une *Humint Operations Team* (HOT) chargée d'identifier, de recruter et de gérer des informateurs (*covert agents*) dans le secteur mondial des télécommunications, entre autres pour obtenir l'accès à certaines clés.[465]

67. Des documents qui ont été montrés lors d'une émission de Fantastico suggèrent que la *network exploitation unit* du GCHQ a utilisé des programmes (FLYING PIG et HUSH PUPPY) capables de surveiller des réseaux TLS/SSL. Les programmes semblent avoir vu le jour parce qu'un nombre croissant de fournisseurs de messagerie électronique, tels que Yahoo, Google ou Hotmail, utilisaient le cryptage SSL et que ces messages étaient dès lors devenus illisibles dans le cadre de la collecte directe en amont (*upstream*). Un document au moins montre que tant la NSA que le GCHQ ont eu recours à des attaques de type *man in the middle* pour contourner le cryptage.[466] FLYING PIG semble également pouvoir montrer des informations sur l'utilisation de Tor (Tor Events).[467]

68. Un document datant du 10 octobre 2012 décrit comment, lors de l'opération MULLENIZE, le GCHQ est parvenu à identifier des utilisateurs individuels sur une adresse IP utilisée simultanément par plusieurs personnes, et ce via la technique du *user agent staining*. C'est par exemple le cas dans un cybercafé, mais aussi dans certaines régions où des milliers d'utilisateurs se servent d'une même adresse IP. Cette technique permet également de reconnaître des utilisateurs Tor individuels. En deux mois, le GCHQ a réussi à infecter ainsi quelque 200 ordinateurs avec des *stains* uniques.[468]

III. ÉNUMÉRATION DES CAS D'ACTIVITÉS D'ESPIONNAGE RELATIFS À DES ACTIVITÉS POLITIQUES DE 'PAYS AMIS' CITÉS DANS DES SOURCES OUVERTES

III.1. ACTIVITÉS D'ESPIONNAGE (SUPPOSÉES) HORS AFFAIRE SNOWDEN

69. La présente liste se concentre sur l'espionnage de pays amis par les États-Unis ou le Royaume-Uni. L'espionnage de pays européens qui faisaient partie du Pacte de Varsovie

---

opportunities being developed". http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

464 *Idem*.

465 *Idem*.

466 "*The document illustrates with a diagram how one of the agencies appears to have hacked into a target's Internet router and covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format"*. http://www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html.

467 *Idem*.

468 http://apps.washingtonpost.com/g/page/world/gchq-report-on-mullenize-program-to-stain-anonymous-electronic-traffic/502/.

durant la Guerre froide n'entre pas en ligne de compte. Les exemples historiques sont donnés à titre d'illustration.

70. L'historien britannique Richard Aldrich a décrit comment, depuis 1940, le prédécesseur du GCHQ écoutait les communications diplomatiques de ses partenaires, dont la France libre sous la direction de De Gaulle, la Turquie, l'Espagne et une vingtaine d'autres pays.[469] Des informations diplomatiques émanant d'Italie, de France, d'Espagne, du Portugal, du Japon et de l'Allemagne de l'Ouest étaient partagées avec les États-Unis sur une base *ad hoc*.[470]

71. Le 21 février 1967, le journal britannique *Daily Express* a révélé comment des entreprises telles que Western Union et Cable & Wireless ont transmis aux autorités britanniques tous les télégrammes et télex internationaux (y compris du matériel issu d'ambassades étrangères), qui ont ensuite été copiés. D'après Aldrich, cette tradition remontait à la Première Guerre mondiale : le Royaume-Uni a donc eu accès à tout le trafic diplomatique de toutes les ambassades sur son territoire pendant une période de plus de cinquante ans.[471]

72. Selon Aldrich, le service néerlandais a intercepté des communications diplomatiques de la Belgique et de l'Allemagne dans les années 1980.[472]

73. En 2006, le rapport annuel *top secret* de 1985-1986 du Government Communications Security Bureau (GCSB), l'agence SIGINT de la Nouvelle-Zélande, était révélé. Ce rapport mentionnait les pays et agences que la Nouvelle-Zélande avait espionnés cette année-là, ainsi que les communications diplomatiques de l'ONU, de l'Égypte, du Japon, des Philippines, de plusieurs îles de l'océan Pacifique, de la France, du Vietnam, de l'Union soviétique, de la Corée du Nord, de l'Allemagne de l'Est, du Laos et de l'Afrique du Sud.[473] En 1985, le service secret français a fait couler le 'Rainbow Warrior' de Greenpeace, et le GCSB a sollicité l'aide de la NSA et du GCHQ pour espionner des sources en France.[474]

74. Alastair Campbell, Director of Communications and Strategy du gouvernement de Tony Blair entre 1997 et 2003, a décrit dans ses mémoires comment des agents de sécurité britanniques ont découvert deux *bugs* dans la chambre d'hôtel qui était destinée à Tony Blair lors de sa visite à New Delhi en octobre 2001. Ces *bugs* ont été attribués au service secret indien.[475]

---

469 R. ALDRICH, *GCHQ. The uncenseored story of Britain's most secret intelligence agancy*, Harper Press, London, 2010, 28 ; 52-53.
470 R. ALDRICH, *o.c.*, 44.
471 R. ALDRICH, *o.c.*, 238-240.
472 R. ALDRICH, *o.c.*, 604.
473 H. BAIN, *Sunday Star*, 15 janvier 2006 ("Lange's secret papers reveal USA's bully tactics").
474 R. ALDRICH, *o.c.*, 446.
475 A. CAMPBELL, *The Blair Years : The Alastair Campbell diaries*, Knopf Doubleday Publishing Group, 2011, 577.

75. En 1999, la presse américaine a publié plusieurs rapports qui affirmaient que tant la NSA que le GCHQ avaient infiltré la mission de l'UNSCOM avec des inspecteurs en désarmement de l'ONU afin d'entreprendre des opérations SIGINT sensibles en Irak. Toutes les informations qui ont été trouvées par ce biais n'ont pas été partagées avec l'UNSCOM.[476] Selon l'inspecteur principal des Nations unies, Hans Blix, ces informations étaient particulièrement pertinentes pour une éventuelle invasion ultérieure.[477]

76. En 2003, *The Observer* a publié l'intégralité d'un mémo de la NSA au GCHQ, dans lequel elle demandait l'aide de ce dernier pour écouter les membres non permanents du Conseil de sécurité des Nations unies de l'époque (Angola, Cameroun, Chili, Bulgarie et Guinée), et ce afin de connaître la position de ces pays à l'égard d'une éventuelle résolution du Conseil de sécurité approuvant une intervention militaire contre l'Irak.[478]

77. À peu près à la même époque, en février 2003, un dispositif d'écoute était trouvé dans les parties du bâtiment Juste Lipse du Conseil européen qui étaient occupées par les délégations britanniques, françaises, allemandes et espagnoles. L'enquête a suggéré que ce dispositif se trouvait dans le bâtiment depuis sa construction en 1993. Bien que cela n'ait jamais été prouvé de manière irréfutable, plusieurs indicateurs ont pointé dans la direction d'Israël en tant que responsable de cet espionnage.[479]

78. En 2004, l'ancienne ministre britannique Clare Short a déclaré lors de l'émission Today sur BBC Radio 4 qu'elle avait régulièrement eu connaissance de SIGINT, où l'on pouvait entendre des conversations du Secrétaire général des Nations unies, Kofi Annan, dans son bureau privé du quartier général de l'ONU à New York, juste avant le début de la guerre en Irak en 2003.[480]

79. En 2004, des dispositifs d'écoute ont été trouvés dans le 'Salon français' du Palais des Nations de l'ONU à Genève. Ce salon faisait partie des pièces utilisées, en septembre 2003, pour des négociations privées sur la question de l'Irak. Aucun responsable n'a jamais été identifié.[481]

80. En décembre 2004, l'on a suggéré que la NSA avait écouté des dizaines de conversations téléphoniques entre Mohamed ElBaradei, responsable de l'Agence

---

476 C. LYNCH, Boston Globe, 6 janvier 1999 ("US used UN to spy on Iraq, aides say"); B. GELLMAN, *The Washington Post,* 6 janvier 1999 ("Annan suspicious of UNSCOM probe").

477 H. BLIX, *Disarming Iraq: The search for weapons of mass destruction*, Bloomsbury, 2005, 36-37.

478 Le mémo mentionnait également: "*We have a lot of special UN-related diplomatic coverage (various UN delegations) from countries not sitting on the UNSC right now that could contribute related perspectives/insights/whatever.*" X., *The Observer*, 2 mars 2003 ("US plan to bug Security Council: the text"). Voir aussi: http://www.theguardian.com/world/2003/mar/02/iraq.unitednations1.

479 Voir entre autres COMITÉ PERMANENT R, *Rapport d'activités 2010*, Intersentia, Anvers, 2010, 6-13.

480 C. SHORT, *An honourable deception? New Labour, Iraq and the misuse of power*, Free Press, 2005, 242-243.

481 B. WHITAKER, *The Guardian*, 18 décembre 2004 ("Bugging device found at UN offices").

internationale de l'énergie atomique (AIEA), et des diplomates iraniens. Le journal *The Washington Post* a avancé que l'on cherchait des éléments susceptibles d'évincer ElBaradei de la direction de l'AIEA.[482]

III.2. RÉVÉLATIONS ÉMANANT DES DOCUMENTS DE SNOWDEN

81. Selon *Der Spiegel*, le Special Collection Service a intercepté des SIGINT clandestins à partir de 80 ambassades et consulats américains.[483] Cette équipe est aussi responsable d'opérations de surveillance top secrètes dans d'autres ambassades et consulats, opérations connues sous le nom de code STATEROOM au sein de la NSA.[484]

82. *Der Spiegel* a également décrit le type d'informations qui intéressait la NSA à propos de l'Union européenne. Les informations relatives à la stabilité économique et à la politique commerciale figuraient au niveau 3 d'une échelle de priorités allant de 1 (plus haut intérêt) à 5 (plus faible intérêt). Les informations concernant la sécurité énergétique, les denrées alimentaires et l'innovation technologique arboraient une priorité 5.[485] *Der Spiegel* a publié des détails sur la manière dont la NSA espionnait l' 'ambassador's room' au 31e étage de la délégation de l'UE auprès des Nations unies à New York, également connue au sein de la NSA sous le nom de code 'Apalachee'. La NSA avait accès aux plans du bâtiment et a infiltré le réseau VPN interne entre la représentation de l'Union européenne auprès de l'ONU à New York et celle à Washington, connue sous le nom de code MAGOTHY. Les missions de l'UE à Washington et à New York ont toutes deux été mises sur écoute. Dans la représentation de l'UE à New York, des disques durs ont également été copiés, tandis qu'à Washington, le réseau informatique interne a été infiltré.[486]

83. Aux Nations unies, la NSA s'est surtout intéressée à tout ce qui a trait au contrôle des armes à l'AIEA (priorité 1), à la politique étrangère (priorité 2) et aux droits de l'homme, aux crimes de guerre, à l'environnement et aux matières premières (tous de priorité 3). Aux Nations unies, la NSA dispose d'une équipe qui travaille sous couverture diplomatique et qui est renforcée par une équipe à Washington pour toutes les séances de

---

482 D. LINZER, *The Washington Post*, 12 décembre 2004 ("IAEA Leader's phone tapped"). El Baradei avait sérieusement mis en doute les renseignements américains relatifs à l'Irak et avait également adopté à l'époque une position très prudente à l'égard de l'Iran.

483 Voir paragraphe 19.

484 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html.

485 "*Of particular note, the data systems of the EU embassies in America are maintained by technicians in Brussels; Washington and New York are connected to the larger EU network. Whether the NSA has been able to penetrate as far as Brussels remains unclear. What is certain, though, is that they had a great deal of inside knowledge from Brussels*". http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

486 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

l'Assemblée générale. La NSA a également écouté les vidéoconférences de diplomates de l'ONU.[487]

84. *Der Spiegel* a également divulgué l'existence du programme RAMPART-T dans le cadre duquel la NSA intercepte, depuis 1991, les communications de chefs d'État et de leur entourage direct de plus de vingt pays, et ce dans le but de pouvoir mieux informer le Président et ses conseillers en matière de sécurité nationale. *Der Spiegel* a indiqué que ces interceptions ne visaient pas seulement des cibles en Chine et en Russie, mais aussi dans des pays de l'Europe de l'Est.[488]

85. *The Guardian* a mentionné que les 38 ambassades et délégations étaient considérées comme des cibles dans un document de la NSA datant de septembre 2010. Aucun bâtiment d'Europe occidentale n'y figure, mais bien les représentations de l'UE susmentionnées, ainsi que les ambassades de France, d'Italie et de Grèce, et les ambassades du Japon, du Mexique, de la Corée du Sud, d'Inde[489] et de Turquie. Les missions grecque et française auprès de l'ONU ont également été espionnées.[490] Le 18 octobre, *Le Monde* a publié un document qui indiquait qu'une collecte de type 'close access' sur le territoire américain contre des cibles diplomatiques étrangères était connue sous le nom de SIGAD US-3136. Un suffixe de deux lettres désigne l'emplacement et la mission concernés. Le document du 10 septembre 2010 décrit une quinzaine de manières qui pouvaient être utilisées pour obtenir des informations.[491] La collecte de type 'close

---

487 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

488 http://www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

489 Pour de plus amples informations, voir S. SAXENA, *The Hindu*, 25 septembre 2013 ("NSA planted bugs at Indian missions in D.C., U.N ").

490 "*The US intelligence service codename for the bugging operation targeting the EU mission at the United Nations is "Perdido". The operation against the French mission to the UN had the covername "Blackfoot" and the one against its embassy in Washington was "Wabash". The Italian embassy in Washington was known to the NSA as both "Bruneau" and "Hemlock". The eavesdropping of the Greek UN mission was known as "Powell" and the operation against its embassy was referred to as "Klondyke"*." http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

491 HIGLANDS: collection from implants, VAGRANT: collection of computer Screens, MAGNETIC: sensor collection of magnetic emanations, MINERALIZE: collection from LAN implant, OCEAN: optical collection system for raster-based computer screens, LIFESAVER: imaging of the hard drive, GENIE: multi-stage operatoins; jumping the airgap…; BLACKHEART: collection from an FBI implant, PBX: Public Branch Exchange Switch, CRYPTO ENABLED: collection derived from AO's efforts to enable crypto, DROPMIRE (1) passive collection of emanations using an antenna (2) laser printer collection, purely proximal access, DEWSWEEPER: USB hardware host tap that provides covert link over USB link into a target network. Operates w/RF delay sybsytem to provide wireless bridge into target network. RADON: bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-direction exploitation of denied networks using standard on-net tools. Par exemple, les techniques HIGHLAND, VAGRANT et PBX ont été utilisées contre les missions françaises. https://www.documentcloud.org/documents/807030-ambassade.html#document/p1.

access' de sources diplomatiques en dehors des États-Unis est connue sous le nom de SIGAD US-3137 avec un suffixe de deux lettres.

86. *Der Spiegel* a également décrit la manière dont la NSA exploite les informations émanant de la diplomatie française. Un document interne à la NSA et datant de juin 2010 décrivait comment la NSA était parvenue à accéder au réseau VPN du ministère français des Affaires étrangères (réseau qui relie toutes les ambassades et tous les consulats français avec Paris), ainsi qu'aux sous-domaines (internes) de l'URL 'diplomatie.gouv.fr'. Des agents de la NSA ont installé des *bugs* au sein de l'ambassade française à Washington et de la mission française à New York. Toujours selon *Der Spiegel*, la NSA s'intéresse surtout à la politique étrangère (plus particulièrement le commerce des armes) et économique de la France.[492]

87. Un document datant du 17 mai 2006 et publié sur le site Internet du Globo indiquait que la mission International Security Issues (ISI) au sein de la NSA est responsable de treize États individuels sur trois continents. Ces treize pays ont un point commun : ils sont importants pour l'économie, le commerce et la politique étrangère des États-Unis. La division 'Western Europe and Strategic Partnerships' au sein de cette mission se concentre principalement « *sur la politique étrangère et les activités commerciales de la Belgique, la France, l'Allemagne, l'Italie, l'Espagne, ainsi que le Brésil, le Japon et le Mexique* ». Cette division transmet également la *key intelligence* concernant 'des activités militaires et de renseignement dans plusieurs de ces pays'. La 'Aegean and Ukraine division' s'occupe de tous les aspects liés à la Turquie ('governmental/leadership, military and intelligence'). L'ISI collabore avec F6 et des partenaires étrangers *second and third party* qui contiennent à la fois des 'données analytiques et capacités techniques précieuses'.[493] Selon *Le Monde*, les numéros qui commencent par US-98 (comme US – 985D (France), US-987 (Allemagne)) font référence à des SIGADS sur le territoire de partenaires *third party* de la NSA. Selon *Der Spiegel,* il s'agit entre autres de la France, l'Allemagne, l'Autriche, la Pologne et la Belgique.[494] Ce même document faisait référence au fait que l'ISI collabore activement avec les « *Combating Proliferation (CP, S2G) and Counterterrorism (CT, S2I) product lines to incorporate financial intelligence analysis into their mission build-out plans* ».[495]

---

492 X., *Der Spiegel*, 1er septembre 2013 (" 'Success Story': NSA targeted French Foreign Ministry").

493 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html.

494 Http://www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-3.html.

495 "*The idea is to integrate financial analysis with traditional target efforts as opposed to working the target from two separate perspectives, as is done in NSA Washington. ISI's long-term goal is to introduce financial analysis a part of the Intelligence Analysis curriculum so any target can be enriched with the use of financial intelligence.*" http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html Dans ce sens, il est peut-être intéressant de souligner que, selon certaines sources du journal *De Standaard*, des problèmes auraient été constatés au sein du SPF Finances et que l'on a cherché à savoir s'il s'agissait du même logiciel malveillant que chez Belgacom. Hans D'Hondt, qui est à la tête du SPF Finances, a toutefois formellement démenti toute

88. Un document datant d'août 2010 confirme que la NSA a intercepté les communications de huit membres du Conseil de sécurité de l'ONU. Seuls la France, le Japon, le Mexique et le Brésil ont été explicitement cités. L'objectif était de fournir à la mission américaine auprès de l'ONU (et à d'autres services américains) les informations les plus actuelles sur leurs intentions de vote et les positions de négociation à propos d'une résolution de l'ONU traitant de sanctions contre l'Iran.[496]

89. Dans une de ses éditions, le *Globo* a confirmé la manière dont la NSA espionnait des pays d'Amérique du Sud tels que le Mexique, le Venezuela, l'Argentine, la Colombie, l'Équateur, le Panama, le Costa Rica, le Nicaragua, le Honduras, le Chili, le Salvador et le Pérou. La NSA s'intéressait à la politique du Venezuela en matière de pétrole, la politique du Mexique en matière d'énergie et de drogues, et la position de la Colombie à l'égard des FARC. L'utilisation de XKEYSCORE a permis de dépister un 'étranger' grâce à la langue qu'il utilisait pour communiquer.[497]

90. Un document *top secret* datant de novembre 2010, publié par *Der Spiegel*, montre que la division TAO de la NSA était parvenue, lors de l'opération FLATLIQUID, à accéder au compte de messagerie public du Président mexicain de l'époque, Felipe Calderon, pour «*se faire une idée du système politique et de la stabilité interne du Mexique*». Ce compte était aussi utilisé par des membres du cabinet de Calderon.[498] Durant deux semaines, au début de l'été 2012, la NSA a également lancé une campagne de 'surveillance structurelle' intensive contre l'actuel Président, Enrique Pena Nieto. Ses schémas de communication ont permis de connaître neuf de ses conseillers les plus proches. Les données de ces personnes ont été stockées dans la base de données DISHIRE, à la suite de quoi leurs communications ont également été interceptées. Par exemple, 85 489 SMS ont ainsi été interceptés. Cette opération avait pour objectif de déterminer si le Mexique adoptait une nouvelle stratégie à l'égard des cartels de la drogue.[499] La NSA s'intéresse surtout au trafic de drogue (niveau 1), aux dirigeants du Mexique, à la stabilité économique, aux capacités militaires, aux droits de l'homme et aux relations commerciales internationales du Mexique (niveau 3) ainsi qu'au contre-espionnage (niveau 4). Pour atteindre ces objectifs, la TAO a mené, en août 2009, l''Operation Whitetamale', par laquelle elle a pu accéder aux e-mails de plusieurs hauts fonctionnaires du 'Public Security Secretariat' mexicain, qui s'occupe notamment du trafic de drogue et de la traite des êtres humains. Grâce à l'opération EVENINGEASEL, la division SCS de la NSA a écouté des conversations téléphoniques depuis l'ambassade de Mexico et a lu les SMS envoyés par le biais du réseau téléphonique mobile mexicain.[500]

---

contamination ou tout piratage de ses services. N. VANHECKE, P. DE LOBEL, *De Standaard*, 4 octobre 2013 ("Vrees voor massale besmetting").

496 http://epoca.globo.com/tempo/noticia/2013/07/spies-bdigital-ageb.html.

497 http://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619.

498 http://www.spiegel.de/fotostrecke/photo-gallery-nsa-hacked-into-mexican-president-s-email-account-fotostrecke-102797-2.html.

499 http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

500 http://www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

91. L'émission d'information Fantastico de la chaîne brésilienne *Globo* a montré des *slides* qui illustraient les schémas de communication entre la Présidente brésilienne Dilma Roussef, ses principaux conseillers et des tiers.[501] Selon Glenn Greenwald, le programme de la NSA en question avait obtenu l'accès à l'ensemble du réseau de communication de la Présidente brésilienne et de son équipe, y compris aux conversations téléphoniques, aux e-mails et aux échanges sur les sites de réseaux sociaux.[502]

92. Le directeur de la DNI, James Clapper, a réagi en déclarant que « ce n'est pas un secret que l'Intelligence Community recueille des informations sur des questions économiques et financières et sur le financement du terrorisme ». D'après Clapper, les États-Unis collectent ce type d'informations notamment pour alerter (*early warnings*) les États-Unis et ses partenaires de l'imminence de crises financières internationales susceptibles d'avoir un impact négatif sur l'économie mondiale.[503]

93. Le lendemain, Fantastico faisait savoir que la NSA considérait également le réseau informatique interne de la compagnie pétrolière brésilienne Petrobras comme une cible d'espionnage. Une présentation datant de mai 2012 qui avait pour but de former de nouveaux agents de la NSA aux méthodes employées pour obtenir l'accès à des réseaux informatiques privés mentionnait la société en tant que cible. On ne sait pas exactement quelles informations étaient recherchées ou quelles informations avaient été obtenues, mais *Globo* suggère qu'il pouvait s'agir, par exemple, de détails sur les gisements pétrolifères inexploités les plus intéressants que Petrobras proposerait à brève échéance aux enchères ou d'informations sur une technologie de pointe en matière d'exploration des fonds marins (*ocean-floor exploration*). La présentation n'a pas (encore) été mise en ligne.[504] Cette même présentation mentionnait également que Google, des diplomates français ayant accès au réseau privé du ministère français des Affaires étrangères[505] et SWIFT étaient considérés comme des cibles.

94. Des *slides* du GCHQ montrent comment le GCHQ a recueilli des données des smartphones, y compris des Blackberries, de plusieurs délégations diplomatiques à la réunion du G20 à Londres en 2009.[506] Ces données ont pu être transmises presque en

---

501 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html.

502 Y.MARULL, AFP, 2 septembre 2013 ("Brazil, Mexico summon US envoys over spy claims). Un représentant du State Department a déclaré : "*while we are not going to comment publicly on every specific alleged intelligence activity, as a matter of policy we have made clear that the United States gathers foreign intelligence of the type gathered by all nations* ".

503 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 septembre 2013. http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence. "*What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of – or give intelligence we collect to – US companies to enhance their international competitiveness or increase their bottom line*".

504 http://www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909.

505 http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

506 "*The document refers to a tactic which was "used a lot in recent UK conference, eg G20 (…) the tactic is defined in an internal glossary as "active collection against an email account that*

temps réel à des analystes, qui ont pu rédiger des briefings pour des ministres britanniques, dont Gordon Brown.[507] Ces informations ont permis d'identifier vingt nouveaux 'e-mail selectors'.[508] Le GCHQ est allé très loin pour obtenir ces informations diplomatiques. Par exemple, il a mis sur pied un faux cybercafé où des *key-loggers* ont pu voir ce qu'un délégué tapait à l'ordinateur. Un autre document démontrait que le GCHQ était parvenu à pirater le réseau du ministre sud-africain des Affaires étrangères et à intercepter ainsi des briefings destinés à des délégués aux réunions du G20 et du G8. Il est également fait mention de tentatives du GCHQ d'intercepter des conversations téléphoniques cryptées entre Medvedev et d'autres représentants russes lorsque ces derniers se trouvaient à Londres. Le GCHQ a aussi espionné le ministre turc des Finances à la réunion, ainsi que quinze autres membres de sa délégation. En outre, le GCHQ a testé, à la réunion, une nouvelle technique visant à inventorier le trafic téléphonique de tous les participants.[509]

95. Le Royaume-Uni prévoyait une opération visant à espionner plusieurs délégations à la réunion des chefs de gouvernement du Commonwealth à Trinidad en 2009, et ce afin d'obtenir des informations diplomatiques supplémentaires. Par exemple, un document décrit comment des SIGINT devaient être recueillis concernant l'opinion de l'Afrique du Sud sur le Zimbabwe avant une réunion entre le Premier ministre Brown et Zuma. Il n'est pas clairement indiqué si ces SIGINT ont été effectivement recueillis.[510]

ANNEXE : ABRÉVIATIONS ET CONCEPTS

1 EF solution	One-End Foreign solution
AG	Attorney General
BICS	Belgacom International Carrier Services
BND	Bundesnachrichtendienst (DE)
CERT-EU	Computer Emergency Response Team
CLANSIG	clandestine signals collection
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DITU	Data Intercept Technology Unit du FBI

acquires mail messages without removing them from the remote server". A PowerPoint slide explains that this means "reading people's email before/as they do". Voir http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

507 Gordon Brown présidait le G20 et souhaitait enregistrer des progrès sur deux fronts : la coordination de la relance économique mondiale pour éviter une nouvelle récession et un accord visant à renforcer la gouvernance économique mondiale et à réformer les institutions financières internationales.

508 http://www.theguardian.com/uk/interactive/2013/jun/16/gchq-surveillance-the-documents.

509 http://www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

510 http://www.theguardian.com/world/2013/jun/16/uk-intelligence-agencies-spy-commonwealth-delegates.

DNI	(1) Director of National Intelligence aux États-Unis (James Clapper), (2) Digital Network Intelligence
DNR	Dialed Number Recognition
ECI	Exceptionally Controlled Information
EO 12333	Executive Order 12333
EXIF	EXchangeable Image File format
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FCCU	Federal Computer Crime Unit
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
Five eyes	Les agences SIGINT des États-Unis, du Royaume-Uni, de l'Australie, du Canada et de la Nouvelle-Zélande
Fornsat	Informations provenant de satellites
FTC	Federal Trade Commission
FRA	Försvarets radioanstalt (agence SIGINT suédoise)
GAO	Division Global Access Operations (NSA)
GCHQ	Government Communications Headquarters (UK)
HOT	Humint Operations Team
IBPT	Institut belge des services postaux et des télécommunications
IM	Instant Messaging
ISA	Intelligence Services Act (UK)
ISC	Intelligence Security Committee
Métadonnées	Les métadonnées – ou 'metadata', parfois également appelées 'communications data' ou 'traffic data' – désignent les informations créées lors de l'envoi des données. Le contenu exact dépend du type de données envoyé et parfois de la législation locale. – Pour les *lignes téléphoniques fixes*: les numéros qui ont été appelés via cet appareil, ainsi que la date et l'heure de l'appel. Parfois aussi le nom et l'adresse de la personne qui a conclu le contrat de la ligne fixe. – *Téléphones portables*: (1) les numéros qui ont été appelés ou auxquels on a envoyé un SMS via cet appareil, (2) la date et l'heure de l'appel ou de l'envoi ou la réception du SMS, (3) l'endroit d'où l'appel a été passé ou le SMS envoyé et où cette communication a été reçue. (4) Parfois aussi le nom et l'adresse de la personne qui a conclu le contrat de la ligne fixe. (5) Parfois aussi le numéro d'abonné IMSI (International Mobile Subscriber Identity) et (6) le numéro d'équipement IIEM (identité internationale d'équipement mobile). (6) Parfois aussi le numéro de la carte téléphonique utilisée. – *Protocole VoIP (Voice over Internet), e-mail, messagerie instantanée, messages Facebook*: (1) le nom d'utilisateur en ligne, le nom de connexion (*login*) ou le nom du compte utilisé pour passer ou recevoir un appel, envoyer des e-mails, des messages instantanés, (2) l'adresse IP des ordinateurs utilisés, (3) l'heure et

	la date de la communication. Certains pays semblent également considérer la ligne d'objet des e-mails comme une métadonnée. – *Comportement sur Internet :* (1) l'adresse IP de l'appareil utilisé pour surfer, (2) l'heure et la date de la connexion et de la déconnexion, ainsi qu'une liste des domaines consultés sur Internet.
NCtC	National Counterterorrism Center
MTI	Mastering the Internet
NSA	National Security Agency
OSN	Online Social Networking
PNR	Passenger Name Records
PSTN	Public switched telephone network
RIPA	Regulation of Investigatory Powers Act (UK)
SCIF	Secure Compartmented Intelligence Facility
SCS	Special Collection Service
SGRS	Service général du renseignement et de la sécurité
SHAPE	Supreme Headquarters Allied Powers Europe
SIGAD	« Signals activity/address designators » – peuvent faire référence à une plateforme de collecte physique spécifique (comme une base de l'armée américaine à l'étranger, une ambassade, un navire…), une plateforme virtuelle de traitement de données (par exemple, PRISM est connu sous le SIGAD US-984XN) ou un satellite spatial.
SIGINT	Signals Intelligence
Sites F6	Missions diplomatiques et consulaires des États-Unis
SRP	Specialized Reconnaissance Program
SSL	Secure Sockets Layer
SSO	Special Source Operations
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAO	Tailored Access Operations
TBB	Tor Browser Bundle
TFTP	Terrorist Finance Tracking Program
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing Systeem
XKS	Xkeyscore

ANNEXE E.
CONSULTATION SUR LES RÈGLES EN VIGUEUR EN BELGIQUE EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE EU ÉGARD AUX MOYENS AUTORISANT L'INTERCEPTION ET L'EXPLOITATION À GRANDE ÉCHELLE DE DONNÉES RELATIVES À DES PERSONNES, ORGANISATIONS, ENTREPRISES OU INSTANCES ÉTABLIES EN BELGIQUE OU QUI ONT UN LIEN AVEC LA BELGIQUE

Annemie Schaus
Professeure ordinaire
Vice-rectrice à la politique académique
Université libre de Bruxelles

I. BREF EXPOSÉ DU CONTEXTE CONNU DES INTERCEPTIONS ET CAPTURES MASSIVES DE DONNÉES À CARACTÈRE PERSONNEL[511]

D'énormes quantités de données personnelles ont pu être captées par le programme PRISM, qui collecte des renseignements à une échelle et à un degré sans précédents, et dont l'objectif va bien au-delà de la lutte contre le terrorisme ou de l'espionnage économique.

Si les faits précis et surtout le rôle de certains acteurs demeurent flous, l'ampleur de l'interception, la surveillance et l'exploitation de données personnelles semble reconnue. En effet, après les premières révélations sur le programme PRISM, le directeur de la NSA a confirmé que celle-ci collecte (à la fois aux États-Unis et en dehors de cet État) des métadonnées sur les communications de tous les principaux opérateurs et qu'elle maintient une base de données contenant ces métadonnées pendant cinq ans.[512]

Il est établi également que le GCHQ a procédé à ce même type d'interception et que des grands opérateurs de réseaux de communications ou de réseaux sociaux[513] ont livrés à la NSA d'importantes données à caractère personnel.

---

511 Voir le rapport de Mathias Vermeulen « De Snowden-revelaties, massale data-captatie en politieke spionage. Open bronnenonderzoek », 25 novembre 2013.

512 « *Le programme de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE* ». Note de la direction générale des politique internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, IPOL-LIBE_NT(2013)474405_FR ; Voir également le rapport de Mathias Vermeulen.

513 E.a. *Facebook, Twitter, Microsoft, Google, Yahoo !, PalTalk, YouTube, Skype, AOL* et *Apple ;* voir le rapport de Mathias Vermeulen.

II. LÉGISLATION APPLICABLE

Il faut d'emblée rappeler que la compatibilité des services de renseignement avec la Convention européenne des droits de l'homme[514] ne fait pas de doute. Comme la Cour européenne des droits de l'homme l'a souligné, la protection des droits de l'homme peut passer par l'existence de services de renseignement, pour autant que leurs méthodes respectent les principes fondamentaux en matière de protection des droits de l'homme :

> *« Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif : elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne ».*[515]

La Cour souligne que les États contractants ne disposent pas d'une marge de manœuvre illimitée pour soumettre les personnes relevant de leur juridiction à des mesures de surveillance secrète. Consciente du danger de méconnaitre, voire de détruire, la démocratie au motif de la défendre, la Cour rappelle que les États ne peuvent prendre, au nom de la lutte contre l'espionnage et le terrorisme, n'importe quelle mesure qu'ils jugent appropriée.

Il faut en la matière respecter le principe de légalité, de finalité et de proportionnalité, dès lors que le but légitime aura été établi.[516] Il s'ensuit que l'arsenal juridique qui protège la vie privée et les données à caractère personnel devra être respecté (A), mais aussi la souveraineté de l'État sur le territoire duquel la récolte, l'interception et le traitement de données à caractère personnel auront été effectués (B). Dans la mesure où les faits qui nous ont été soumis le permettent, nous analyserons l'application des règles aux récoltes massives des données à caractère personnel qui ont été portées à notre connaissance. Enfin, un aperçu des éventuels remèdes juridiques sera exposé (C).

A. LE RESPECT DU DROIT À LA VIE PRIVÉE ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Plusieurs dispositions légales protégeant le droit à la vie privée sont susceptibles de trouver à s'appliquer dans l'affaire qui nous préoccupe ; ces dispositions sont *complémentaires*. Elles seront synthétiquement exposées, de la disposition au champ d'application le plus général à la disposition à vocation plus particulière, à savoir, l'article 17 du Pacte sur les droits civils et politiques (1) ; l'article 8 de la CEDH (2) ; la Convention n° 108 pour la protection du traitement automatisé des données à caractère personnel (3) et le droit de l'Union européenne : les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne (4), la directive 95/46/CE du Parlement européen

514 Ci-après, CEDH.

515 CEDH, *Klass et autres c. Allemagne* du 6 septembre 1978 ; CEDH, *Vereniging weekblad Bluf ! c. Pays-Bas* du 9 février 1995.

516 Si la lutte contre le terrorisme peut constituer un but légitime, le profilage économique des individus ne l'est pas forcément.

et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[517] (telle que complétée par la directive 2002/58/CE du 12 juillet 2002 concernant la protection des données personnelles dans le secteur des communications électroniques) (5) et la directive 2006/24/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques[518] (6). Enfin, il faut rappeler que la loi belge du 8 décembre 1992 sur la protection de la vie privée[519] s'applique si les critères de rattachement avec la

Belgique le justifient[520], ce qui n'est pas clairement déterminé. Dans le cadre de cette étude, nous ne pourrons donc pas analyser spécifiquement cette législation. Dans la mesure où elle s'inscrit

dans ligne des dispositions de droit international et exécute le droit européen applicable en la matière, les analyses reprises ci-dessous lui sont transposables.

Nous verrons ensuite comment le respect de normes de protection des données à caractère personnel a fait l'objet de l'accord *Safe Harbour* entre l'UE et les États-Unis (7).

En matière de transfert, de surveillance, de contrôle de conservation de données à caractère personnel par de nouvelles technologies, il ne faut pas entendre, comme le soulignent Cécile de Terwangne et Jean-Noël Colin[521], la vie privée de façon classique dans le sens restreint de protection de la sphère privée, intime, familiale ou confidentielle. Elle s'entend, conformément à l'évolution du droit et des technologies, comme la faculté d'autodétermination, d'autonomie et la capacité de l'individu à effectuer des choix existentiels ou informationnels.[522] Comme l'a consacré la Charte des droits fondamentaux de l'Union européenne[523], il s'agit d'autodétermination informationnelle, c'est-à-dire du droit pour l'individu de connaître les données le concernant qui sont détenues, d'en maîtriser les circuits de communication, d'en empêcher les utilisations impropres ou abusives. Dans ce domaine, la vie privée ne se réduit donc pas à une quête d'intimité ; c'est la maîtrise par chacun de son image informationnelle.[524] Cela dit, comme le souligne la

---

517 Ci-après, directive 95/46.

518 Ci-après, directive 2006/24.

519 Ci-après, LPVP.

520 La LPVP est applicable au traitement de données à caractère personnel lorsque le traitement est effectué dans le cadre des activités réelles et effectives d'un établissement fixe du responsable du traitement sur le territoire belge comme l'indique son article 3*bis*, 1°.

521 *Défis pour la vie privée et la protection des données posés par la technologie,* Rapport, Namur FNDP, février 2011.

522 Pour la reconnaissance explicite d'un droit à l'autodétermination ou l'autonomie personnelle contenu dans le droit au respect de la vie privée de l'article 8 CEDH, voir CEDH, *Evans c. Royaume- Uni,* arrêt du 7 mars 2006 (confirmé par la Grande Chambre dans son arrêt du 10 avril 2007) ; *Tysiac c. Pologne,* arrêt du 20 mars 2007 ; *Daroczy c Hongrie,* arrêt du 1er juillet 2008.

523 Voir *infra* et la note suivante.

524 Paul De Hert, Katja de Vries et Serge Gutwirth, Note d'observation sur l'arrêt de la Cour constitutionnelle fédérale allemande du 27 février 2008, *Revue du droit des technologies et de l'information,* 2009, 87. Dans cet arrêt, la Cour reconnait, sur la base du droit général à la personnalité, un tout nouveau droit fondamental à la protection de « la confidentialité et l'intégrité des systèmes d'information technologiques ». Ce nouveau droit fondamental en matière de technologie de l'information doit compléter les droits fondamentaux existants là où ils font défaut.

CEDH, « *la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Conventioná* ».[525] C'est en ce sens qu'elle doit être ici comprise.

1. L'article 17 du Pacte International relatif aux droits civils et politiques[526]

L'article 17 du PIDESC est la seule disposition internationale de portée universelle qui garantit le droit à la vie privée. Tout comme les dispositions sœurs de l'article 17 qui lui sont contemporaines, cet article ne fait aucune référence aux données à caractère personnel comme élément constitutif du droit à la vie privée. Toutefois, la protection de la vie privée telle que garantie par l'article 17, mise à l'épreuve des nouvelles ingérences rendues possibles par les nouvelles technologies, a amené la 35ème Conférence internationale des commissaires à la protection des données et de la vie privée à encourager les États à adopter l'observation générale n°16 du PIDESC de 1988, de manière à renforcer la protection de la vie privée.[527] Celle-ci favorise la mise en place d'un cadre juridique mondial concernant la protection des données à caractère personnel et la protection de la vie privée. Les États-Unis n'ont pas adhéré à cette observation, raison pour laquelle de nombreuses propositions visent à réactualiser l'article 17 du PIDESC lui-même à l'ère du numérique[528] parce que États-Unis en sont signataires. D'autres proposent d'adopter un protocole additionnel sur la base de l'observation générale n°16 adoptée par l'Assemblé générale des Nations Unies en 1996.[529]

Notons que la troisième Commission des Nations Unies vient d'adopter un texte sur le droit à la vie privée à l'ère du numérique.[530] Elle préconise la protection de la vie privée des personnes « hors ligne » autant que celle « en ligne » et invite tous les États « *à respecter et à protéger le droit à la vie privée, notamment dans le contexte de la communication numérique* ».[531] L'interprétation qui peut être donnée de l'article 17 du PIDESC aujourd'hui est que sa protection couvre les données à caractère personnel.

2. L'article 8 de la CEDH

L'article 8 de la CEDH garantit à chacun le droit au respect de la vie privée. La Cour européenne des droits de l'homme a expressément élargi le champ de la vie privée à celui de la protection des données à caractère personnel. Pour la Cour, « la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée consacré par l'article 8.[532] La Cour considère que « *la protection*

525 CEDH, *S. et Marper c. Royaume-Uni* du 4 décembre 2008.

526 Ci-après, PIDESC.

527 http://www.unhchr.ch/tbs/doc.nsf/0/7dc7e7821c5da97680256523004a423d?Opendocument.

528 http://www.franceonu.org/IMG/pdf/Vie_privee_FR.pdf.

529 Http ://droitdu.net/2013/10/35eme-conference-internationale-des-commissaires-a-la-protection-des-donnees-et-de-la-vie-privee-une-volonte-duniformiser-la-protection-des-donnees-personnelles/.

530 http://www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&Lang=F.

531 Article 4 du texte de la troisième Commission des Nations Unies.

532 Voir document « Case law of the European Court of Human Rights concerning the protection of personal data», DP(2013)CASE LAW, 30 janvier 2013 [non disponible en français],

offerte par l'article 8 serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part ».[533]

Selon la Cour, l'article 8 impose que le droit interne ménage des garanties appropriées pour empêcher toute utilisation impropre et abusive de données à caractère personnel. La législation nationale doit également assurer que les données sont pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées, et qu'elles ne sont conservées sous une forme permettant l'identification des personnes que pendant la durée nécessaire aux finalités pour lesquelles elles sont enregistrées.

La Cour rappelle que *« dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire […] ».*

La Cour a ainsi jugé que la mémorisation par une autorité publique de données relatives à la vie privée d'un individu constituait une ingérence dans le droit au respect de sa vie privée garanti par l'article 8, paragraphe 1er, de la CEDH, en précisant que l'utilisation qui en est faite importe peu, notamment en ces termes :

> *« La mémorisation par une autorité publique de données relatives à la vie privée d'un individu constitue une ingérence au sens de l'article 8. L'utilisation ultérieure des informations mémorisées importe peu ».*[534]

La collecte et l'archivage de données doivent donc contenir les garanties nécessaires à la sauvegarde du droit à la vie privée des individus.[535]

Le 1er juillet 2008, dans une affaire dont les faits sont proches de ceux qui nous occupent, la Cour a condamné le Royaume-Uni pour violation de l'article 8, pour l'interception illégale de communications terrestres par l'agence de renseignement GCHQ, de 1990 à 1998. Le GCHQ interceptait toutes les communications terrestres (fax, emails, télex et communications informatiques) entrant et sortant de la République irlandaise via la tour de *Capenhurst,* située dans une centrale nucléaire et fonctionnant 24 heures sur 24. Outre des informations sur le terrorisme, la tour de *Capenhurst* servait à l'espionnage économique ainsi qu'à l'interception des communications diplomatiques de l'Irlande et des communications personnelles de résidents irlandais notables, à l'aide de listes ciblées de numéros de téléphone ou de systèmes de reconnaissance vocale.[536]

---

http://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20Law_Eng%20%28final%29.pdf.

533 CEDH, *S. et Marper c. Royaume- Uni* du 4 décembre 2008.

534 CEDH, *Leander c. Suède* du 26 mars 1987 ; *Kopp c. Suisse* du 25 mars 1998 ; *Amann c. Suisse* du 16 février 2000 ; *Association « 21 Décembre 1989 » et autres c. Roumanie* 24 du mai 2011.

535 CEDH, *Rotaru c. Roumanie* du 4 mai 2000.

536 CEDH, *Liberty et d'autres ONG c. le Royaume-Uni* du 1er juillet 2008.

La CEDH estime aussi que les États ont l'obligation de mettre en place une procédure effective permettant aux personnes intéressées d'accéder aux documents rassemblés par les services de sécurité à leur sujet.[537]

Le caractère massif et indifférencié de l'interception, la surveillance, l'utilisation, et l'archivage des données personnelles dont question en l'espèce contrevient manifestement en tous points à l'article 8; les mesures dénoncées visent des personnes physiques ou morales, privées ou publiques, de manière indéterminée; les victimes sont pour la plupart non identifiables; ces mesures ne se fondent sur aucune base légale valable et au contraire méconnaissent le droit applicable aux transferts de données à caractère personnel, elles sont manifestement disproportionnées au but poursuivi qui eux- mêmes ne sont pas définis.

Dès lors que les certains acteurs susceptibles d'avoir participé à ce système pourraient être des personnes privées, il convient de souligner que l'article 8 de la CEDH est susceptible de déployer un effet horizontal.

Dès 1979, la Cour européenne des droits de l'homme soulignait en effet:

> *« Si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences: à cet engagement plutôt négatif s'ajoutent des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux ».*[538]

Dans l'arrêt *Soderman c. Suède* du 12 novembre 2013, la Cour rappelle que lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, ou que les activités en cause concernent un aspect des plus intimes de la vie privée, la marge laissée à l'État pour réglementer l'obligation qui pèse sur les particuliers, est d'autant plus restreinte.[539]

Dans leurs activités susceptibles de porter atteinte aux droits à la vie privée des individus ou des personnes morales, publiques ou privées, le respect de la vie privée incombe clairement aux fournisseurs de réseaux sociaux, aux entreprises commerciales qui œuvrent dans le domaine des nouvelles technologie et autres acteurs responsables du traitement des données à caractère personnel, sous réserve bien entendu de l'étude dans chaque cas particulier du champ d'application territoriale de l'activité de ces fournisseurs.[540]

3. La Convention n° 108 pour la protection du traitement automatisé des données à caractère personnel

La Convention n° 108 du Conseil de l'Europe pour la protection du traitement automatisé des données à caractère personnel est le seul instrument juridique spécifique contraignant pour tous les États du Conseil de l'Europe dans ce domaine. Ces grands principes sont les suivants:

– principe de loyauté et licéité de la collecte principe de finalité (données enregistrées pour des finalités déterminées et légitimes et pas utilisées de manière incompatible avec ces finalités);

---

537 CEDH, *Joanna Szulc c. Pologne* du 13 novembre 2012.

538 *Airey c. Irlande* du 9 octobre 1979.

539 Voir aussi e.a. CEDH, *I.B. c. Grèce* du 3 octobre 2013.

540 Pour la directive 95 /46, voir *infra*.

- principe de qualité des données (pertinentes, adéquates, à jour, conservées pour une durée limitée) ;
- régime spécifique réservé aux données sensibles ;
- exigence de sécurité ;
- droits d'accès, de rectification et de recours ;
- possibilité de dérogations au nom d'intérêts publics ou privés prépondérants.

En 2001, un Protocole additionnel concernant les autorités de contrôle et les flux transfrontaliers de données a complété la Convention. La Convention 108 constitue l'un des meilleurs instruments juridiques pour protéger les individus contre les risques associés à la surveillance électronique. Ainsi, elle confère des droits étendus, par exemple, un droit d'accès de rectification ou d'effacement, aux données à caractère personnel.

Notons que la Convention est en cours de modernisation[541] afin de combler les lacunes qu'elle présente malheureusement encore face au défi des technologies, notamment quant à son application extra-territoriale.[542]

4. Les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne

L'article 7 garantit le droit à la vie privée dans la droite ligne des autres instruments protecteurs des droits de l'homme. L'article 8 a une portée plus originale puisqu'il dispose que toute personne a droit à la protection des données à caractère personnel la concernant et que les données doivent être traitées loyalement, à des fins déterminées, sur la base d'un fondement légitime (consentement ou autre fondement prévu par la loi) ; et que toute personne a un droit d'accès et de rectification de ses données. L'article 7 consacre donc un droit autonome à la protection des données à caractère personnel.

Ainsi que le souligne l'avocat général Pedro Cruz Villalon dans ses conclusions du 12 décembre dernier[543], l'article 8 de la Charte consacre le droit à la protection des données personnelles comme un droit distinct du droit au respect de la vie privée. Si la protection des données tend à assurer le respect de la vie privée, elle est surtout soumise à un régime autonome, principalement défini par la directive 95/46, la directive 2002/58, le règlement n° 45/2001 et la directive 2006/24, ainsi que, dans le domaine relevant de la coopération policière et judiciaire en matière pénale, par la décision-cadre 2008/977/JAI.[544]

A l'inverse, la « sphère du privé » constituant le noyau de la « sphère du personnel », il ne saurait être exclu qu'une réglementation restreignant le droit à la protection des

---

541 Proposition de modernisation du Comité consultatif de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, 18 décembre 2012, STE n° 108 (T-PD) ; voir projet de recommandation http://www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD%282013%295rev_fr_Projet%20de%20Rec.%20emploi.pdf ; Sur la révision de la *Convention n°108* État des travaux en cours : www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp.

542 *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques,* Cécile de Terwangne, Jean-Philippe Moiny, Yves Poullet et Jean-Marc Van Gyzeghem, Novembre 2010, Bureau du comité consultatif de la Convention n° 108.

543 Conclusions de l'avocat général M. Pedro Cruz Villalon du 12 décembre 2013 dans les affaires C-293/12 et C-494/12 pendantes devant la CJCU.

544 Voir *infra*.

données personnelles en conformité avec l'article 8 de la Charte puisse néanmoins être considérée comme portant une atteinte disproportionnée à l'article 7 de la Charte ».[545]

Evidemment, le droit à la protection des données à caractère personnel repose sur le droit fondamental au respect de la vie privée. On peut donc dire, comme la Cour JUE, que *« les articles 7 et 8 de la Charte sont étroitement liés, au point de pouvoir être considérés comme établissant un « droit à la vie privée à l'égard du traitement des données à caractère personnel »*.[546]

5. La directive 95/46/CE du 24 octobre 1995

La directive 95/46 du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, entrée en vigueur en octobre 1998, est la norme de base en droit communautaire dérivé. L'objet de la directive 95/46 est d'imposer aux États membres l'obligation de garantir le droit à la vie privée des personnes physiques à l'égard du traitement de leurs données à caractère personnel, en vue de permettre la libre circulation de ces données entre les États membres.

Elle impose dès lors le respect de règles définissant les conditions de licéité des traitements de données à caractère personnel, précisant les droits des personnes dont les données sont collectées et traitées (droit à l'information, le droit d'accès et de rectification ou droit d'opposition et le droit de recours, et le droit à la confidentialité et la sécurité des traitement).

Cette directive a été complétée par la directive 2002/58 du 12 juillet 2002 concernant la protection des données personnelles dans le secteur des communications électroniques qui garantit la confidentialité des communications électroniques. L'obligation de garantir cette confidentialité pèse sur les fournisseurs de service de communications électroniques accessibles au public. Elle impose aussi aux États membres de garantir, sauf exception, la confidentialité non seulement des communications, mais également des données relatives au trafic des abonnés et des utilisateurs de services de communications électroniques. Son article 6 prévoit l'obligation pour les fournisseurs des services de communications d'effacer ou d'anonymiser les données relatives au trafic de leurs abonnés et utilisateurs qu'ils traitent et stockent.

– *Les principes*

La directive 95/46 vise à protéger les droits et les libertés des personnes par rapport au traitement de données à caractère personnel en établissant des principes directeurs déterminant la licéité de ces traitements.

Ces principes[547] portent sur :

– la qualité des données : les données à caractère personnel doivent notamment être traitées loyalement et licitement, et collectées pour des finalités déterminées, explicites et légitimes. Elles doivent en outre être exactes et, si nécessaire, mises à jour ;

545 Conclusions de l'avocat général M. Pedro Cruz Villalon, précitées.

546 Arrêt C-92/09 et C-93/09 du 9 novembre 2010.

547 Voir synthèse de la législation sur : http://europa.eu/legislation_summaries/information_society/data_protection/l14012_fr.htm (décembre 2013).

- la *légitimation* des traitements de données : le traitement de données à caractère personnel ne peut être effectué que si la personne concernée a indubitablement donné son consentement ou si le traitement est nécessaire :
- à l'exécution d'un contrat auquel la personne concernée est partie ; ou
- au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; ou
- à la sauvegarde de l'intérêt vital de la personne concernée ; ou
- à l'exécution d'une mission d'intérêt public ; ou
- à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ;
- les catégories particulières de traitements : doit être interdit le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions publiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle. Cette disposition est assortie de réserves concernant, par exemple, le cas où le traitement est nécessaire à la défense des intérêts vitaux de la personne concernée ou aux fins de la médecine préventive et des diagnostics médicaux ;
- l'information des personnes concernées par les traitements de données : un certain nombre d'informations (identité du responsable du traitement, finalités du traitement, destinataires des données, etc) doivent être fournies par le responsable du traitement à la personne auprès de laquelle il collecte des données la concernant ;
- le droit d'accès de ces personnes aux données : toute personne concernée doit avoir le droit d'obtenir du responsable du traitement :
- la confirmation que des données la concernant sont ou ne sont pas traitées et la communication des données faisant l'objet des traitements ;
- la rectification, l'effacement ou le verrouillage des données dont le traitement n'est pas conforme à la présente directive – notamment en raison du caractère incomplet ou inexact des données – ainsi que la notification de ces modifications aux tiers auxquels les données ont été communiquées ;
- les *exceptions et limitations* : les principes relatifs à la qualité des données, à l'information de la personne concernée, au droit d'accès et à la publicité des traitements peuvent voir leur portée limitée afin de sauvegarder, entre autres, la sûreté de l'État, la défense, la sécurité publique, la poursuite d'infractions pénales, un intérêt économique ou financier important d'un État membre ou de l'UE ou la protection de la personne concernée ;
- le droit d'opposition aux traitements de données : la personne concernée doit avoir le droit de s'opposer, pour des raisons légitimes, à ce que des données la concernant fassent l'objet d'un traitement. Elle doit également pouvoir s'opposer, sur demande et gratuitement, au traitement des données envisagé à des fins de prospection. Elle doit enfin être informée avant que des données ne soient communiquées à des tiers à des fins de prospection et doit se voir offrir le droit de s'opposer à cette communication ;
- la confidentialité et la sécurité des traitements : toute personne agissant sous l'autorité du responsable du traitement ou celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données personnelles, ne peut les traiter que sur instruction du responsable du traitement. Par ailleurs, le responsable du traitement doit mettre en œuvre les mesures appropriées pour protéger les données à caractère personnel

contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé ;
- la notification des traitements auprès d'une autorité de contrôle : le responsable du traitement doit adresser une notification à l'autorité de contrôle nationale préalablement à la mise en œuvre d'un traitement. Des examens préalables sur les risques éventuels au regard des droits et libertés des personnes concernées sont effectués par l'autorité de contrôle après réception de la notification. La publicité des traitements doit être assurée et les autorités de contrôle doivent tenir un registre des traitements notifiés.

Toute personne doit disposer d'un recours juridictionnel en cas de violation des droits qui lui sont garantis par les dispositions nationales applicables au traitement en question. En outre, les personnes ayant subi un dommage du fait d'un traitement illicite de leurs données personnelles ont le droit d'obtenir réparation du préjudice subi.

- *Le champ d'application territorial*

En vertu de cette directive, des obligations incombent aux fournisseurs d'accès internet, aux moteurs de recherches, aux réseaux sociaux et autres fournisseurs de service de communication, étant tous des responsables du traitement de données à caractère personnel. Dans chaque cas particulier, l'étendue de la responsabilité du responsable du traitement de donnée peut être analysée, notamment au regard la question de l'application territoriale de la directive 95/46. En vertu de l'article 4 de la directive, un État doit appliquer sa législation de protection des données à caractère personnel conforme à la directive, si le responsable du traitement a son lieu d'établissement sur son territoire, ou en fonction du lieu du moyen de traitement des données, c'est-à-dire si les moyens de traitement des données sont situés sur le territoire de cet État.

Le groupe « Article 29 »[548], dans son avis 5/2009 sur la protection des données par les réseaux sociaux en ligne[549], a souligné que « *Les dispositions de la directive relative à la protection des données s'appliquent dans la plupart des cas aux fournisseurs de SRS, même lorsque leur siège est situé en dehors de l'EEE* ».

Pareillement, l'une des principales conclusions de l'avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche est que la directive sur la protection des données s'applique généralement au traitement des données à caractère personnel par les moteurs de recherche, même lorsque le siège de ces derniers se trouve en dehors de l'EEE, et qu'il incombe aux fournisseurs de moteurs de recherche qui se trouvent dans cette situation de clarifier leur rôle dans l'EEE ainsi que l'étendue de leurs responsabilités en vertu de la directive.[550]

Les transferts de données à caractère personnel d'un État membre vers un pays tiers ayant un niveau de protection adéquat sont autorisés. En revanche, ils ne peuvent être

548 Ce groupe de travail a été institué en vertu de l'article 29 de la directive 95/46. C'est un organe consultatif européen. Ses missions sont décrites à l'article 30 de la directive et 15 de la directive 2002/58.

549 Groupe 29, WP 163 « Avis 5/2009 sur les réseaux sociaux en ligne » du 12 juin 2009.

550 Groupe 29, WP 148 « Avis 1/2008 sur les aspects de la protection des données liés aux moteurs de recherche » du 4 avril 2008.

effectués vers un pays tiers ne disposant pas d'un tel niveau de protection, sauf dérogations limitativement énumérées.

Il conviendra donc déterminer en fonction de faits précis, la responsabilité de chaque acteur déterminé.

– *Exclusions du champ d'application matériel*

L'article 3, paragraphe 2, de ladite directive indique une des limites du *champ d'application matériel* de celle-ci dans la mesure où il dispose que :

> « *La présente directive ne s'applique pas au traitement de données à caractère personnel :*
> – *mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne, et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal* ».

La protection des données à caractère personnel dans le cadre de la sécurité publique et le droit pénal sont donc régis par différents instruments spécifiques. Il s'agit notamment d'instruments qui instaurent des systèmes d'information communs au niveau européen, tels que la convention d'application de l'Accord de Schengen qui contient des dispositions spécifiques sur la protection des données dans le cadre du système d'information Schengen (SIS) ; la convention sur la base de l'article K.3 du traité sur l'Union européenne portant création d'un office européen de police ; la décision du Conseil créant Eurojust et les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel ; la convention établie sur la base de l'article K.3 du traité sur l'Union européenne, sur l'emploi de l'informatique dans le domaine des douanes, qui contient des dispositions relatives à la protection des données à caractère personnel applicables au système d'information des douanes, et la convention relative à l'entraide judiciaire en matière pénale entre les États membres de l'Union européenne.[551] Le 27 novembre 2008, le Conseil a adopté une décision-cadre 2008/977/JAI du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Cependant, il s'applique seulement aux transferts de données entre États membres (articles 26 et 13).

6. *La directive 2006/24/CE sur la Conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques*

La directive 2006/24 est importante pour la question qui nous préoccupe parce qu'elle modifie les directives 95/46 et 2002/58 en prévoyant l'établissement par les États membres d'une obligation de collecte et de conservation des données de trafic et de localisation en imposant aux fournisseurs de services de communications électroniques accessibles au public ou de réseaux publics de communications, des obligations de conservation des données de trafic et de localisation qu'elle définit, en vue de garantir leur disponibilité

551 CJUE, arrêts C-317/04 et C-318/04 du 30 mai 2005, Conclusions de l'Avocat général LEGER, point 41.

« aux fins de la recherche, de la détection et de la poursuite d'infractions graves telles que définies par chaque État membre dans son droit interne ». Ce faisant, la directive déroge aux règles dérogatoires établies par l'article 15, paragraphe 1er, de la directive 2002/58 et régissant la faculté pour les États membres de limiter, pour les motifs prévus à l'article 13, paragraphe 1er, de la directive 95/46, la portée du droit à la protection des données personnelles et, plus largement, du droit au respect de la vie privée dans le cadre spécifique de la fourniture de services de communications électroniques ou de réseaux publics de communications.

La directive 2006/24 vise à l'harmonisation des réglementations des États membres concernant la conservation des données de trafic et de localisation afférentes aux communications électroniques et, dès lors, impose aux États membres qui ne disposeraient pas d'une telle réglementation, d'une obligation de collecte et de conservation desdites données.

Cette obligation faites aux États par la directive a été jugée contraire à la Charte des droits fondamentaux par l'avocat général M. Pedro Cruz Villalon le 12 décembre 2013.[552] La Cour JUE doit encore rendre son arrêt.

La motivation de l'avocat général mérite d'être citée[553] :

> *« 72. Il n'en demeure cependant pas moins que la collecte et, surtout, la conservation, dans de gigantesques bases de données, des multiples données générées ou traitées dans le cadre de la plus grande partie des communications électroniques courantes des citoyens de l'Union constituent une ingérence caractérisée dans leur vie privée, quand bien même elles ne feraient que créer les conditions de possibilité d'un contrôle rétrospectif de leurs activités tant personnelles que professionnelles. La collecte de ces données crée les conditions d'une surveillance qui, pour ne s'exercer que rétrospectivement à l'occasion de leur exploitation, menace néanmoins de manière permanente, pendant toute la durée de leur conservation, le droit des citoyens de l'Union au secret de leur vie privée. Le sentiment diffus de surveillance généré pose de manière particulièrement aiguë la question de la durée de conservation des données.*
>
> *73. Il doit à cet égard être tout d'abord tenu compte du fait que les effets de cette ingérence se trouvent démultipliés par l'importance acquise par les moyens de communications électroniques dans les sociétés modernes, qu'il s'agisse des réseaux mobiles numériques ou d'Internet, et leur utilisation massive et intensive par une fraction très importante des citoyens européens dans tous les champs de leurs activités privées ou professionnelles.*
>
> *74. Les données en question, il importe également d'insister encore une fois à cet égard, ne sont pas des données personnelles au sens classique du terme, se rapportant à des informations ponctuelles sur l'identité des personnes, mais des données personnelles pour ainsi dire qualifiées, dont l'exploitation peut permettre l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voire d'un portrait complet et précis de son identité privée.*
>
> *75. L'intensité de cette ingérence se trouve accentuée par des éléments aggravant le risque que, nonobstant les obligations imposées par la directive 2006/24 tant aux États membres eux-mêmes qu'aux fournisseurs de services de communications électroniques, les données conservées ne soient utilisées à des fins illicites, potentiellement attentatoires à la vie privée ou, plus largement, frauduleuses, voire malveillantes.*

552 Onclusions dans les affaires C-293/12 et C-494/12 pendantes devant la CUCJ.

553 Es références ont été omises pour faciliter la lecture ; voir la référence note précédente.

76. En effet, les données ne sont pas conservées par les autorités publiques elles-mêmes, ni même sous leur contrôle direct, mais par les fournisseurs de services de communications électroniques eux-mêmes sur lesquels pèsent l'essentiel des obligations garantissant leur protection et leur sécurité ».

Et plus loin :

« 102. L'ingérence caractérisée dans le droit au respect de la vie privée que, comme conséquence de l'effet constitutif de la directive 2006/24, les États membres sont censés incorporer à leur propre ordre juridique, apparaît ainsi hors de proportion avec la seule nécessité de garantir le fonctionnement du marché intérieur, quand bien même il doit, par ailleurs, être considéré que cette collecte et cette conservation constituent des moyens adéquats et même nécessaires à la réalisation de l'objectif ultime poursuivi par ladite directive et visant à garantir les disponibilités desdites données aux fins de la recherche et de la poursuite d'infractions criminelles graves. En résumé, la directive 2006/24 ne parviendrait pas à surmonter le test de proportionnalité pour les raisons mêmes qui justifiaient sa base juridique. Les motifs de son salut au regard de la base juridique seraient, paradoxalement, les motifs de sa perte au regard de la proportionnalité. »

Avant de conclure :

« 131. En conclusion, la directive 2006/24 est dans son ensemble incompatible avec l'article 52, paragraphe 1, de la Charte, dans la mesure où les limitations à l'exercice des droits fondamentaux qu'elle comporte, du fait de l'obligation de conservation des données qu'elle impose, ne s'accompagnent pas des principes indispensables appelés à régir les garanties nécessaires à l'encadrement de l'accès auxdites données et de leur exploitation ».

7. L'accord du Safe Harbor ou « sphère de sécurité » – Décision de la commission du 26 juillet 2000[554]

Les normes de protection de la vie privée en Europe et aux États-Unis sont nettement différentes, et plus particulièrement aux États-Unis, le droit à la vie privée au sens défini ci-dessus ne protège presque pas les personnes ne se trouvant pas sur ce territoire.[555]

---

554 Décision de la Commission du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique document C(2000) 2441 (http://eur lex.europa.eu/LexUriServ/LexUriServ.do ?uri=OJ :L :2000 :215 :0007 :0047 :FR :PDF).

555 Note de la direction générale des politique internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, IPOL-LIBE_NT(2013)474405_FR.

Il est dès lors apparu nécessaire de trouver un cadre juridique apte à permettre le transfert de données à *des fins commerciales*, de l'Espace économique européen[556] vers les États-Unis.

Ce cadre juridique était d'autant plus nécessaire que, comme nous l'avons vu, les règles spécifiques de la directive 95/46 concernant l'échange de données avec des États-tiers, interdit le transfert de données personnelles en dehors des États non membres de l'EEE qui protégeraient les données personnelles à un niveau inférieur à celui de l'EEE.

Or, les États-Unis disposent d'un système de protection des données de leurs concitoyens, qui ne répond pas aux mêmes normes que celles adoptées dans le cadre de l'EEE. Sans le système du *Safe Harbor,* les exigences mises en place par la directive 95/46 auraient pu constituer une barrière aux échanges et transactions transatlantiques, puisque le non-respect des règles européennes relatives aux données personnelles par une entreprise américaine aurait pu ralentir ou suspendre des négociations commerciales ou conduire à des poursuites judiciaires en cas de violation des règles en vigueur.

Le cadre juridique de la « sphère de sécurité », le *Safe Harbor,* établit une passerelle entre les deux approches de respect de la vie privée en établissant un commun dénominateur à respecter par les entreprises et organisations américaines et permettant le transfert de données personnelles dans les respect du droit de l'EEE.

L'accord du *Safe Harbor* a été négocié entre le Département du Commerce des États-Unis *(Federal Trade Commission* ou *FTC)* et la Commission européenne afin de permettre aux entreprises américaines de certifier qu'elles respectent la législation de l'EEE afin d'obtenir l'autorisation de transférer des données à caractère personnel à des fins commerciales de l'EEE vers les États-Unis.

L'annexe I de la décision du 26 juillet 2000 précise que par donnée ou information à caractère personnel : « *il faut entendre toute donnée ou information concernant une personne identifiée ou identifiable qui entre dans le champ d'application de la directive, qui est transférée de l'Union européenne vers une organisation américaine et qui est enregistrée sous quelque forme que ce soit* ».

Si une entreprise américaine déclare par écrit adhérer aux principes de la sphère de sécurité, l'entreprise européenne devrait, en principe pourvoir, exporter des données à caractère personnel vers cette entreprise.

– *Les principes*

Le cadre juridique du *Safe Harbor* repose sur 7 principes qui doivent être respectés par l'entreprise désireuse d'obtenir la certification. Ces principes sont détaillés dans l'Annexe I de la Décision de la Commission du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et sont largement inspirés des principes mis en place par la directive 95/46 :

– Notification : l'information des personnes ;
– Choix : la possibilité accordée à la personne concernée de s'opposer à un transfert à des tiers ou à une utilisation des données pour des finalités différentes, le consentement explicite des personnes pour le recueil de données sensibles ;

556 Ci-après, EEE ; le *Safe Harbor* a été intégré dans l'accord sur l'EEE, par conséquent, l'Islande, le Liechtenstein et la Norvège ne sont pas considérés comme États-tiers dans l'application de cette norme.

- Transfert ultérieur : les principes de notification et de choix devraient être applicable au transfert de données à des tiers ;
- Sécurité : mesures de protection des données ;
- Intégrité des données : qualité et pertinence des données ;
- Accès : le droit d'accès, de rectification, de suppression des données ;
- Mise en œuvre : droit de recours, procédures de suivi et sanctions.[557]

Il faut cependant noter que la description des principes utilise un langage flou et ouvert à interprétation, qui de plus, est soumis au droit américain.

Le processus repose sur un système d'auto-certification volontaire par les entreprises américaines et prévoit un renouvellement de la certification tous les douze mois. L'entreprise intéressée par la certification doit faire parvenir à la *Federal Trade Commission,* une déclaration écrite annuelle attestant qu'elle respecte les principes du *Safe Harbor.* La *Federal Trade Commission* a pour mission de gérer le programme de certification et de surveiller sa mise en œuvre. Elle peut lancer des actions en justice contre une entreprise défaillante ou appliquer des amendes administratives aux entreprises qui, malgré leur déclaration, ne respectent pas *de facto* les principes du *Safe Harbor.*

Une fois que l'entreprise américaine est certifiée « *Safe Harbor* », elle rejoint la liste d'entreprises accréditées et tenue par le Département du Commerce des États-Unis. La liste de 3246 entreprises est consultable sur le site internet du Département du Commerce des États-Unis.[558]

Le système du *Safe Harbor* prévoit également que les plaintes de citoyens de l'EEE contre une entreprise ou organisation américaine relative à la protection des données personnelles devront être introduites devant des juridictions américaines (hormis quelques exceptions).

Mais en pratique, comme l'indique la récente étude commissionnée par le Parlement européen sur le *Safe Harbor : « Les négociateurs américains du ministère du commerce ont travaillé en étroite collaboration avec les lobbies commerciaux américains afin d'élaborer une liste de « questions fréquemment posées » permettant aux entreprises américaines d'interpréter l'accord sur la sphère de sécurité de manière à réduire les droits de l'UE en matière de protection de la vie privée, indiquant comment contourner les règles liées aux données identifiables, refuser les droits d'accès, et se soustraire à tout devoir de finalité ou à toute demande de suppression. La sphère de sécurité s'est avérée tellement complexe que pendant de nombreuses années, aucun citoyen de l'UE n'a suivi toutes les étapes du processus bureaucratique pour déposer une plainte ».*[559]

La directive 95/46 ainsi que les « *Safe Harbour Principles* » ne couvrent pas les données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en

---

557 Pour le détail des 7 principes, voir Annexe I de la décision de la Commission du 26 juillet 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:FR:PDF).

558 http://export.gov/safeharbor/ (fin septembre 2013).

559 Le programme de surveillance des États-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE, Note de la direction générale des politique internes, Département thématique C : Droits des citoyens et affaires constitutionnelles, IPOL-LIBE_NT(2013)474405_FR. http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%282013%29474405_FR.pdf.

matière pénale[560], ce qui inclut l'ensemble des fichiers de police, de justice et de renseignement. En effet, l'article 1er de la Décision de la Commission du 26 juillet 2000 relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité », indique que la décision ne s'applique qu'aux activités rentrant dans le domaine d'application de la directive 95/46.

Par ailleurs, l'annexe I paragraphe 4 de ladite Décision prévoit que « L'adhésion aux principes peut être limitée par : a) les *exigences relatives à la sécurité nationale*, l'intérêt public et le respect des lois des États-Unis ; b) les textes législatifs, les règlements administratifs ou les décisions jurisprudentielles qui créent des obligations contradictoires ou prévoient des autorisations explicites, pour autant qu'une organisation qui a recours à une telle autorisation peut démontrer que le non-respect des principes est limité aux mesures nécessaires pour garantir les intérêts légitimes supérieurs que cette autorisation vise à servir ; c) les exceptions ou les dérogations prévues par la directive ou par le droit national, à condition que ces exceptions ou dérogations soient appliquées dans des contextes comparables ».

L'échange de données à caractère personnel entre l'Union européenne et les États-Unis à des fins répressives, y compris la prévention et la répression du terrorisme et d'autres formes graves de criminalité, est régi, du moins en théorie, par un certain nombre d'accords au niveau de l'UE. Il s'agit de l'accord d'entraide judiciaire, de l'accord sur l'utilisation et le transfert des données des dossiers passagers (données PNR), de l'accord sur le traitement et le transfert de données de messagerie financière aux fins du programme de surveillance du financement du terrorisme (TFTP) et de l'accord entre Europol et les États-Unis.

– *Lacunes*

A la suite des diverses révélations qui nous préoccupent ici concernant des programmes américains de collecte de renseignements à grande échelle, la confiance bâtie notamment sur les « *Safe Harbour principles* » a été sévèrement ébranlée. Ces révélations ont abouti à une prise de conscience de l'insuffisance de la protection dont jouissent actuellement les données à caractère personnel et de la nécessité de revisiter et renforcer les règles en vigueur qui présentent de *sérieuses lacunes*.

En effet, depuis que le FISA a été amendé et élargi notamment en 2008, des entreprises américaines peuvent être contraintes de transmettre à la NSA des informations électroniques concernant des non-Américains. L'article 702 de la FISA[561] constitue un mandat général permettant aux autorités américaines de recueillir des données et d'intercepter des informations liées aux affaires étrangères des États-Unis, alors que les données à caractère personnel concernant les Américains bénéficient d'une protection supérieure. L'étendue que peut atteindre une telle délégation de compétences apparait aujourd'hui de manière manifeste et démesurée au regard des révélations de Snowden et des évolutions technologiques permettant la captation de quantités de données gigantesques au niveau mondial.

560 Article 25 de la directive 95/46.

561 Foreign Intelligence Surveillance Act of 1978 (décrit les procédures des surveillances physiques et électroniques, ainsi que la collecte d'informations sur des puissances étrangères soit directement, soit par l'échange d'informations avec d'autres puissances étrangères), modifié en 2008 par le FISA Amendments Act.

Le 27 novembre 2013, la Commission européenne a rendu public[562] le fruit de ses réflexions dans (1) un document stratégique (communication) sur les transferts de données transatlantiques, qui présente les enjeux et les risques faisant suite aux révélations sur les programmes américains de collecte de renseignements, ainsi que les mesures à prendre pour y répondre ; (2) d'une analyse du fonctionnement de la « sphère de sécurité », qui réglemente les transferts de données à des fins commerciales entre l'Union européenne et les États-Unis ; et (3) d'un rapport sur les conclusions du groupe de travail UE-États-Unis (MEMO/13/1059) sur la protection des données, créé en juillet 2013.

Ce rapport révèle aussi que d'importantes entreprises actives dans les nouvelles technologies qui ont participé à l'opération PRISM, sont des entreprises certifiées « *Safe Harbor* » et qu'il est donc permis de déduire que le système *Safe Harbor* doive être considéré comme ayant été un conduit important de données à caractère personnel ayant abouti à la collecte massive de données par la NSA.

Pourtant, ces pratiques, même si autorisées par la loi américaine, ne sont pas prévues dans le cadre juridique du *Safe Harbor* et ont, par conséquent, eu lieu en violation de cet accord et de la décision de la Commission qui le formalise dans le cadre juridique européen. Les principes du *Safe Harbor* ayant été établis pour assurer, aux États-Unis, un niveau de « protection adéquat » garantissant une protection des données à caractère personnel proche du niveau qui leur est garanti au sein de l'EEE, il faut considérer que les États-Unis ont détourné l'esprit de l'accord à leur profit. Le système du *Safe Harbor* n'a certainement pas été mis en place pour permettre le transfert de données qui pourraient ensuite être remises en masse aux autorités américaines de la sûreté, alors même que les autorités européennes de sûreté ne peuvent agir de la sorte.

La Commission européenne considère que la captation massive de données à caractère personnel par la NSA ne peuvent pas être considérées comme étant couvertes par la limitation de la protection des données, prévue dans le *Safe Harbor,* pour les besoins de la sûreté nationale. En effet, le caractère massif et sans autorisation préalable de la captation de données empêche que ce processus puisse être considéré comme nécessaire et proportionné aux intérêts de la sécurité nationale. S'agissant d'une atteinte à un droit fondamental de l'homme, il faut que celle-ci soit appréciée restrictivement comme prévue par la loi et limitée.

Par ailleurs, la Commission européenne présente aussi son réexamen des accords en vigueur sur les données des dossiers passagers (données PNR) (MEMO/13/1054) et sur le programme de surveillance du financement du terrorisme (TFTP), qui réglementent les échanges de données à des fins répressives dans ces secteurs.

Dans cette communication, la Commission indique notamment sa volonté d'adopter d'ici au printemps 2014 une réforme de la protection des données dans l'UE afin de garantir que les données à caractère personnel soient plus efficacement et intégralement protégées.

Par ailleurs, s'agissant plus particulièrement des relations transatlantiques, la Commission a présenté *13 recommandations visant à améliorer le fonctionnement de la « sphère de sécurité »*, jugé déficient à plusieurs égards d'après les conclusions d'une analyse également publiée le même jour par la Commission. Le dispositif devrait donc être revu et amélioré.

---

562 Newsroom de la Commission européenne : http://ec.europa.eu/justice/newsroom/data-protection/news /131127_en.htm.

S'agissant de la coopération policière et judiciaire en matière pénale, la Commission voudrait faire pression sur l'administration américaine pour qu'elle s'engage, comme principe général, à recourir à un cadre juridique, tel que les accords sectoriels et d'entraide judiciaire conclus entre l'UE et les États-Unis (comme l'accord sur les données PNR et le programme de surveillance du financement du terrorisme), chaque fois que des transferts de données sont nécessaires à des fins répressives. *S'adresser directement aux entreprises ne devrait être possible que dans des cas exceptionnels clairement définis et susceptibles d'un contrôle juridictionnel.*

Plus largement, la Commission européenne a déclaré souhaiter que le réexamen annoncé par la présidence américaine des activités de l'Agence de sécurité nationale, comporte une protection des citoyens de l'Union européenne ne résidant pas aux États-Unis. Ces derniers devraient pourvoir bénéficier des mêmes garanties que les citoyens américains.

– *Réforme globale des règles en matière de protection des données*

Comme annoncé en janvier 2012[563], la Commission planche sur une réforme globale en matière de protection des données. La réforme vise à mettre à jour et moderniser les principes inscrits dans la directive de 1995 relative à la protection des données afin de garantir à l'avenir les droits en matière de respect de la vie privée. Cette réforme comprend deux propositions législatives : un *règlement* définissant un cadre général de l'UE pour la protection des données et une *directive* relative à la protection des données à caractère personnel traitées à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ainsi que d'activités judiciaires connexes.

Les principales modifications envisagées par la réforme sont notamment les suivantes[564] :

- un *corpus unique de règles relatives à la protection des données sera valable dans toute l'Union*. Les obligations administratives inutiles, comme celles en matière de notification qui incombent aux entreprises, seront supprimées, ce qui représentera pour ces dernières une économie annuelle de quelque 2,3 milliards d'EUR ;
- en lieu et place de l'obligation actuelle imposée à toutes les entreprises de notifier l'ensemble des activités concernant la protection de données à des autorités de contrôle compétentes en la matière – cette obligation étant à l'origine de formalités administratives inutiles coûtant 130 millions d'EUR par an aux entreprises, le règlement impose davantage d'obligations aux entités procédant au traitement de données à caractère personnel et accroît leur responsabilité ;
- Ainsi, les entreprises et organisations devront, dans les meilleurs délais (si possible, dans un délai de 24 heures), notifier à l'autorité de contrôle nationale les violations graves de données à caractère personnel ;
- les organisations n'auront plus comme interlocuteur qu'une seule autorité nationale chargée de la protection des données dans le pays de l'Union où elles ont leur établissement principal. De même, les citoyens pourront s'adresser à l'autorité chargée de la protection des données dans leur pays, même lorsque leurs données

563 Ommuniqué de presse : http://europa.eu/rapid/press-release_IP-12-46_fr.htm.
564 Ommuniqué de presse : http://europa.eu/rapid/press-release_IP-12-46_fr.htm.

sont traitées par une entreprise établie en dehors du territoire de l'UE. Chaque fois que le consentement de la personne concernée est exigé pour que ses données puissent être traitées, il est précisé que ce consentement ne sera pas présumé, mais devra être donné explicitement.
- l'accès des personnes concernées à leurs propres données sera facilité, de même que le transfert de données à caractère personnel d'un prestataire de services à un autre (droit à la portabilité des données). La concurrence entre prestataires de services s'en trouvera renforcée.
- un « droit à l'oubli numérique » aidera les citoyens à mieux gérer les risques liés à la protection des données en ligne : ils pourront obtenir la suppression de données les concernant si aucun motif légitime ne justifie leur conservation.
- les règles de l'Union devront s'appliquer si des données à caractère personnel font l'objet d'un *traitement à l'étranger* par des entreprises implantées sur le marché européen et proposant leurs services aux citoyens de l'Union.
- les autorités nationales indépendantes chargées de la protection des données seront renforcées afin qu'elles puissent mieux faire appliquer et respecter les règles de l'UE sur le territoire de l'État dont elles relèvent. Elles seront habilitées à infliger des amendes aux entreprises qui enfreignent les règles de l'Union relatives à la protection des données. Ces amendes pourront atteindre 1 million d'EUR ou 2 % du chiffre d'affaires annuel global de l'entreprise.
- Une nouvelle *directive appliquera les règles et principes généraux relatifs à la protection des données à la coopération policière et judiciaire en matière pénale*. Les règles s'appliqueront aux traitements aussi bien transfrontières que nationaux de données à caractère personnel ».

B. SOUVERAINETÉ DE LA BELGIQUE

Le programme de surveillance dont il est question dans la présente étude, se fonde manifestement sur une structure internationale à laquelle collaborent certainement les États-Unis (NSA) et le Royaume-Uni *(*GCHQ), mais aussi sans doute d'autres États du Conseil de l'Europe et de l'Union européenne. Ces derniers ont sans doute été dépassés par la structure à laquelle ils ont collaboré et se sont retrouvés eux-mêmes victimes de la surveillance massive.

Il faut se rappeler que l'accord sur le renseignement en matière de télécommunications UK-USA, déjà conclu en 1947 et auquel sont parties 5 pays anglo-saxons (États-Unis, Royaume-Uni, Canada, Nouvelle-Zélande et Australie) est l'accord de base pour la surveillance des communications au sens large, et était déjà à la base de l'ossature du système de surveillance Echelon, qui a bousculé l'Europe dans les années 2000. L'excellente étude que Dimitri Yernault a consacrée à ce système d'écoute garde toute son actualité et pourrait être ici quasi-intégralement reproduite.[565]

[565] Dimitri Yernault, « De la fiction à la réalité : le programme d'espionnage électronique global « Echelon » et la responsabilité internationale des États au regard de la convention européenne des droits de l'homme », *RBDI,* 2000, 137 et suiv.

Une question fondamentale posée par la surveillance massive de communications électroniques non consenties par l'État sur le territoire duquel la surveillance a lieu, même au départ, d'une installation sur le territoire d'un État tiers, est de savoir si elle viole la souveraineté de cet État. La réponse est positive si l'État n'y a pas consenti, même si ces écoutes sont conformes au droit de l'État qui y procède (directement ou par l'intermédiaire d'entreprises commerciales qui y collaborent volontairement ou contraintes) : ce type d'écoutes porte atteinte à la souveraineté de l'État sur le territoire duquel les communications sont interceptées.

En effet, l'interception de communication est par définition un acte de contrainte – clandestin ou autorisé par la législation de l'État tiers – qui s'exerce sur le territoire d'un autre État et viole sa souveraineté.[566]

L'État sur le territoire duquel s'exerce la contrainte doit donner son consentement préalable.[567] Si ce n'est pas le cas, les écoutes, surveillance, interceptions clandestines, et *a fortiori* celles opérées par des systèmes de *malware* violent la souveraineté de cet État. A ce titre, elle peut justifier une réaction diplomatique.

Il en va de même des écoutes clandestines opérées au départ des ambassades des États tiers situées sur le territoire de l'État sur le territoire duquel les écoutes et surveillances sont effectuées. Elles peuvent pareillement justifier la mise en cause des bonnes relations diplomatiques.

En effet, elles enfreignent la Convention de Vienne sur les relations diplomatiques du 18 avril 1961, notamment l'article 3d qui [ne] permet à la mission diplomatique [que] de *d)* S'informer par tous les *moyens licites* des conditions et de l'évolution des événements dans l'État accréditaire et faire rapport à ce sujet au gouvernement de l'État accréditant ;

Les missions diplomatiques ont en vertu de l'article 41.1 « *le devoir de respecter les lois et règlements de l'État accréditaire. Elles ont également le devoir de ne pas s'immiscer dans les affaires intérieures de cet État* ». Du reste, comme l'exige l'article 41.3, les locaux de la mission ne peuvent être utilisés d'une manière incompatible avec les fonctions de la mission qui comme on vient de le voir, ne peut s'informer que par des moyens licites (art. 3d susmentionné).

Enfin, l'article 27.1. stipule : « *1. L'État accréditaire permet et protège la libre communication de la mission pour toutes fins officielles. En communiquant avec le gouvernement ainsi qu'avec les autres missions et consulats de l'État accréditant, où qu'ils se trouvent, la mission peut employer tous les moyens de communication appropriés, y compris les courriers diplomatiques et les messages en code ou en chiffre. Toutefois, la mission ne peut installer et utiliser un poste émetteur de radio qu'avec l'assentiment de l'État accréditaire* ».

Il va sans dire que ce type d'interception clandestine et sauvage de communications viole en soi le droit à la vie privée, tel que protégé par les dispositions précitées et engage la responsabilité internationale de l'État, qu'il soit membre du Conseil de l'Europe ou non, de l'Union européenne ou non. En effet, si c'est le cas, la responsabilité internationale pour violation de la souveraineté de l'État se double de la violation des traités internationaux applicables au droit au respect de la vie privée.

---

566 CPJI, *Affaire du Lotus,* 7 septembre 1927, *Recueil,* Série A, n° 9, 18.

567 Voir Les travaux de l'Institut de droit international, *Annuaire de droit international,* vol. 68-I, 1999 ; voir aussi Dimitri Yernault, *op. cit.,* 180.

C. APERÇU DES MOYENS D'ACTION À LA DISPOSITION DE L'ÉTAT, DES CITOYENS ET DES ENTREPRISES

Il est évidemment impossible, à défaut d'être saisi de faits établis précis dénoncés dans des cas particuliers, d'étudier toutes les voies de recours possibles dans une affaire aux dimensions tentaculaires comme celle dénoncée par E. Snowden et dont toutes les responsabilités n'ont pas encore été établies. Une des actions à mener pourrait être de demander la tenue d'une enquête parlementaire pour établir précisément les faits et les éléments de responsabilité des acteurs. L'État sur le territoire duquel des violations structurelles de droits de l'homme ont lieu a l'obligation générale de « prévenir » celles-ci ou de les sanctionner.[568] Il ne peut donc rester indifférent. En l'occurrence, il semble clair que surveillance massive des données à caractère personnel tel qu'effectué par la NSA et/ou d'autres acteurs sur le territoire belge est structurelle.

A ce stade, il ne peut s'agir ici que de soumettre quelques pistes.

1. La Cour internationale de Justice

L'État peut soumettre le différend international, à savoir la mise en cause de la responsabilité internationale de l'État étranger qui a effectué les écoutes illégales ou qui a permis que soient effectuées les écoutes illégales, par exemple en mettant son territoire à disposition de l'interception et l'écoute illégale, et ce devant la Cour internationale de Justice, si les conditions très restrictives de sa compétence sont réunies. La même juridiction peut être saisie de la question du respect de la Convention de Vienne sur les relations diplomatiques et consulaires.

2. La Cour européenne des droits de l'homme[569]

Si l'État responsable de la surveillance ou qui y a collaboré est membre du Conseil de l'Europe, une requête inter-étatique devant la Cour européenne des droits de l'homme est un moyen juridique de faire cesser les violations et d'obtenir réparation. Elle avait été sérieusement envisagée dans l'affaire dite « Echelon ».[570] Si en l'occurrence, l'intervention des services secrets du Royaume-Uni ou d'autres États parties à la CEDH étaient démontrée, il s'agirait d'une action exemplaire.

3. Juridictions belges : piratage informatique et infractions pénales

– Les entreprises belges victimes d'interceptions illégales des données dont elles disposent peuvent, selon les faits qui seront établis, déposer plainte contre l'État étranger devant les juridictions de cet État, mais aussi devant les juridictions belges, s'il est établi que les faits ont un lien avec la Belgique (interception en Belgique). Par exemple, le *malware* qui semble avoir infecté le système informatique de Belgacom

568 Voir notamment Dimitri Yernault, op. cit. 214.

569 Ce recours paraît plus efficace qu'un recours devant le Comité des droits de l'homme, mais cette possibilité ne doit pas être exclue.

570 Voir Dimitri Yernault, *op. cit.,* 154 et suiv.

peut faire l'objet d'action judiciaire en Belgique. Un exposé des faits plus précis est toutefois nécessaire pour donner une étude juridique sur cette possibilité !

- Dans la mesure où les dispositions spécifiques sur la protection des données à caractère personnel le prévoient, elles sont évidemment susceptibles de s'appliquer aux personnes privées dès qu'elles sont responsables du traitement de données à caractère personnel au sens des dispositions analysées ci-dessus. Ainsi en est-il particulièrement des directives qui s'adressent aussi aux fournisseurs de réseaux, de services de télécommunication, etc. qui doivent évidemment être affinées dans chaque cas d'espèce. Pour Facebook, par exemple, une étude exhaustive a été réalisée.[571] Elle devrait l'être pour chaque responsable potentiel dont le rôle pourrait être déterminé dans l'affaire qui nous préoccupe.
- Selon l'établissement des faits, s'il était établi que des entreprises privées ont collaboré, à l'insu de l'État, à la mise en œuvre des procédés d'interception (sur le câble optique à Ostende par exemple ou en transmettant volontairement des données à caractère personnel un État étranger (NSA ou autre), l'État ou des particuliers ou des entreprises victimes de ce piratage informatique peuvent déposer plainte au pénal en vertu de la loi sur la protection de la vie privée du 8 décembre 1992, sur la base notamment des articles 550*bis* et 314*bis* du code pénal et 124 et 145 de la loi du 13 juin 2005 relative aux communications électroniques. Le piratage informatique est en effet pénalement sanctionné.[572]

Le titre IX*bis* du code pénal belge est intitulé : *« Infractions contre la confidentialité, l'intégrité et la disponibilité des systèmes informatiques et des données qui sont stockées, traitées ou transmises par ces systèmes ». Les articles 550bis et 550ter punissent divers comportements de peines allant de 3 mois à 5 ans d'emprisonnement. La loi pénale belge interdit d' « accéder à un système informatique » ou de « s'y maintenir » (article 550bis, § 1er, alinéa 1), mais également de faire « un usage quelconque d'un système informatique appartenant à un tiers » (article 550bis, § 3, 2°) ou de « causer un dommage quelconque à ce système » (article 550bis, § 1er, 3°). La loi punit « celui qui ordonne la commission d'une des infractions visée aux §§ 1 à 5 »* (article 550*bis*, § 6), et sanctionne *« celui qui, sachant que des données ont été obtenues par la commission d'une des infractions visées aux §§ 1 à 3, les détient, les révèle à une autre personne ou les divulgue, ou fait un usage quelconque des données ainsi obtenues » d'un emprisonnement de six mois à trois ans et/ou d'une amende de 26 à 100.000 euros (article 550bis, § 7) ».*

Le titre V du code pénal belge (*« Des crimes et des délits contre l'ordre public commis par des particuliers »*) contient un chapitre VII*bis* intitulé *« Infractions relatives au secret des communications et des télécommunications privées »*. L'article 314*bis,* § 1er puni d'un emprisonnement de 6 mois à 1 an et/ou d'une amende de cent à dix mille euros celui qui *« prend connaissance »*, *« enregistre » « pendant leur transmission »* des *« communications privées »*, *« auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications »* ou *« installe ou fait installer un appareil quelconque »* à cette fin. L'article 314*bis,* § 2 puni d'un emprisonnement de six mois à deux ans et/ou à une amende

571 Jean-Philippe Moiny, Facebook au regard des règles européennes concernant la protection des données, *Rev. Eur.de droit de la consommation,* 235.

572 La législation belge est exemplaire à ce sujet.

de cinq cent à vingt mille euros celui qui révèle, divulgue, ou « *utilise sciemment d'une manière quelconque une information obtenue de cette façon* ».

Les individus et entreprises qui ont été victimes de ces infractions peuvent déposer une plainte pénale en Belgique, soit auprès du procureur du Roi, soit en se constituant partie civile. La question de la compétence territoriale afin de pouvoir déposer une telle plainte se résout en fonction des faits de la cause. Soit le fait infractionnel a été commis en Belgique (par exemple l'accession illégale à un système informatique en Belgique), soit les conséquences du crime ont fait sentir leurs effets en Belgique (si on applique aux cybercrimes un enseignement classique de la cour de Cassation, initiée à l'occasion d'une affaire relative à un chèque émis à Téhéran, et tiré sur une banque belge[573]).

Cela dit, en droit belge, ces intrusions informatiques peuvent être légales dans le cas où elles sont réalisées, par le biais des dispositions du code d'instruction criminelle relatives à la saisie de données informatiques, via le procédé de la perquisition d'un ordinateur et de l'extension de cette perquisition, ordonnée par le juge d'instruction par ordonnance motivée, « vers un système informatique qui se trouve dans un autre lieu » (article 88*ter* du code d'instruction criminelle) et par l'injonction donnée par le même magistrat à une personne ayant « *une connaissance particulière* » afin d'accéder aux données stockées « *dans une forme compréhensible* » (article *88quater* du code d'instruction criminelle). Cette mesure d'enquête peut également être réalisée à de strictes conditions, en tant que « *méthode exceptionnelle de recueil de données* » par la Sûreté de l'État ou par le Service général du renseignement et de la sécurité des Forces armées (article 18/16, §§ 1 à 5 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité).

Toute intrusion informatique ou utilisation de données recueillies ou utilisées en Belgique, sans autorisation légale, demeure une infraction pénale. Le code d'instruction criminelle belge prévoit en son article 29, une obligation pour tout fonctionnaire qui viendrait à découvrir une infraction, de la dénoncer au procureur du roi. Cette obligation est générale et concerne toute infraction.[574]

4. Usage des informations obtenues par un système de surveillance illégal

La question est de savoir dans le cas où un service de police ou de renseignement reçoit ce type d'information, s'il peut l'utiliser dans le cadre de ses missions. La loi sur le recueil de données prévoit que si une mesure de recueil de donnée exceptionnelle, comme l'intrusion informatique, a été réalisée illégalement, la commission chargée de la surveillance des méthodes spécifiques et exceptionnelles de recueil de données des services de renseignement et de sécurité, conserve ces données et interdit aux services de renseignement et de sécurité, d'exploiter ces données (article 18/10, § 6, alinéa 4 de la loi du 30 novembre 1998 organique des services de renseignement et de sécurité). Il est à noter qu'aucune disposition ne réglemente les conséquences à donner dans le cas où cette illégalité a été réalisée par un service étranger. Une indication de la solution à développer peut être trouvée dans les discussions qui ont précédé l'adoption de la loi du 4 février 2010

573 Tribunal correctionnel, Dendermonde, 29 septembre 2008, *Tijdschrift voor Strafrecht,* 2009/2, 111-114.

574 Alain Winants, De Veiligheid van de Staat en de BIM-Wet, in Wauter Van Laethem, Dirk Van Daele en Bart Vangeebergen(Eds), *De Wet op de bijzondere inlichtingenmethoden,* Intersentia, Antwerpen Oxford, 141.

relative aux MRD. En effet, la loi de 1998 relative aux services de renseignement mentionne la coopération avec les services étrangers en son article 20, § 1er. Néanmoins, le président du Comité permanent R a indiqué que *« le Comité ne peut pas contrôler les services de renseignement étrangers. Il serait indiqué de compléter la loi sur ce point de telle sorte que la légalité des opérations de services de renseignement étrangers amis, admis sur notre territoire, puisse également être contrôlée par la Sûreté de l'État »*.[575] Monsieur Winants a déclaré à cette occasion : *« Si un service de renseignement étranger excède ses pouvoirs, la Sûreté de l'État a la possibilité d'intervenir, sur la base de l'article précité (article 20 de la loi de 1998) »*.[576] Monsieur Hellemans, chef du SGRS, a quant à lui déclaré : *« Le SGR part du principe qu'il est systématiquement informé par les services étrangers dès lors que ceux-ci poursuivent un objectif en Belgique. Le service entretient de bons contacts avec les pays amis et a recours à un système d'échange de données. Le service reste bien évidemment responsable des données qui sont recueillies sur le territoire belge »*.[577]

Il ressort de tout ceci, premièrement, que la réalisation par un service étranger d'une méthode de recueil de donnée exceptionnelle en Belgique, telle que l'intrusion informatique n'est pas réglementée, deuxièmement que cette méthode de renseignement est une infraction pénale, et, troisièmement, qu'il est interdit aux services belges d'utiliser les informations obtenues de manière illégale, à défaut de quoi les services belges se rendraient également coupable de la commission d'une infraction s'ils le font sciemment.

La problématique de la coopération avec les services étrangers et la manière de contrôler celle-ci est une des priorités du Comité permanent R. Dès son rapport d'activités de 2008, le Comité a relaté diverses contributions réalisées à l'étranger afin de promouvoir un contrôle démocratique effectif sur les services de renseignement, et ces initiatives bénéficient du soutien du Rapporteur Spécial des Nations Unies pour la promotion et la protection des droits de l'homme et des libertés fondamentales dans la lutte contre le terrorisme, Martin Sheinin.[578] L'échange d'informations avec des services « amis » n'est pour le moment soumis qu'à des principes éthiques, et cette faille dans les lois de contrôle des services de renseignement a été critiquée, en proposant que des réglementations nouvelles viennent remplir ce vide juridique.[579]

La question de l'utilisation judiciaire de ce type d'informations se résout différemment. En effet, le droit de la procédure pénale belge prévoit une règle d'exclusion des éléments de preuve obtenus de manière illégale. Cette exclusion n'est néanmoins pas absolue. En effet, la loi du 24 octobre 2013 a inséré dans le code d'instruction criminelle un nouvel article 32, qui se lit de la manière suivante :

« Art. 32. La nullité d'un élément de preuve obtenu irrégulièrement n'est décidée que si :
- *le respect des conditions formelles concernées est prescrit à peine de nullité, ou ;*
- *l'irrégularité commise a entaché la fiabilité de la preuve ou ;*
- *l'usage de la preuve est contraire au droit à un procès équitable ».*

---

575 *Doc. Parl,* Chambre, Session 52ème législature, 2009-2010, DOC 52 / 2128/000, 41.

576 *Ibid.*

577 *O.c.,* 46.

578 Comité permanent R, *Rapport d'activités 2008*, 87.

579 Pour une étude approfondie consacrée à cette question, voir e.a. Elizabeth Sepper, Democracy, Human Rights and Intelligence Sharing, *Texas International Law Journal,* Vol. 46 : 151, 2010, pp. 153-206 ; European Parliament, Committee on Civil Liberties, Justice and Home Affairs, *Working Document 5 on Democratic oversight of Member State intelligence services and of EU intelligence bodies,* 11 novembre 2013, DT\1009342EN.doc.

Cette loi fait suite à la jurisprudence de la cour de Cassation belge dite « Antigone » du 14 octobre 2003.[580] Cette jurisprudence avait déjà donné lieu à une loi du 9 décembre 2004 *« sur l'entraide judiciaire internationale en matière pénale et modifiant l'article 90ter du Code d'Instruction Criminelle »*, qui dispose, en son article 13 :

> *« Art. 13. Ne peuvent être utilisés dans le cadre d'une procédure pénale menée en Belgique, les éléments de preuve :*
> *1° recueillis irrégulièrement à l'étranger, lorsque l'irrégularité :*
> *– découle, selon le droit de l'État dans lequel l'élément de preuve a été recueilli, de la violation d'une règle de forme prescrite à peine de nullité ;*
> *– entache la fiabilité de la preuve ;*
> *2° ou dont l'utilisation viole le droit à un procès équitable ».*

Cette réglementation de la preuve implique donc que toute illégalité/irrégularité n'entraîne pas l'écartement automatique de cet élément de preuve. Néanmoins, à l'occasion d'un livre qui a fait date[581], le président de la section pénale de la cour de Cassation de Belgique a indiqué qu'au-delà des nullités prévues spécifiquement par un texte de loi, ou de celles qui entachent la fiabilité de la preuve ou dont l'usage viole le droit à un procès équitable, il existe également les nullités infractionnelles, c'est-à-dire le cas où la preuve est *« entachée par la commission d'un délit »*.[582] A l'occasion d'une étude de la jurisprudence rendue en la matière, cet éminent magistrat distingue, en ce qui concerne les délits commis par les organes de recherche, la situation d'un délit commis afin d'obtenir une preuve, de celle d'une infraction commise au moment du constat d'une infraction commise par un délinquant.[583] Dans le premier cas, par exemple une intrusion illégale dans un système informatique, la preuve ne sera pas recevable. Dans le second cas, par exemple la participation à un trafic de stupéfiants en vue d'en arrêter les auteurs, *« dès lors que la résolution criminelle est manifestement antérieure à l'intervention policière et que l'autorité verbalisante ne commet que des irrégularités extérieures aux saisies, perquisitions, observations et auditions, la preuve serait recevable ».*[584]

580 RG P.03.0762.N.
581 Jean de CODT, *Des nullités de l'instruction et du jugement,* Bruxelles, Larcier, 2006, 233 pp.
582 *O.c.,* 16.
583 *O.c.,* 103-104.
584 *O.c.,* 105.

ACTIVITEITENVERSLAG 2013
RAPPORT D'ACTIVITÉS 2013

Quis custodiet ipsos custodes?

Quis custodiet ipsos custodes? is een publicatiereeks die een bijdrage wil leveren tot het bevorderen van een geïnformeerde discussie over de werking, de bevoegdheden en de controle op de inlichtingen- en veiligheidsdiensten en op het inlichtingenwerk. In deze reeks worden o.m. wetenschappelijke studies, de activiteitenverslagen van het Vast Comité I en verslagboeken van colloquia opgenomen.

Redactie

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, Leuvenseweg 48 bus 5, 1000 Brussel (02 286 29 88).

Reeds verschenen in deze reeks

1) D. Van Daele, en B. Vangeebergen, *Inlichtingendiensten en strafprocedure in Nederland, Duitsland en Frankrijk,* 2006, 166 p.
2) Vast Comité I, *Activiteitenverslag 2006,* 2007, 147 p.
3) Vast Comité I, *Activiteitenverslag 2007,* 2008, 87 p.
4) Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.
5) Vast Comité I, *Activiteitenverslag 2008,* 2009, 131 p.
6) W. Van Laethem, D. Van Daele en B. Vangeebergen (eds.), *De Wet op de bijzondere inlichtingenmethoden,* 2010, 298 p.
7) Vast Comité I, *Activiteitenverslag 2009,* 2010, 127 p.
8) Vast Comité I, *Activiteitenverslag 2010,* 2011, 119 p.
9) Vast Comité I, *Activiteitenverslag 2011*, 2012, 134 p.
10) W. Van Laethem en J. Vanderborght (eds), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, 2013, 565 p.
11) Vast Comité I, *Activiteitenverslag 2012*, 2013, 115 p.
12) Vast Comité I, *Activiteitenverslag 2013*, 2014, 210 p.

ACTIVITEITENVERSLAG 2013

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

intersentia
Antwerpen – Cambridge

Voorliggend *Activiteitenverslag 2013* werd door het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten goedgekeurd op de vergadering van 24 juli 2014.

(*getekend*)
Guy Rapaille, voorzitter
Gérald Vande Walle, raadsheer
Pieter-Alexander De Brock, raadsheer
Wouter De Ridder, griffier

Activiteitenverslag 2013
Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten

ISBN 978-94-000-0551-8
D/2014/7849/156
NUR 823

INHOUD

LIJST MET AFKORTINGEN

ACOS-IS	*Assistant Chief of Staff Intelligence and Security*
ACOS Ops & Trg	Stafdepartement *Operations and Training*
ADIV	Algemene Dienst inlichting en veiligheid van de Krijgsmacht
BELINT	*Belgian intelligence*
BENIC	*Belgian National Intelligence Cell*
BIA	*Belgian Intelligence Academy*
BIC	*Battle Group Intelligence Cell*
BIM	Bijzondere inlichtingenmethoden
BIM-Commissie	Bestuurlijke Commissie belast met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door inlichtingen- en veiligheidsdiensten
BIM-Wet	Wet van 4 februari 2010 betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten
BISC	*Belgian Intelligence Studies Centre*
BOM	Bijzondere opsporingsmethoden
BS	Belgisch Staatsblad
CANVEK	Commissie van advies voor de niet-verspreiding van kernwapens
CBPL	Commissie voor de bescherming van de persoonlijke levenssfeer
CCB	Centrum voor Cybersecurity België
CFI	Cel voor Financiële Informatieverwerking
CHOD	*Chief of Defense*
CIA	*Central Intelligence Agency*
CPOE	*Comprehensive Preparation of the Operational Environment*
CRIV	Compte Rendu Intégral – Integraal Verslag
EVRM	Europees Verdrag voor de Rechten van de Mens
FragO	*Fragmentary Orders*
FOD	Federale overheidsdienst
GCHQ	*Government Communications Headquarters*
Parl.St.	Parlementaire Stukken van Kamer en Senaat

Hand.	Handelingen
HUMINT	*Human intelligence*
ICT	*Information and Communication Technologies*
IMINT	*Image intelligence*
ISAF	*International Security Assistance Force*
ISTAR	*Intellligence, Surveillance, Target Acquisition and Reconnaissance*
JIB	*Joint Information Box*
K.B.	Koninklijk besluit
KB C&VM	Koninklijk besluit van 24 maart 2000 tot uitvoering van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veilig-heidsadviezen
KB OCAD	Koninklijk besluit van 28 november 2006 tot uitvoering van de Wet van10 juli 2006 betreffende de analyse van de dreiging
MAT	*Military Assistance Team*
M.B.	Ministerieel besluit
MCIV	Ministerieel Comité voor inlichting en veiligheid
NAVO	Noord-Atlantische Verdragsorganisatie
NSA	*National Security Agency*
NVO	Nationale Veiligheidsoverheid
OCAD	Coördinatieorgaan voor de dreigingsanalyse
OEF	*Operation Enduring Freedom*
OSINT	*Open sources intelligence*
PRT	*Provincial Reconstruction Team*
RFI	*Request for information*
SIGINT	*Signals intelligence*
s.l.	*sine loco*
SOP	*Standing Operating Procedure*
Sv.	Wetboek van Strafvordering
Sw.	Strafwetboek
UNO	*United Nations Organisation*
Vast Comité I	Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten
Vast Comité P	Vast Comité van Toezicht op de politiediensten
Vr. en Antw.	Schriftelijke vragen en antwoorden (Kamer of Senaat)
VSSE	Veiligheid van de Staat
W.Beroepsorgaan	Wet van 11 december 1998 houdende oprichting van een beroepsorgaan inzake veiligheidsmachtigingen, veilig-heidsattesten en veiligheidsadviezen
W.C&VM	Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen

W.I&V	Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst
WEP	Wetenschappelijk en economisch potentieel
WOB	Wet van 11 april 1994 betreffende de openbaarheid van bestuur
W.OCAD	Wet van 10 juli 2006 betreffende de analyse van de dreiging
W.Toezicht	Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatie-orgaan voor de dreigingsanalyse

WOORD VOORAF

2013 stond voor het Vast Comité I in het teken van twee totaal verschillende gebeurtenissen, die elk op hun manier belangrijk waren.

De eerste was zijn twintigjarig bestaan. Op 24 mei 1993 ging het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten immers effectief van start. Deze verjaardag konden wij niet onopgemerkt laten voorbij gaan. Er werd een meer dan 500 bladzijden tellende feestbundel 'Inzicht in toezicht' opgesteld, waarin omzeggens elk aspect van de democratische controle op de inlichtingendiensten aan bod kwam en waarbij alle betrokken actoren van vroeger en nu de gelegenheid kregen hun visie te belichten. Het boek werd onder auspiciën van de Senaatsvoorzitster op gepaste wijze voorgesteld in de Senaat.

Als één ding duidelijk is geworden, is het wel dat het Vast Comité I in die twintig jaar een vaste plaats heeft verworven in ons democratisch bestel. Het is een organisatie geworden die waakt over de concrete werking van de inlichtingendiensten en die met zijn verslagen en aanbevelingen een fundamentele bijdrage levert in het debat over de taken en de bevoegdheden ervan. Dit was alleen mogelijk dankzij de inzet en de expertise van eenieder die werkt of gewerkt heeft voor het Vast Comité I, ongeacht zijn of haar positie binnen de organisatie.

Het Vast Comité I van vandaag is zeker niet meer hetzelfde als het toezichtorgaan dat in 1993 van start ging. Daar hebben vele wetswijzingen en voortschrijdende inzichten in de praktijk voor gezorgd. Soms betrof het zeer kleine, technische ingrepen. Maar sommige aanpassingen hebben de gedaante van het Comité en zijn werkprocessen, danig gewijzigd. Dat die evolutie nog niet ten einde is, bewijst de Wet van 6 januari 2014: met de hervorming van de Senaat ingevolge de zesde staatshervorming, is het aanspreekpunt van het Comité in het Parlement sinds de verkiezingen van 25 mei 2014 verhuisd naar een eengemaakte 'Commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I' in de Kamer die zowel de politie- als de inlichtingendiensten zal controleren. Maar er is meer. De commissie wordt anders samengesteld – de voorzitters van alle politieke fracties krijgen vanaf nu een zitje – én haar leden zouden ook kennis kunnen nemen van geclassificeerde informatie. De toekomst zal uitwijzen welke invloed die wijzigingen hebben op de parlementaire controle.

Dé andere gebeurtenis uit 2013, die vooral de tweede helft van het jaar kleurde, was het feit dat Edward Snowden, een voormalig medewerker van een Amerikaanse inlichtingendienst, er in geslaagd was tienduizenden uiterst

gevoelige documenten van de *National Security Agency* te kopiëren en door te spelen aan journalisten. Herhaaldelijk verschenen er dan ook ontluisterende berichten in de pers over wereldwijde, massale data-captatie en economische en politieke spionage door de Amerikaanse en Britse inlichtingendiensten. Het hoeft geen betoog dat hierdoor de internationale inlichtingengemeenschap behoorlijk door mekaar werd geschud. Deze onthullingen vormden het startschot van parlementaire, gerechtelijke en inlichtingenonderzoeken over de hele wereld. Zo ook in België. Het Vast Comité I startte in dit kader niet minder dan vier onderzoeken op.

Dat bepaalde grootmachten al geruime tijd over verregaande middelen en programma's beschikten om aan massale data-captatie te doen, was niet nieuw. Wel nieuw was het gegeven dat deze elektronische informatiegaring alomvattend en massaal plaatsgreep en dit met de meest geavanceerde *soft-* en *hardware* en met een ongekende inzet aan menselijke en financiële middelen. Een tweede nieuw element was dat het steeds duidelijker werd dat grootmachten niet nalieten 'bevriende landen' economisch en politiek te bespioneren door er aan massale of gerichte data-captatie te doen. Hieruit zullen door bewindslieden, inlichtingendiensten maar ook toezichthouders, de nodige lessen moeten worden getrokken.

Guy Rapaille,
Voorzitter van het Vast Comité van Toezicht
op de inlichtingen- en veiligheidsdiensten

1 juni 2014

HOOFDSTUK I
DE OPVOLGING VAN DE AANBEVELINGEN VAN HET VAST COMITÉ I

Eén van de voornaamste taken van het Vast Comité I bestaat erin om ten behoeve van de wetgever en de uitvoerende macht aanbevelingen te formuleren die in het bijzonder betrekking hebben op de rechtmatigheid, de coördinatie en de doelmatigheid van het optreden van de twee Belgische inlichtingendiensten, van het OCAD en – in beperkte mate – van diens ondersteunende diensten.[1] De aanbevelingen die het Comité in 2013 formuleerde, zijn opgenomen in het laatste hoofdstuk van dit activiteitenverslag. In dit inleidende hoofdstuk worden de belangrijkste initiatieven opgesomd die de diverse actoren namen in de lijn van voorgaande aanbevelingen van het Vast Comité I. Tevens wordt extra aandacht gevestigd op aanbevelingen die het Comité essentieel acht, maar die vooralsnog niet werden geïmplementeerd.

I.1. INITIATIEVEN EN REALISATIES IN DE LIJN VAN DE DIVERSE AANBEVELINGEN

I.1.1. EEN FEDERALE STRATEGIE VOOR DE BEVEILIGING VAN INFORMATIE- EN COMMUNICATIESYSTEMEN

In de huidige samenleving is de beveiliging van communicatie- en informaticasystemen cruciaal. Het Comité formuleerde in dit kader eerder al aanbevelingen om te werken aan een geïntegreerd veiligheidsbeleid rond cyberaanvallen, hield een pleidooi voor de bevoegdheidsuitbreiding van de ADIV en de VSSE alsook voor de aanwerving van gekwalificeerde personeelsleden, beval de grootste omzichtigheid aan bij de keuze van beveiligde technische uitrustingen voor de verwerking van geclassificeerde informatie en wees op het tekort aan technische certificatie- en homologatiemiddelen op vlak van informatieveiligheid.[2]

---

1 Wat het OCAD en de ondersteunende diensten betreft, gebeuren de onderzoeken samen met het Vast Comité P (art. 53, 6° W.Toezicht).

2 VAST COMITÉ I, *Activiteitenverslag 2011*, 108-109 (IX.2.3. Aanbevelingen met betrekking tot de informatieveiligheid).

Verwijzend naar deze aanbevelingen, werden door de Senaat en de Kamer van Volksvertegenwoordigers diverse voorstellen van resolutie ingediend. Al in 2011 werd door de toenmalige leden van de parlementaire Begeleidingscommissie van het Vast Comité I een '*voorstel van resolutie tot het snel ontwikkelen van een federale strategie voor de beveiliging van informatie- en communicatiesystemen*'[3] geformuleerd, eind november 2012 gevolgd door een '*voorstel van resolutie ter beveiliging van elektronische informatie en bescherming tegen cyberaanvallen*'.[4] In diezelfde zin werd in juni 2013 in de Kamer een voorstel van resolutie ingediend '*waarbij de oprichting wordt gevraagd van een Centrum voor cyberbeveiliging in België*'.[5] De Ministerraad van 19 december 2013 keurde op zijn beurt het ontwerp van Koninklijk besluit goed voor de oprichting van het Centrum voor Cybersecurity België (CCB) dat onder het gezag van de eerste minister moet instaan voor de uitvoering van de Belgische strategie inzake *cybersecurity*.[6]

I.1.2. VERNIETIGING VAN OUDE DOSSIERS

Artikel 21 W.I&V bepaalt dat persoonsgegevens verwerkt door inlichtingendiensten slechts mogen bewaard worden '*voor een duur die niet langer mag zijn dan die welke noodzakelijk is om de doeleinden waarvoor ze opgeslagen worden, met uitzondering van de gegevens die een door het Rijksarchief erkend historisch karakter hebben*' en dat ze pas mogen worden '*vernietigd na een zekere termijn volgende op de laatste verwerking waarvan zij het voorwerp zijn geweest*'. De bewaartermijnen en de procedure met betrekking tot hun vernietiging dienen – reeds sinds de Wet van 30 november 1998! – te worden bepaald bij Koninklijk besluit, na advies van de Commissie voor de bescherming van de persoonlijke levenssfeer. Dergelijk besluit werd nog niet genomen en het Comité drong hierop aan[7]; niet alleen om uitvoering te geven aan een wettelijke verplichting, maar ook omdat het bijhouden door de inlichtingendiensten van oude gegevens een inbreuk kan betekenen op artikel 8 EVRM.

In 2012 stelde de minister van Justitie een ontwerpbesluit op dat aan het advies van de Privacy-commissie werd onderworpen. Het advies werd bekend gemaakt op 20 februari 2013.[8] Sindsdien is het Comité zonder nieuws over het ontwerpbesluit.

---

3 *Parl. St.* Senaat 2011-12, nr. 5-1246/1.

4 *Parl. St.* Senaat 2012-13, nr. 5-1855/1.

5 *Parl. St.* Kamer 2012-13, nr. 53K2918/001. In dezelfde zin: 'Resolutie van het Europees Parlement van 12 juni 2012 over de bescherming van kritieke informatie-infrastructuur – bereikte resultaten en volgende stappen: naar mondiale cyberveiligheid', *Publicatieblad van de Europese Unie*, C 332 E/22, 15 november 2013.

6 www.presscenter.org/nl/pressrelease/20131219/oprichting-van-het-centrum-voor-cybersecurity-belgie.

7 VAST COMITÉ I, *Activiteitenverslag 2008*, 22-33, i.h.b. 32 (II.2. 'Gereserveerde dossiers' bij de VSSE).

8 Commissie voor de bescherming van de persoonlijke levenssfeer, Advies nr. 07/2013 van 20 februari 2013 aangaande het voorontwerp van Koninklijk besluit tot uitvoering van arti-

I.1.3. EEN NIEUWE DIENSTNOTA VAN DE VSSE OVER DE OPVOLGING VAN PARLEMENTSLEDEN

Drie onderzoeken uit 2013 (zie II.2, II.3 en II.4) hadden aangetoond dat de meldingsplicht aan de minister van Justitie telkens wanneer een parlementslid in het vizier van de VSSE komt, in regel niet wordt nageleefd. Het Vast Comité I had voorheen al gewezen op het belang van dergelijke melding. Ze beval de bevoegde ministers aan om hun informatiebehoeften en de eventuele beperkingen tegenover de informatie-inwinning ten aanzien van politieke mandatarissen en politieke partijen in eenduidige richtlijnen om te zetten (IX.1.3). Daarenboven suggereerde het Comité dat beide inlichtingendiensten een gezamenlijk initiatief zouden nemen naar het Ministerieel Comité voor inlichting en veiligheid met het oog op de aanname van een richtlijn.

Kort na het afsluiten van bedoelde toezichtonderzoeken verspreidde de Veiligheid van de Staat – en dus niet de minister van Justitie en ook niet in overleg met de ADIV – een dienstnota '*omtrent het linken van parlementsleden en politieke mandatarissen in de documenten van de VSSE*'. Daarin werd onder meer opgenomen dat de minister van Justitie niet langer automatisch diende geïnformeerd te worden wanneer een parlementslid of minister opdook in een verslag van de Buitendiensten. De minister dient slechts te worden geïnformeerd wanneer deze politieke mandatarissen bij naam worden vermeld in de analysedocumenten. Hierdoor stroomt er minder informatie door naar de bevoegde minister.

I.1.4. DE FUNCTIE 'OPERATIONELE ANALIST' BIJ DE ALGEMENE DIENST INLICHTING EN VEILIGHEID

Naar aanleiding van de audit bij de ADIV[9] gaf het Comité aan dat '*er diende te worden bepaald welke samenwerking tussen en binnen de divisies opportuun én noodzakelijk is*'.[10] De ADIV nam deze aanbeveling ter harte en creëerde binnen de Divisie C(ounter) I(ntelligence)[11], de figuur van de 'operationele analist'. Deze vervult een brugfunctie tussen de analisten en de mensen op het terrein (collecte) en dit met het oog op een betere afstemming van de onderlinge behoeften.

---

kel 21 van de Wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst (CO-A-2012-044).

9 VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 (II.1. Een audit bij de militaire inlichtingendienst).

10 VAST COMITÉ I, *Activiteitenverslag 2011*, 105.

11 De Divisie C(ounter)I(ntelligence) werd ondertussen samengevoegd met de Divisie S(ecurity) tot de Divisie CIS.

I.2. EEN HERNEMING VAN EERDERE AANBEVELINGEN

Artikel 35, 3° W.Toezicht geeft het Vast Comité I de opdracht verslag te doen aan het Parlement '*wanneer het vaststelt dat, bij het verstrijken van een termijn die het redelijk acht, geen gevolg werd gegeven aan zijn besluiten of dat de genomen maatregelen niet passend of ontoereikend zijn*'. In dit kader herneemt het Comité jaarlijks een of meerdere aanbevelingen die het essentieel acht vanuit zijn dubbele finaliteit: de efficiënte werking van de diensten en het waarborgen van fundamentele rechten.

Het Vast Comité I blijft in dit kader met klem herhalen dat er nu dringend uitvoering moet worden gegeven aan de verplichtingen gesteld in de artikelen 19 en 20 W.I&V om de informatie-uitwisseling en de samenwerking van de Belgische inlichtingendiensten met andere (ook buitenlandse) overheden nader te regelen.[12] Al bij zijn 'Overzicht van de voornaamste aanbevelingen van het Vast Comité I (1994-2005)'[13] drong het Comité aan op een reflectie hieromtrent.[14] Het wetsontwerp waarbij de bijzondere inlichtingenmethoden (de huidige BIM-Wet) zouden worden omschreven, bood hiertoe een uitgelezen kans. De wetgever heeft evenwel van deze opportuniteit geen gebruik gemaakt. In 2007 herhaalde het Comité zijn aanbeveling.[15] Naar aanleiding van het toezichtonderzoek naar de zogenaamde 'gereserveerde dossiers', werd in 2008 nogmaals gevraagd een duidelijke regeling uit te werken voor de overzending van persoonsgegevens naar buitenlandse (inlichtingen-)diensten en werd in het bijzonder verwezen naar de Nederlandse, Duitse en Noorse regeling ter zake.[16] In 2009 stelde het Comité dat de afwezigheid van richtlijnen hieromtrent '*de informatiedoorstroming discutabel [maakt] vanuit legaliteitsoogpunt*'.[17] De twee volgende jaren 2010-2011 toonden enkele BIM-dossiers aan dat de Belgische inlichtingendiensten soms opereren op aangeven van buitenlandse diensten waarna persoonsgegevens kunnen doorgegeven worden. Het Comité vraagt aandacht voor deze delicate materie, zeker nu het Ministerieel Comité ter zake nog steeds geen richtlijn heeft uitgewerkt.[18] In de

12 Deze aanbeveling werd ook steeds onderschreven door de Begeleidingscommissies.

13 VAST COMITÉ I, *Activiteitenverslag 2006*, 4 en 132.

14 '*Ondanks het feit dat het Vast Comité I er zich van bewust is dat de (buitenlandse) inlichtingendiensten de 'regel van de derde dienst' als onwrikbaar beschouwen, heeft het Comité diverse malen aangedrongen op een reflectie over de toepassing van deze regel en de controle erop. Immers, de toepassing van de derdenregel kan leiden tot een verkeerde interpretatie gelieerd aan een zekere 'cultuur van het geheim', of zelfs, in extreme gevallen, tot een verkeerd gebruik. Verder is het Vast Comité I altijd de mening toegedaan dat de samenwerking met de buitenlandse en vooral de Europese inlichtingendiensten moest worden versterkt, maar niet zonder te voorzien in de nodige controle*' in VAST COMITÉ I, *Activiteitenverslag 2006*, 4.

15 VAST COMITÉ I, *Activiteitenverslag 2007*, 73-74.

16 VAST COMITÉ I, *Activiteitenverslag 2008*, 6, 109-110.

17 VAST COMITÉ I, *Activiteitenverslag 2009*, 4, 106-107.

18 VAST COMITÉ I, *Activiteitenverslag 2010*, 3-4 en *Activiteitenverslag 2011*, 5-6.

aanbevelingen van het *Activiteitenverslag 2012* komt de kwestie opnieuw aan bod.[19] En zo ook in voorliggend activiteitenverslag. Twee belangrijke onderzoeken (II.1 'De rol van de Algemene Dienst inlichting en veiligheid bij de opvolging van het conflict in Afghanistan' en II.10 'Tussentijdse verslagen in de onderzoeken naar aanleiding van de Snowden-onthullingen') tonen nogmaals aan dat er dringend nood is aan regelgeving ter zake.

19 VAST COMITÉ I, *Activiteitenverslag 2012*, 2 en 95.

HOOFDSTUK II
DE TOEZICHTONDERZOEKEN

In 2013 werden negen onderzoeken afgesloten. Tevens werd een tussentijds verslag afgerond naar een van de onderzoeken die volgende op de Snowden-onthullingen (zie II.10). Zes van de tien onderzoeken gebeurden op verzoek van de Begeleidingscommissie van de Senaat (waarvan één ook gedeeltelijk het resultaat van een initiatief van de minister van Justitie); vier toezichtonderzoeken werden opgestart na een klacht of een aangifte. In wat volgt, worden de negen eindverslagen (II.1 tot II.9) en het tussentijdse verslag toegelicht (II.10). Daarna volgt een opsomming en een korte situering van de nog lopende onderzoeken (II.11).

Onder deze laatste rubriek staan ook de tien in 2013 geopende toezichtonderzoeken vermeld. Drie van die onderzoeken gebeuren gezamenlijk met het Vast Comité P. Van de tien nieuwe onderzoeken werden er vier opgestart op verzoek van de Senaat, vijf naar aanleiding van een klacht en één op gemeenschappelijk initiatief van de Vaste Comités I en P.

In totaal ontving het Comité in 2013 28 klachten of aangiften. Na verificatie van een aantal objectieve gegevens wees het Comité 22 van deze klachten of aangiften af omdat ze kennelijk niet gegrond waren (art. 34 W.Toezicht) of omdat het Comité zich onbevoegd wist voor de opgeworpen vraag. In die laatste gevallen werden de klagers zo mogelijk doorverwezen naar de bevoegde instantie. In enkele gevallen werden daarenboven de politionele of gerechtelijke overheden in kennis gesteld omwille van een potentieel risico. Zoals gezegd, gaven vijf klachten uit 2013 aanleiding tot het openen van een toezichtonderzoek. Eén klacht, die op het einde van het jaar werd ingediend, gaf pas begin 2014 aanleiding tot de opening van een onderzoek. Daarom blijft ze hier verder onvermeld.

II.1. DE ROL VAN DE ALGEMENE DIENST INLICHTING EN VEILIGHEID BIJ DE OPVOLGING VAN HET CONFLICT IN AFGHANISTAN

In december 2001 besliste België deel te nemen aan de 'International Security Assistance Force' (ISAF), een internationale macht voor het behoud van de vrede

in Afghanistan, die werd opgezet binnen de Verenigde Naties. Naast de NAVO (en zijn lidstaten), participeerden hieraan een twintigtal andere landen.

Het overgrote deel van het Belgische contingent was gestationeerd in Kaboel en stond in voor de bescherming van de internationale luchthaven. In de provincie Kunduz, in het noorden van het land, ondersteunden de Belgen ploegen die instonden voor de heropbouw van het land en verleenden zij technisch advies aan het Afghaanse leger. Ten slotte opereerden sinds 2008 een aantal Belgische gevechtsvliegtuigen vanuit Kandahar.

Om zich een globaal beeld te kunnen vormen van de wijze waarop de militaire inlichtingendienst werd betrokken bij deze operatie, besliste het Comité in januari 2010 een toezichtonderzoek te openen '*betreffende de rol van de ADIV in de opvolging van de situatie in Afghanistan*'.[20] Het Vast Comité I had met dit toezichtonderzoek een duidelijke finaliteit voor ogen: één van de belangrijkste opdrachten van de ADIV zo volledig mogelijk[21] in kaart brengen om op die wijze een referentiekader op te stellen voor latere missies alsook voor toezichtonderzoeken die daaromtrent kunnen worden ingesteld.

Uiteraard kon in deze niet voorbij worden gegaan aan de conclusies van de parlementaire onderzoekscommissie Rwanda[22], ingesteld in 1997 ten gevolge de tragische dood van tien Belgische para-commando's. Over het verzamelen en analyseren van inlichtingen oordeelde deze commissie onder meer het volgende:

- Het Belgische contingent moet steeds beschikken over een eigen, solied inlichtingennetwerk, bestaande uit inlichtingenofficieren die voldoende gevormd zijn en die, in de mate van het mogelijke, de taal beheersen van het land. Op zijn minst moet men beschikken over betrouwbare tolken.
- Om de inlichtingen te analyseren, moet de militaire inlichtingendienst beschikken over voldoende analisten die de inhoud van de informatie kunnen beoordelen. Bovendien moet er een systematische *feedback* worden gegeven aan de eenheden op het terrein.
- Het is noodzakelijk de militaire inlichtingendienst te hervormen, onder andere rekening houdend met de Wet van 30 november 1998 op de inlichtin-

---

20 Het Vast Comité I kon in het kader van dit onderzoek, waarvan een zeer omstandig "GEHEIM – Wet 11-12-1998" geclassificeerd eindrapport werd bezorgd aan de minister van Defensie in september 2013, rekenen op de grote openheid van de chef en de betrokken leden van de ADIV. Ook de onberispelijke organisatie van de plaatsbezoeken in Afghanistan verdient vermelding. Het verslag werd in zijn versie 'BEPERKTE VERSPREIDING' besproken op de vergadering van de Begeleidingscommissie van de Senaat van 12 maart 2014. Tijdens die vergadering en nadien (bij brief van 16 juni 2014) wenste de ADIV en de minister van Defensie enkele verduidelijkingen en nuanceringen toe te voegen aan het rapport. In voorliggend verslag is met die opmerkingen rekening gehouden.

21 Alleen het verzamelen van SIGINT in Afghanistan werd niet belicht. Dit aspect werd opgenomen in een later toezichtonderzoek (zie II.10.12. Vier toezichtonderzoeken in het kader van de Snowden-onthullingen).

22 *Parl. St.* Senaat 1997-1998, nr. 1-611/7.

gen- en veiligheidsdiensten. De dienst moet, voor alles, een efficiënt en coherent instrument worden ter ondersteuning van de verantwoordelijken van de operaties. Het is nodig dat de analysecapaciteit ter beschikking wordt gesteld van de verantwoordelijken ten einde hen toe te laten de politieke opties te bepalen. Er moet worden over gewaakt dat de informatiebronnen voldoende divers van aard zijn en dat de analyse tegensprekelijk gebeurt. Dit houdt in dat er voortdurend informatie dient uitgewisseld te worden tussen de inlichtingendienst enerzijds en de verantwoordelijken op het terrein anderzijds.

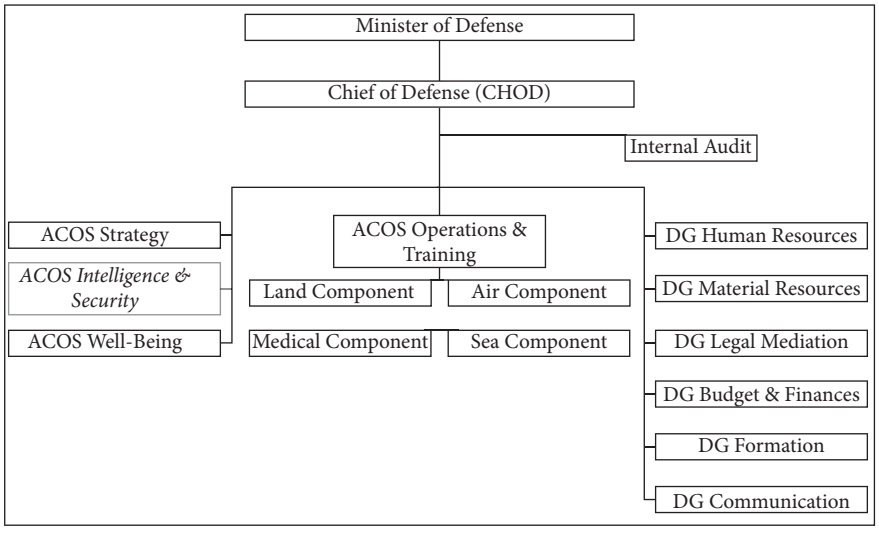
– De militaire inlichtingendienst moet zijn eenheden op het terrein op inlichtingenvlak versterken, in het bijzonder door het ter beschikking stellen van gespecialiseerd personeel of via technische middelen.

II.1.1. DE PLAATS, DE STRUCTUUR EN DE BEVOEGDHEDEN VAN DE ADIV

II.1.1.1. Plaats en structuur van de ADIV

Voor een goed begrip is van belang te weten hoe de ADIV gestructureerd is en waar de dienst zich situeert binnen de Krijgsmacht (waarin overigens nog andere componenten belast zijn met inlichtingengaring).

Structuur van de Belgische Krijgsmacht



De Algemene Dienst inlichting en veiligheid, ook de *Assistant Chief of Staff Intelligence and Security* (ACOS-IS)[23] genoemd, is één van de stafdepartementen van de Krijgsmacht.[24] De dienst was op het moment van het onderzoek opgebouwd uit vier divisies.[25]

De Divisie S(ecurity) voert veiligheidsonderzoeken uit ten aanzien van bepaalde personen of firma's en waakt over de naleving van de richtlijnen met betrekking tot de militaire veiligheid van domeinen, personen, ICT-systemen …

De Divisie A(ppui) staat onder meer in voor personeelsbeheer, budgettair beheer, ICT en logistieke aspecten die binnen de ADIV zelf worden beheerd.

De Divisie C(ounter)I(ntelligence) volgt op Belgisch grondgebied bedreigingen op tegen de militaire veiligheid of tegen andere belangen die de ADIV moet verdedigen. Deze divisie heeft echter ook een rol te vervullen bij de *force-protection* van Belgische eenheden in het buitenland: ze verleent deze eenheden steun om specifieke bedreigingen (bijvoorbeeld infiltratie door lokale groeperingen), tegen te gaan.

De Divisie I(intelligence) ten slotte vormt het grootste onderdeel van de ADIV. Ze richt zich op fenomenen die zich in het buitenland voordoen en is dan ook werkzaam op plaatsen waar Belgische troepen worden ingezet. De analysediensten van de Divisie I zijn grotendeels per regio georganiseerd, terwijl er ook bureaus voor *Naval-* en *Land-Intelligence* en transnationale aangelegenheden bestaan. Inzake collecte (gegevensverzameling) zijn binnen deze Divisie verschillende diensten actief: *Human Intelligence* (HUMINT), *Image Intelligence* (IMINT), *Signals Intelligence* (SIGINT of COMINT) en *Open Sources Intelligence* (OSINT). De opdracht om ter plaatse inlichtingen te verzamelen berust bij de Afdeling I/Ops. De onderdelen van I/Ops die in het buitenland worden ontplooid, worden aangeduid onder de benaming BENIC (*Belgian National Intelligence Cell*) of BELINT (*Belgian Intelligence*).

II.1.1.2. De opdrachten van de ADIV

De vier opdrachten van de ADIV staan omschreven in artikel 11 W.I&V: de klassieke inlichtingentaak, het zorgen voor het behoud van de militaire veiligheid, het beschermen van militaire geheimen en het uitvoeren van veiligheidsonderzoeken. Elk van deze taken kan een link hebben met buitenlandse operaties. Zo bij-

---

23 Aangezien de meeste instructies en permanente orders van deze dienst in het Engels zijn gesteld, neemt het Comité de aldus gebruikte militaire terminologie over.

24 De W.Toezicht en de W.I&V hanteren de term 'Algemene Dienst inlichting en veiligheid van de Krijgsmacht' (ADIV), het Koninklijk besluit 21 december 2001 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten (KB Defensie) spreekt dan weer van het Stafdepartement Inlichtingen en Veiligheid of *Assistant Chief of Staf Intelligence and Security* (ACOS-IS). Het betreft eenzelfde dienst.

25 In 2013 werden de Divisies S(ecurity) en C(ounter) (I)ntelligence samengevoegd.

voorbeeld heeft de ADIV als opdracht het inwinnen, analyseren en verwerken van inlichtingen (met andere woorden: zijn inlichtingentaak) die betrekking hebben op elke activiteit die de vervulling van de '*opdrachten, acties of operaties in nationaal verband, in het kader van een bondgenootschap of een internationaal of supranationaal samenwerkingsverband*' van de '*Belgische Krijgsmacht, van de geallieerde strijdkrachten of van intergeallieerde defensieorganisaties*' bedreigt of zou kunnen bedreigen. Ook mag informatie worden ingewonnen over collectieve dreigingen tegen '*het leven of de lichamelijke integriteit van Belgen in het buitenland en van hun familieleden*'. Ook de tweede opdracht – het zorgen voor het behoud van de militaire veiligheid[26] van bijvoorbeeld '*het personeel dat onder de Minister van Landsverdediging ressorteert*' en '*de militaire installaties, wapens, munitie, uitrusting, plannen, geschriften, documenten, informatica- en verbindingssystemen of andere militaire voorwerpen*' – is van belang bij buitenlandse operaties.

II.1.1.3. De bevoegdheden van de ADIV en het territorialiteitsbeginsel

Artikel 11 W.I&V laat er geen twijfel over bestaan dat de ADIV informatie kan inzamelen *over* het buitenland. Maar kan de dienst ook informatie inzamelen *in* het buitenland? Nergens wordt uitdrukkelijk gesteld dat de ADIV in het buitenland kan optreden. Dit volgt evenwel logisch uit de omschrijving van een aantal opdrachten (bijvoorbeeld de veiligheid van operaties in het kader van een bondgenootschap en de veiligheid van Belgische onderdanen in het buitenland) die onmogelijk uitsluitend vanuit België kunnen waargenomen worden. Hetzelfde geldt voor de andere opdrachten. Zo wordt bijvoorbeeld wat betreft de 'beschermingstaak' geen onderscheid gemaakt al naargelang het personeel of materieel zich in het binnen- dan wel in het buitenland bevinden.

Maar dat de ADIV in het buitenland kan optreden, betekent nog niet dat alle inlichtingenmethoden kunnen aangewend worden. Zo is het aanwenden van specifieke of uitzonderlijke inlichtingenmethoden bij artikel 18/1, 2° W.I&V alleen toegelaten binnen het Belgische grondgebied. Het inzetten van deze methoden in het kader van een onderzoek naar een mogelijke bedreiging voor een buitenlandse missie, is dus wel mogelijk als dit gebeurt op het Belgische grondgebied.

De ADIV was van mening dat de BIM-methoden wél in het buitenland mogen worden ingezet. Het Comité is van oordeel dat dergelijke interpretatie indruist tegen de wet. Wel bestaat de mogelijkheid om in het buitenland uitgezonden communicaties te onderscheppen, bijvoorbeeld om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerde partners tijdens de opdrachten in het buitenland. Hiervoor beschikt de ADIV immers over een specifiek wettelijk mandaat (art. 259*bis* § 5 Sw. *juncto* art. 11 § 2, 3° W.I&V.) dat ont-

[26] Deze opdracht beperkt zich tot het opstellen van richtlijnen én het garanderen van de naleving ervan, bijvoorbeeld door het uitvoeren van controles ter plaatse.

breekt voor de andere methoden. Onder meer met het oog op de naleving van mensenrechten en de operationele behoeften op het terrein, onderschreef de minister van Defensie de idee om aan deze problematiek specifiek aandacht te besteden in het kader van de evaluatie van de BIM-Wet.

II.1.1.4. De mededeling van inlichtingen aan derde landen

Een specifiek probleem vormt de mededeling van inlichtingen aan derde landen en het gebruik dat die daarvan mogelijks maken. Ingevolge de artikelen 19 en 20 W.I&V mag/moet de ADIV samenwerken en informatie uitwisselen met buitenlandse diensten. De vraag daarbij is of een dergelijke situatie tot de juridische verantwoordelijkheid van de dienst kan leiden.[27] Het Engelse *High Court of Justice* moest zich reeds uitspreken over de eis van een Pakistaans staatsburger. De Pakistaan hield voor dat de leden van het Britse GCHQ zich schuldig hadden gemaakt aan misdaden (medeplichtigheid aan moord) door het leveren van SIGINT die de NSA en de CIA vervolgens zouden gebruikt hebben bij het uitvoeren van *drone*-aanvallen waarbij zijn vader was omgekomen. De *High Court of Justice* wees de vordering af omdat het lid van de inlichtingendienst *in casu* niet in staat was om te bepalen welke inlichtingen hij eventueel wel of niet zou mogen doorspelen aan de verantwoordelijken op het terrein.[28]

II.1.1.5. Enkele andere actoren op het vlak van inlichtingengaring

ADIV is lang niet de enige entiteit binnen de Belgische Krijgsmacht die inlichtingen verzamelt en in het buitenland actief kan zijn.

Zo zijn er binnen de Land-, Zee- en Luchtcomponent[29] van het Stafdepartement *Operations and Training* (ACOS-Ops & Trg) diensten die bij de operaties en de voorbereiding ervan via allerlei bronnen (bijvoorbeeld via de ADIV of bevelhebbers op het terrein) inlichtingen inwinnen en verwerken. Hoe die diensten met elkaar moeten samenwerken, werd op het moment van het onderzoek omschreven in de *Standing Operating Procedure* (SOP) *Joint Intelligence, Counter-Intelligence and Security Structure* van 2008[30], die uitging van ACOS-Ops & Trg. Deze SOP beschreef onder meer de positie van ADIV in het geheel van de 'inlichtingenstructuur' van Defensie. Zo werd bepaald dat de ADIV richtlijnen ontvangt van de minister van Landsverdediging en van de *Chief of Defense* (CHOD), zich

---

27 Zie hierover verder voetnoot 35 met betrekking tot de uiteenzetting van de ADIV in de Senaat.

28 High Court of Justice, Queens Bench division, Administrative Court, *R – Noor Khan v Foreign Secretary* – 2012.

29 Zo bijvoorbeeld was er in Afghanistan een divisie van Air-Intel actief die gespecialiseerd is in de analyse van de operationele luchtbedreigingen.

30 Deze *Standing Operating Procedure* (SOP) werd vervangen door de SOP '*The Belgian Joint Intelligence and Security Structure*' van november 2013 (eveneens van ACOS-Ops & Trg).

moet richten op politiek-strategische en operationele inlichtingen en indien nodig een inlichtingencel in het buitenland kan ontplooien.

Verder is er in elk operationeel onderdeel van de Krijgsmacht een dusgenaamde 'S2-functie' die wordt uitgeoefend door de officier die de *Commanding Officer* bijstaat om inlichtingen te verschaffen over de situatie op het terrein. Hij levert vooral tactische informatie aan.[31]

Tijdens operaties wordt de *Commanding Officer* bijgestaan door een *Battle Group Intelligence Cell* (BIC). Sinds 2011 werd ook een verkenningsbataljon 'Intelligence, Surveillance, Target Acquistion and Reconnaissance' (ISTAR) opgericht. Dit bataljon zal missies uitvoeren met het oog op het voorbereiden van acties op het terrein en in dit kader vooral tactische informatie verzamelen.[32]

Ten slotte is er ook nog de '*Information Operations Group*' van de Landmacht waaronder de zogenaamde '*Psyops*' en de '*Human Factor Analysis*' ressorteren. *Psyops* richt zich op het verzorgen van de communicatie met de lokale bevolking en autoriteiten op plaatsen waar de Belgische troepen ontplooid zijn. De dienst moet ook reageren op eventuele anti-Belgische propaganda. De *Human Factor Analysis* bestudeert diverse menselijke factoren die een opdracht kunnen beïnvloeden, zoals *antropology* en *human geography*.

II.1.2. DE PLAATS EN DE BEVOEGDHEDEN VAN DE ADIV BINNEN DE ISAF

II.1.2.1. De ISAF-operatie

Drie dagen na de aanslagen van 9/11 nam het Amerikaanse Congres een resolutie aan waarbij het gebruik van gewapend geweld werd toegestaan tegen de verantwoordelijken voor de aanslag én tegen diegenen die aan deze laatsten een toevluchtsoord zouden hebben geboden. Op 15 september 2001 kwam de Noord-Atlantische Raad van de NATO bijeen en verklaarde op vraag van de Verenigde Staten artikel 5 van het Noord-Atlantisch Verdrag toepasselijk: het betreft het recht op bijstand van de NAVO-lidstaten aan die lidstaat die het slachtoffer werd van een gewapende aanval.[33]

Op 20 september 2011 duidden de Verenigde Staten Osama Bin Laden en zijn organisatie Al Qaida aan als verantwoordelijke voor de aanvallen van 9/11. Bin Laden verbleef op dat ogenblik in Afghanistan, waar het Taliban-regime hem de hand boven het hoofd hield en weigerde hem uit te leveren.

---

31 Tijdens de parlementaire voorbereiding van de W.I&V werd reeds een onderscheid gemaakt tussen strategische of geopolitieke inlichtingen enerzijds en de tactische inlichtingen die verband houden met de concrete werkelijkheid van het terrein en met de ontplooiing van een eenheid anderzijds (*Parl. St. Kamer* 1996-1997, 49-638 /14, 22-24 en 38).

32 Zie ook Hoofdstuk V.2.

33 Sinds het ontstaan van de NAVO is dit de enige maal dat dit artikel werd toegepast.

Vanaf oktober 2001 kwamen Amerikaanse, Britse, Franse en Australische troepen in Afghanistan in actie samen met lokale verzetsgroepen en vormden er de zogenaamde 'Noordelijke alliantie'. Deze operatie werd *Operation Enduring Freedom* (OEF) genoemd.

België – en dus ook ADIV – opereert niet binnen dit kader.[34] De activiteiten van de Belgische Krijgsmacht zijn te kaderen binnen een UNO-mandaat. Dat mandaat vond zijn oorsprong in het 'Akkoord van Bonn' van 5 november 2001 waarin de oprichting van een '*International Security Assitance Force* (ISAF)' in het vooruitzicht werd gesteld. De Afghaanse ondertekenaars van het akkoord verzochten de Veiligheidsraad van de Verenigde Naties met name '*to consider authorizing the early deployment to Afghanistan of a United Nations mandated force. This force will assist in the maintenance of security for Kabul and its surroundings. Such a force could, as appropriate, be progressively expanded to other urban centres and other areas*'.

Hieraan gevolg gevend, nam de VN-Veiligheidsraad op 20 december 2001 Resolutie 1386(2001) aan. Deze resolutie gaf het mandaat voor de ontplooiing van een ISAF '*to assist the Afghan Interim Authority in the maintenance of security for Kabul and its surrounding areas, so that the Afghan Interim Authority as well as the personnel of the United Nations can operate in a secure environment*'.

Reeds op 21 december 2001 besliste de Belgische Regering om aan deze missie deel te nemen. Eind januari 2002 werd een eerste transportvliegtuig ingezet, terwijl de inzet van troepen op het terrein ongeveer een jaar later gebeurde.

In eerste instantie viel de ISAF-missie onder een om de zes maanden wisselend commando. Sinds maart 2003 nam de NAVO het commando van ISAF over. Naast NAVO-leden zijn nog een twintigtal andere troepenmachten aanwezig.

Het is van belang te onderlijnen dat de ISAF-troepenmacht tot doel heeft de veiligheid van de bevolking te garanderen en de legitieme Afghaanse autoriteiten te ondersteunen zodat deze, samen met de UNO-autoriteiten, hun burgerlijke taken kunnen uitvoeren. Vanuit militair standpunt betekent dit dat de ISAF-troepen het terrein moeten beveiligen door de militaire krachten van de tegenstrevers te counteren en te verzwakken zodat deze niet langer in staat zouden zijn het land te destabiliseren. Niettemin vormt deze militaire taak niet de essentie van de ISAF-missie. Die missie is hoofdzakelijk gericht op wat heet *counter insurgency*. Daarbij wordt gepoogd de (al dan niet passieve) steun die de opstandelingen bij de bevolking genieten, te verminderen en op termijn te doen verdwijnen. Het is immers deze voedingsbodem die de opstandelingen toelaat hun verzet voort te zetten. De operatie is dus eigenlijk een strijd om de '*minds and hearts*' van de bevolking. De militaire inzet kan deze taak slechts faciliteren door een veiligheidssituatie te scheppen waarin de burgerlijke autoriteiten hun taak kunnen uitvoeren.

---

[34] België nam enkel in de vorm van steunoperaties deel aan *Operation Enduring Freedom* en dit buiten het Afghaanse grondgebied (onder meer door de inzet van C-130 transportvliegtuigen voor humanitaire hulp, het stationeren van een fregat in de Middellandse Zee en het leveren van bemanning voor de AWACS-toestellen boven de Verenigde Staten).

ISAF is niet alleen geen zuiver militaire operatie, het is – anders dan de *Operation Enduring Freedom* – ook geen strijd tegen terreur. In dit verband moet verwezen worden naar het *CHOD OPORDER for Bel contribution to ISAF* (zie verder onder II.1.3.3.4) die stelt dat de Belgische troepen niet aan *Counter Terrorist*-operaties zullen deelnemen. Op het vlak van de inlichtingendoorstroming is het evenwel niet uitgesloten dat inlichtingen die in het kader van de ISAF-operatie met de leden van deze coalitie gedeeld worden, via de bondgenoten die ook deel uitmaken van de *US-led coalition*, een weg vinden naar de OEF, ook al is dat laatste niet de bedoeling.[35] De nauwe verwevenheid op het terrein tussen beide missies blijkt bijvoorbeeld ook uit het feit dat het commando van ISAF en dat van de *US-forces* in Afghanistan (USFOR-A) samenvallen.

II.1.2.2. De Belgische aanwezigheid in Afghanistan met aandacht voor de ADIV

Tot 30 september 2012 stond het overgrote deel van het Belgische contingent (320 personen) in voor de bescherming van de internationale luchthaven van Kaboel (KAIA). België vervulde eveneens een rol binnen de generale staf van de ISAF in Kaboel en stationeerde een nationale steuneenheid in de Kaboul International Airport. Wat betreft Kunduz, stuurde België ongeveer 25 militairen als steun aan de provinciale wederopbouwteams (*provincial reconstruction teams*, PRT) die als opdracht hadden de omgeving te beveiligen, wederopbouwprojecten te coördineren en steun te bieden op het vlak van gezondheid, onderwijs en NGO's.

Anderzijds leverde België in het noorden van Afghanistan een *Military Assistance Team* (MAT) van ongeveer 60 militairen die als opdracht hadden technisch advies te leveren aan de generale staf van een brigade en een bataljon van het Afghaanse nationale leger.

Verder waren er Belgische F-16 gevechtsvliegtuigen op de basis in Kandahar en nam België vanaf 2008 deel aan de Operatie Guardian Falcon en leidde zij Afghaanse piloten en medisch personeel in Kandahar op.

Ten slotte waren ook een aantal militairen ontplooid in Mazar-E-Sharif.

Wat de ADIV betreft namen zowel de Divisies I, CI als S deel aan de opdrachten in Afghanistan. Uiteraard wisselde de samenstelling en getalsterkte van de personeelsleden van de ADIV in functie van de noden en beschikbaarheden. De opvolging van de strategische situatie werd uitgeoefend door personen die zijn ondergebracht in wat heet de *Belgian National Intelligence Cell* (BENIC). Daarnaast ontplooide de ADIV ook personeelsleden die bijvoorbeeld instonden voor

---

35 Voor de parlementaire Commissie Buitenlandse operaties van 19 april 2012 stelde de ADIV mondeling het volgende: *'En conclusion, nous sommes en mesure de certifier qu'en aucun cas les informations collectées, ni les analyses fournies aux unités ou aux partenaires ont un objectif de 'targeting'. Tous nos produits servent uniquement à des fins de protection, de prévention et de contextualisation du processus de décision. Mais nous ne pouvons pas nier que dans la communauté dite des Four Eyes (UK/US) ou des Five Eyes (US/UK/CAN/NZ/AUS) d'autres pratiques sont d'application'.*

de uitwisseling van inlichtingen tussen de ter plaatse ontplooide Belgische eenheden en de buitenlandse militaire bondgenoten en die informatie doorspeelden naar de *Battle Group Intelligence Cell* (BIC), de S2 en eventuele andere partners. Ook werden op punctuele basis soms analisten van de Divisie I naar Afghanistan gezonden. Het Comité stelde vast dat hun opdrachten niet steeds even duidelijk waren omschreven. De Divisie CI was aanwezig onder meer om eventuele veiligheidsproblemen voor de Belgische eenheden te detecteren, om het lokale personeel dat voor de Belgische eenheden werkt op te volgen[36] en om de graad van waardering die de Belgen genieten bij onder meer de Afghanen die met de ISAF samenwerken, te beoordelen. ADIV-S ten slotte zond een team indien een veiligheidsaudit werd aangevraagd. Desgevallend controleert dit team de uitvoering van de veiligheidsregels met betrekking tot het personeel, het materieel en de infrastructuur.

De situatie in Afghanistan werd door de ADIV uiteraard niet alleen ter plaatste opgevolgd. In Brussel is een 'bureau Afghanistan' gevestigd dat bemand wordt door analisten. Zij beantwoorden *Requests for Information* (RFI) komende vanuit ACOS-IS, de NAVO, de EU en zogenaamde 'bevriende diensten' en analyseren de informatie afkomstig van de verschillende collecte-organen (HUMINT, IMINT, SIGINT …). Het bureau verzorgt tevens de briefings voor de generale staf, voor de eenheden die zijn opgeroepen om ontplooid te worden op het terrein, voor de BENIC, alsook voor externe partners (bijvoorbeeld ambassadeurs).

Het overgrote deel van de RFI's die de analisten ontvangen, betreffen vragen van operationele of tactische aard (meestal komende van ACOS-Ops & Trg); strategische vragen vormen slechts een minderheid.

Het Comité moest vaststellen dat de analisten van het 'bureau Afghanistan' niet steeds precies wisten welk soort inlichtingen hun partners uit de inlichtingen- en militaire wereld verwachtten. Omgekeerd zijn de vragen die deze laatsten stellen vaak weinig gespecificeerd aangezien zij niet weten wat de ADIV precies kan aanleveren. De aanwezigheid van analisten op het terrein bleek belangrijk om de vraag en het aanbod beter op elkaar af te stemmen.

II.1.3. NORMEREND KADER VAN TOEPASSING OP DE ADIV IN AFGHANISTAN

II.1.3.1. Het nationale kader

Uiteraard dient in eerste instantie te worden verwezen naar artikel 11 W.I&V dat een algemene omschrijving geeft van de vier opdrachten van de ADIV (zie hoger II.1.1.2). Wat betreft de klassieke inlichtingenopdracht, moet benadrukt worden

[36] De screening van dit *'Local Employed Personnel'* wordt uitgevoerd door het bureau 'vetting' van de NAVO.

dat de wet zelf geen onderscheid maakt tussen (politiek-)strategische, operationele of tactische inlichtingen.[37] Alhoewel uit de voorbereidende werken van de wet blijkt dat het inwinnen van puur tactische informatie niet echt als opdracht van de ADIV werd gezien (zie hoger II.1.1.5), is de dienst op de drie inlichtingenterreinen bedrijvig. Inzake het opsporen van de activiteiten die een bedreiging kunnen vormen voor de vervulling van de opdrachten van de strijdkrachten, kunnen immers alle vormen van inlichtingen van belang zijn.

Verder bepaalt artikel 23 van het Koninklijk besluit van 21 december 2001 tot bepaling van de algemene structuur van het ministerie van Landsverdediging en tot vastlegging van de bevoegdheden van bepaalde autoriteiten, dat de onderstafchef inlichtingen en veiligheid (ACOS-IS), onder meer belast is met '*de organisatie van de steun inlichtingen en veiligheid aan operaties*'.

In uitvoering van de W.I&V zou het Ministerieel Comité voor inlichting en veiligheid (MCIV) bijkomende richtlijnen kunnen uitvaardigen over de werking van de militaire inlichtingendienst ingeval van buitenlandse operaties. Hiervan werd nog geen gebruik gemaakt. Ook heeft het Ministerieel Comité tot op heden geen richtlijnen uitgewerkt over de uitwisseling van inlichtingen met buitenlandse diensten. Het Vast Comité I heeft reeds meermaals op deze lacune gewezen.[38]

De prioriteiten van de ADIV staan omschreven in het Inlichtingenstuurplan (van de divisie I) en het Veiligheidsinlichtingenstuurplan (van de divisie CI). Sinds 2001 verdient Afghanistan volgens de inlichtingenstuurplannen een permanente en intensieve analyse, gebaseerd op een continue en doorgedreven opsporing van informatie door de collecte-organen. Voordien was dit niet het geval. Dezelfde evolutie zien we in de Veiligheidsinlichtingenstuurplannen.

Daarenboven is het *CHOD Operations Order for Bel contribution to ISAF* (2012) van belang. Deze richtlijn beschrijft de bijdrage van de ADIV in het kader van de militaire interventie in Afghanistan in algemene termen: de dienst komt vanuit inlichtingenstandpunt tussen bij de voorbereiding en de uitvoering van de buitenlandse operatie. De richtlijn bepaalt ook dat de Belgische inlichtingencapaciteit (BELINT) onder eigen nationaal commando blijft. De taken van de BELINT strekken zich zowel uit tot de strategische als tot de operationele en tactische inlichtingenvergaring en of –verspreiding.

Verder werden door de ADIV zelf richtlijnen uitgevaardigd die meer praktische details bevatten over alle organisatorische en operationele aspecten die van

---

37 Strategische inlichtingen zijn bestemd ter ondersteuning van de politiek-militaire besluitvormers. Operationele inlichtingen daarentegen zijn inlichtingen die nuttig zijn voor het voorbereiden en uitvoeren van campagnes op het terrein (bijvoorbeeld: Wat is de troepensterkte van de tegenstander in een regio en wat is de toestand van het terrein?). Tactische inlichtingen ten slotte zijn zeer concrete inlichtingen die slaan op zeer specifieke situaties die onmiddellijk dienstig zijn voor de personen op het terrein.

38 Zie VAST COMITÉ I, *Activiteitenverslag 2006*, 132; *Activiteitenverslag 2007*, 73, *Activiteitenverslag 2008*, 6 en 109-110; *Activiteitenverslag 2009*, 4 en 106-107; *Activiteitenverslag 2010*, 3-4 en *Activiteitenverslag 2012*, 95.

belang zijn bij het inzetten van personeel in het buitenland en waarbij meer in detail wordt ingegaan op de opdracht inzake '*force protection*'.

Ten slotte zijn er nog een aantal zogenaamde *Fragmentary Orders* (FragO) die betrekking hebben op specifieke zendingen, bijvoorbeeld van een welbepaald team binnen een bepaalde periode. Een FragO vormt in feite een verbijzondering van een algemeen *Operations Order* voor een specifieke opdracht.

II.1.3.2. Het internationale kader

Op internationaal vlak moet vooral rekening worden gehouden met het *SACEUR Operational Plan for ISAF*, dat een kader biedt voor de inlichtingendiensten van de naties die aan de ISAF operaties meewerken.[39] Als principe geldt hier dat de ADIV-componenten ter plaatse niet onder ISAF/NATO commando staat, en dit in tegenstelling tot de operationele Belgische eenheden. BELINT kan dus geen specifieke instructies krijgen om bepaalde handelingen te verrichten. Vanzelfsprekend belet dit niet dat de BELINT met de ISAF-instanties samenwerken (bijvoorbeeld onder de vorm van informatie-uitwisseling). Wel integendeel. Zo gaat het *SACEUR Operational Plan for ISAF* er van uit dat de aan de operatie deelnemende landen bereid zijn om vanwege ISAF '*Requests for Information*' te krijgen en uit te voeren. Verder zal BELINT zich ook zoveel als mogelijk inschrijven in de prioriteitenbepaling van ISAF zodat zijn inlichtingengaring bijdraagt tot de inlichtingendoelstellingen die door het *Operational Plan* werden bepaald.

II.1.3.3. Enkele verbeterpunten[40]

II.1.3.3.1. Geïntegreerde normen, een gemeenschappelijk begrippenkader en precieze inlichtingendoelen

Het Vast Comité I is van oordeel dat er in bovenstaande documenten en normen meer aandacht kon worden besteed aan onderlinge afstemming, ook al zijn ze

---

[39] Er zijn ook een aantal interne NAVO-regels van toepassing, enerzijds omdat België lid is van de NATO en anderzijds omdat ISAF opereert onder NATO-commando. Zo is er bijvoorbeeld de *NATO Human Intelligence (HUMINT) Policy IMSTAM(INT)–0157-2011(SD1)* die het algemene NATO-beleid inzake HUMINT bevat. In het document, dat niet specifiek voor de ISAF-operatie bedoeld is, wordt onder andere ingegaan op de noodzaak tot informatie-uitwisseling door de diverse Lidstaten en de '*interoperability*' van de systemen die daarvoor worden gebruikt. Verder kan verwezen worden naar de *NATO STANAG 2578 – Allied Intelligence Publication – AIntP-5 – Doctrine for Human Intelligence Procedures*. Deze richtlijn beschrijft onder andere de voorwaarden waaraan een HUMINT-operator moet voldoen en geeft aan hoe gegevens best worden verzameld en hoe een rapport wordt opgemaakt. Ook de HUMINT-organisatie en -structuur komen aan bod. Deze instructie is bedoeld om een eenvormige aanpak tussen de diverse Lidstaten tot stand te brengen en een bepaald kwaliteitsniveau te waarborgen.

[40] In de loop van het onderzoek anticipeerde de ADIV al op een aantal geformuleerde bemerkingen en voerde de dienst een aantal wijzigingen door.

niet met elkaar in tegenspraak. Zo is er tussen de internationale normen en de normen op Belgisch niveau weinig of geen integratie. Het gaat weliswaar om verschillende bevoegdheidsniveaus die van elkaar onafhankelijk zijn, maar voor de personen op het terrein biedt dit geen houvast.

Het Comité is ook van oordeel dat het op niveau van de Belgische normen mogelijk moet zijn een soort gemeenschappelijk begrippenkader te hanteren waarin alle opdrachten en taken van de militaire inlichtingendienst zouden kunnen worden gesitueerd. Dit begrippenkader zou moeten vertrekken vanuit de door de W.I&V omschreven bedreigingen. Daarop voortbouwend, zou een omschrijving moeten volgen van wat dit voor de ADIV, de bureaus én elk van de personeelsleden precies betekent. Met andere woorden: er moet gestreefd worden naar de vertaling van de taakstelling in informatiebehoeften en in te zetten middelen zodat alle medewerkers de precieze inlichtingendoelen kennen.[41] Deze vaststelling geldt zowel voorafgaand aan een operatie, als tijdens de uitvoering ervan.

Zo werd over de precieze rol van de ADIV bij de voorbereiding van de internationale interventie tot voor kort weinig of niets bepaald. Dit vertaalde zich bijvoorbeeld in het feit dat na de beslissing van de Regering in 2002 om aan de internationale interventie in Afghanistan deel te nemen, de 'inlichtingeninspanning' ten aanzien van de situatie in Afghanistan zeer beperkt bleef.

II.1.3.3.2. Gedocumenteerde methodologie bij de voorbereiding van een missie

Het Comité moest vaststellen dat er voorafgaand aan de missie geen gedocumenteerde methodologie werd gehanteerd. Dit is vandaag anders. Sinds een tweetal jaar hanteert ACOS-Ops & Trg de C*omprehensive Preparation of the Operational Environnement*-methode (CPOE) bij de voorbereiding van missies. Wat betreft de inlichtingenfunctie, blijkt er voor de ADIV een belangrijke, maar geen exclusieve, rol weggelegd. Het Comité is van mening dat het (verder) uitwerken en volgen van een dergelijke doctrine of methodologie moet gepromoot worden.

II.1.3.3.3. Gedocumenteerde methodologie tijdens de uitvoering van een missie

Ook tijdens de uitvoering van de operatie van Afghanistan waren de precieze informatie- en inlichtingendoelen van de ADIV niet altijd goed afgebakend. Idealiter zouden de informatie- en inlichtingenbehoeften en de in te zetten middelen moeten worden bepaald, vertrekkend vanuit de doelstellingen en bedreigingen uit de W.I&V.

---

41 Ook in de audit van de ADIV van 2011 werd het ontbreken van dergelijke gestructureerde aanpak vastgesteld (VAST COMITÉ I, *Activiteitenverslag 2011*, 7-14 en 104-107).

II.1.3.3.4. Geïntegreerde aanpak voor alle divisies

Het onderzoek heeft aangetoond dat er tot eind 2012 geen document bestond waarin de Divisies I, CI en S samen en op geïntegreerde wijze werden opgenomen. Het *CHOD OPORDER for Bel contribution to ISAF* bevatte wel een aantal bepalingen in verband met de inlichtingenopdracht, maar zweeg over de bijdrage van de Divisies CI en S. In januari 2013 werd hieraan verholpen wat betreft de Divisie CI.[42]

II.1.3.3.5. Onduidelijkheid over de aard van in te winnen inlichtingen

Het Vast Comité I stelde een onduidelijkheid vast over de aard van inlichtingen waarop de ADIV zich in hoofdzaak moet richten: strategische, operationele en/of tactische. Volgens de SOP OPS *Joint Intelligence, Counter-Intelligence and Security Structure* van ACOS-Ops & Trg (zie II.1.1.5) moet de ADIV vooral politico-strategische en operationele inlichtingen aanleveren. In het CHOD OPORDER inzake Afghanistan (zie II.1.3.3.4) krijgt de ADIV echter ook een taak inzake '*tactical intelligence*' mee.

In de praktijk blijkt dat de analysediensten van de ADIV eerder op strategische *intelligence* gericht zijn, maar dat de men op het terrein vooral operationeel/tactische inlichtingen nodig heeft.

Het Vast Comité I stelt vast dat deze onduidelijkheid reeds enige tijd bestaat. Deze kwestie is niet onbelangrijk voor de manier waarop de ADIV zijn inlichtingengaring en -verwerking organiseert. Het zonder onderscheid vermengen van de verschillende typen van inlichtingen kan de efficiëntie bemoeilijken. Bovendien is er ook een weerslag op de kennisdomeinen die nodig zijn voor de collecte en analyse: de meer 'politico-civiele benadering' voor de strategische inlichtingen, tegenover de 'militaire *facts and figures*' voor de tactische en operationele inlichtingen.

II.1.4. HET OORDEEL VAN DE KLANTEN VAN DE ADIV

Het Vast Comité I heeft een bevraging gehouden van de voornaamste klanten van de ADIV: de FOD Buitenlandse Zaken (waar vooral zijn Crisiscentrum wat betreft de bescherming van Belgische onderdanen in het buitenland en de zogenaamde Veiligheidsdienst wat betreft de veiligheid in de buitenlandse diplomatieke posten betrokken partij zijn), ACOS-Ops & Trg die binnen Defensie onder meer is belast met het operationele commando van de interventietroepen en het Kabinet van de minister van Defensie.

Algemeen gesproken bleken deze 'klanten' vrij tevreden te zijn over de samenwerking met de ADIV. De dienst blijkt enerzijds flexibel en snel te reageren op

[42] Sindsdien is de gezamenlijke inzet van de divisies op het terrein een feit.

vragen die hem worden gesteld en anderzijds wordt de relevantie en de accuraatheid van de producten benadrukt. De ADIV heeft bovendien een uitstekende reputatie als het op de betrouwbaarheid van zijn producten aankomt.

De ADIV heeft zowel formele en structurele contacten met zijn partners en ter zelfde tijd heeft de dienst tal van informele contacten die zowel de flexibiliteit als de souplesse van het optreden bevorderen.

De producten van de ADIV beslaan hoofdzakelijk veiligheidsthema's op het operationele, tactische en strategische niveau en slaan in mindere mate op de politieke thema's. Nochtans heeft de ADIV ook als opdracht om economische, sociale en mediagerelateerde domeinen te behandelen zoals voorzien is in de *Comprehensive Preparation of the Operational Environnement* (CPOE). Volgens de ADIV worden deze domeinen slechts gedeeltelijk gecoverd omwille van een gebrek aan personeel. Recent werd daarom afgesproken dat Defensie zich op veiligheidsproblemen zal concentreren en Buitenlandse Zaken op voornoemde domeinen.

ACOS-Ops & Trg heeft te kennen gegeven dat ze een grotere betrokkenheid van de ADIV verwacht, in het bijzonder in het kader van de CPOE. Gezien het belang van deze opdracht zowel voor de militaire autoriteiten als voor het kabinet van de minister, komt het er voor de ADIV op aan om na te denken over zijn capaciteit om aan deze vraag tegemoet te komen.

Ten slotte moest het Comité vaststellen dat de klanten onvoldoende weten wat de ADIV kan produceren en – alhoewel ze over de bijdrage van de ADIV tevreden zijn – bijgevolg niet alle mogelijk vragen stellen. Van zijn kant betreurt de analysedienst van de ADIV een gebrek aan *feedback* over zijn producten.

II.1.5. CONCLUSIES

II.1.5.1. De wettigheidstoets en andere reglementaire aspecten

Het Comité was van oordeel dat de ADIV zijn opdrachten in Afghanistan uitvoert conform de nationale en internationale regelgeving en dit ondanks het feit dat deze normen niet alleen talrijk zijn, maar ook weinig geïntegreerd.

Het Comité betreurde evenwel dat de ADIV geen studie had gewijd aan haar eventuele verantwoordelijkheid wanneer ze informatie of inlichtingen verschaft aan een buitenlandse dienst of instantie. Het feit dat het Ministerieel Comité voor inlichting en veiligheid ter zake (nog) geen richtlijnen had opgesteld, deed daaraan geen afbreuk.

Ten slotte wees het Comité op de noodzaak van een herdefiniëring van de concepten 'operationele', 'tactische' en 'strategische' inlichtingen. De meeste internationale en nationale normen hanteren deze begrippen om de competentiedomeinen van de diverse actoren (BENIC, inlichtingenofficier S2, BIC…) af te bakenen. Maar de Wet van 30 november 1998 gebruikt deze terminologie niet; ze

bepaalt de bevoegdheid van de ADIV in functie van dreigingen die moeten worden opgevolgd. Om aan deze opdracht te voldoen, moet de ADIV alle beschikbare informatie verzamelen. Het Comité stelde bovendien vast dat deze begrippen in de praktijk niet bepalend zijn voor het verzamelen of de verspreiding van informatie. Het Comité meende derhalve dat het nuttig zou zijn om na te denken over het verband tussen deze begrippen en de wettelijke opdrachten van de ADIV. Dit lijkt des te meer noodzakelijk gezien het bestaan van het bataljon ISTAR (cf. *supra*).

II.1.5.2. De noodzaak om het risico voor het personeel in conflictzones in te schatten

Het Comité heeft meermaals kunnen vaststellen dat het personeel van de ADIV in sommige situaties risico's loopt. Vandaar dat het sterk de nadruk legde op de kwaliteit van de opleiding voorafgaand aan de ontplooiing en op de noodzaak om over adequate materiële en logistieke middelen te kunnen beschikken.

Meer in het bijzonder stelde het Comité vast dat de ADIV nog geen algemene inschatting maakte van de risico's die inherent verbonden zijn aan het inzetten van militairen of burgerpersoneel in conflictzones. Dergelijke inschatting moet bijvoorbeeld toelaten te oordelen of een ontplooiing van burgerpersoneel (analisten) te overwegen valt en zo ja, om de behoeftes inzake opleiding en materieel te bepalen. Daarenboven zou kunnen gepreciseerd worden welke rol de analisten kunnen spelen in een omgeving waarin aan informatiegaring wordt gedaan, in het bijzonder om de objectiviteit van de analysefunctie te garanderen en elke beïnvloeding te vermijden. Deze reflectie inzake risico's moet evident ook gelden voor de militairen van ADIV. Het Comité was van oordeel dat dit nog onvoldoende gebeurde.

II.1.5.3. De noodzaak om een meer systematische benadering bij de inzet van de ADIV in een conflictzone

Het Comité was van oordeel dat de ontplooiing van de ADIV in Afghanistan op pragmatische wijze gebeurde. Een dergelijke benadering is niet noodzakelijk verkeerd, maar levert het risico op dat aan een aantal meer conceptuele aspecten voorbij wordt gegaan. Een geïntegreerde benadering, waarbij vertrokken wordt van de op te volgen bedreigingen, biedt de mogelijkheid om coherente verbanden te leggen tussen de W.I&V, de *mission statement* van de ADIV, het geïntegreerde strategisch plan van I, CI en S, de Inlichtingen- en Veiligheidsinlichtingenstuurplannen, het collecteplan en vooral de menselijke en materiële middelen die moeten worden ingezet om de inlichtingendoelstellingen te bereiken. In het algemeen laat enkel een geïntegreerde benadering toe om objectief vast te stellen of de ADIV over voldoende personeel en materieel beschikt om zijn wettelijke opdrachten te vervullen.

II.1.5.4. De noodzaak om over adequaat materieel te beschikken

Het Comité heeft moeten vaststellen dat de fysieke integriteit van de personeelsleden van de ADIV gevaar kan lopen. Het is dan ook noodzakelijk dat zij over adequate, materiële middelen beschikken. In het algemeen is dit zeker ook het geval. Wel zijn de communicatiemiddelen die ter beschikking worden gesteld aan de BENIC, voor verbetering vatbaar.

II.1.5.5. De aanbevelingen van de Rwanda-commissie

II.1.5.5.1. Duidelijke regels in verband met de inzetbaarheid en de vertaling daarvan in begrijpbare richtlijnen

Het Comité wees op de verscheidenheid van nationale en internationale regels die van toepassing zijn bij de ontplooiing van het Belgische leger in Afghanistan. Daarenboven is deze regelgeving bijzonder complex, enerzijds omdat er een gebrek aan integratie is (er is geen codex voorhanden) en anderzijds omdat er een gebrek is aan 'vertaling' van de regels in begrijpbare richtlijnen. Een dergelijke complexiteit kan er toe leiden dat de regels niet gekend zijn of verkeerd geïnterpreteerd worden. Daarom pleitte het Comité voor een geïntegreerde voorstelling van de vigerende normen.

Wat de nationale regels betreft, was het Comité bovendien van oordeel dat zij beter op elkaar dienen afgestemd te worden, bijvoorbeeld vertrekkende vanuit de wettelijke opdrachten van de ADIV.

II.1.5.5.2. Een adequate voorbereiding van een opdracht

Het Comité heeft kunnen vaststellen dat de leden van de ADIV voor hun vertrek een specifieke voorbereiding genoten. Deze voorbereiding omvatte verschillende aspecten zoals het gedrag ter plaatse, de situatie in het land alsook een praktische uiteenzetting over de regels inzake de inzetbaarheid. Met uitzondering van dit laatste aspect, kon het Comité in deze recent belangrijke verbeteringen vaststellen.

II.1.5.5.3. Een solied inlichtingennetwerk

De Rwanda-commissie drong er op aan dat de ADIV in de toekomst over een eigen inlichtingennetwerk zou beschikken alsook over opgeleide en getrainde inlichtingenofficieren die de taal machtig zijn of een beroep kunnen doen op vertalers. Het Comité heeft kunnen vaststellen dat deze doelstelling bereikt was. Niettemin zag het Comité twee mogelijke verbeterpunten.

Enerzijds kon de opleiding van het ontplooide personeel van de ADIV verbeterd worden. De ADIV dient in deze een belangrijke en blijvende inspanning te leveren. De recente aanpassingen hebben ontegensprekelijk een toegevoegde waarde, maar

ze waren volgens het Comité niet voldoende. De opleiding moet praktisch en flexibel zijn en mag niet afhangen van de beschikbaarheid van de opleiders.

Anderzijds moet de rol van de ADIV in de voorbereiding van een internationale opdracht versterkt worden. In deze moet de ADIV zich inschrijven in de methodologie van de *Comprehensive Preparation of the Operational Environnement* (CPOE) en aanpassen aan de door de partners binnen het leger uitgedrukte behoeften en ter zake proactief optreden. Dit vergt onder andere dat de ADIV analyses uitvoert in de domeinen die tot haar bevoegdheid behoren.

II.1.5.5.4. Beschikken over voldoende, bekwame analisten

De Rwanda-commissie drong aan op een hervorming van de ADIV zodat de dienst voor diegenen die voor een opdracht verantwoordelijkheid dragen, een efficiënt en coherent instrument zou vormen. Het stelde ook voor de analysecapaciteit te verbeteren en deze ter beschikking te stellen voor het uitwerken van politieke opties ten behoeve van de verantwoordelijken.

Het Comité stelde vast dat deze doelstellingen in grote mate bereikt waren. De ADIV is inderdaad een onmisbare en belangrijke partner geworden bij het verzamelen en het uitbaten van informatie ten behoeve van de troepen op het terrein en in het bijzonder in het kader van de *force protection*. Ook werd zijn rol als raadgever van de hiërarchische en politieke verantwoordelijken en zijn optreden in het kader van de voorbereiding van operaties of tijdens de uitvoering ervan bevestigd.

Het Comité meent niettemin dat de rol van raadgever voor de hiërarchische en politieke verantwoordelijken nog niet ten volle kan gespeeld worden. Dit is mogelijks en ten dele het gevolg van een gebrek aan analisten binnen de ADIV. Dit gebrek zou evenwel kunnen ondervangen worden wanneer de inzet van analisten meer gebeurt in functie van duidelijke inlichtingendoelstellingen.

De klanten van de ADIV bevestigden dat ze tevreden waren over de producten van de ADIV, al werd toegegeven dat zij niet echt op de hoogte zijn welke producten precies zouden kunnen worden aangeleverd. De analisten meenden van hun kant dat zij vanwege hun klanten onvoldoende *feedback* kregen op de door hen geleverde producten. Deze vaststellingen pleiten voor een meer proactieve benadering van de ADIV naar zijn klanten toe. Concreet betekent dit dat de ADIV actief de behoeften en wensen van zowel de interne als externe klanten van Defensie zou moeten gaan bevragen, om de efficiëntie van zijn producten te kunnen optimaliseren. Wel was het Comité er zich van bewust dat ook de klanten tot deze optimalisatie moeten bijdragen.

II.1.5.5.5. De noodzaak om gespecialiseerde ploegen te ontplooien

Het Comité heeft tijdens haar missie in Afghanistan kunnen vaststellen dat de door de ADIV ontplooide ploegen zeer professioneel te werk gaan en dit tot tevredenheid van de Belgische en buitenlandse autoriteiten. De commandanten van de

Belgische onderdelen ter plaatse erkennen dat er een systematische *return* bestaat naar de eenheden op het terrein.

II.2. GEHEIME NOTA'S OVER DE SCIENTOLOGY-KERK IN DE PERS

Op 17 januari 2013 citeert de pers passages uit de nota '*Eglise de Scientologie – Infiltration de la communauté congolaise ou d'origine congolaise de Belgique, Implantation en République démocratique du Congo*' van de VSSE.[43] Deze geheim geclassificeerde nota van 11 december 2012 was door de dienst kort daarvoor verspreid onder bepaalde overheden. In de artikels wordt beweerd dat de Scientologykerk haar activiteiten probeert uit te breiden in Afrika en in dat kader tussenpersonen zoekt in de Belgisch-Congolese gemeenschap. Daarenboven worden een aantal politici bij naam genoemd[44]: Bertin Mampaka, toen ondervoorzitter van het Brussels Hoofdstedelijk Parlement en gemeenteraadslid te Brussel[45]; Justine Kasa-Vubu, voormalig minister in de eerste regering van Laurent-Désiré Kabila en nadien ambassadrice in Brussel; Gisèle Mandaila, in die periode Brussels Volksvertegenwoordiger en in 2004 Staatssecretaris voor Gezinnen en Personen met een handicap en tevens gemeenteraadslid in Etterbeek en ten slotte Pierre Migisha, ten tijde van het lek Brussels Volksvertegenwoordiger en gemeenteraadslid in Anderlecht.

Op verzoek van de Begeleidingscommissie wordt een toezichtonderzoek geopend waarbij zowel de totstandkoming als de verspreiding van de nota moet bestudeerd worden.

Amper veertien dagen later wordt in de pers gewag gemaakt van een andere nota van de VSSE.[46] Ditmaal betrof het de '*Fenomeenanalyse – Niet-staatsgestuurde inmengingsactiviteiten*'. Ook in dit geheime rapport zouden tal van politici worden geciteerd omwille van hun relaties met onder meer de Scientologykerk. Hierop werd het Comité door de minister van Justitie belast met een toezichtonderzoek. Er moest worden onderzocht of de ministeriële richtlijn van 25 mei 2009, volgens dewelke de minister van Justitie op de hoogte moet worden gebracht telkens de naam van een federaal parlementslid wordt vernoemd in een verslag, correct werd toegepast en of het al dan niet aangewezen was om parlementsleden bij naam te noemen in een fenomeenanalyse. Een dag later werd door

43 A. CLEVERS, *La Dernière Heure*, 17 januari 2013 (La Scientologie infiltre les milieux belgo-congolais); K. VAN EYCKEN en H. ADRIAEN, *Het Laatste Nieuws*, 17 januari 2013 (Scientology infiltreert in Congolese gemeenschap in Brussel).

44 De namen van deze politici kwamen uitgebreid aan bod in de media.

45 Nadien werd betrokkene door het parlement van de Franse Gemeenschap aangewezen tot Senator.

46 M. BUXANT en S. SAMYN, *De Morgen*, 2 februari 2013 (Staatsveiligheid houdt Wetstraat in de gaten).

de Begeleidingscommissie de opdracht gegeven haar eerste onderzoek uit te breiden naar de totstandkoming en de openbaarmaking van deze fenomeenanalyse en naar de vraag of de Belgische inlichtingendiensten een correcte toepassing hebben gemaakt van het *need to know*-principe.[47]

De opdrachten die de Begeleidingscommissie en de minister van Justitie toewezen aan Comité, hadden grotendeels betrekking op dezelfde problematiek. Het Comité besliste dan ook al die aspecten onder te brengen in één enkel onderzoek met als titel '*Toezichtonderzoek naar de wijze van aanmaak en verspreiding door de VSSE van de nota over de infiltratie door de Scientology-beweging van de Congolese gemeenschap in Brussel en het rapport 'Fenomeenanalyse – Niet-staatsgestuurde inmengingsactiviteiten', hierbij inbegrepen het bestuderen van de problematiek van de vermelding van de namen van politieke mandatarissen en de lijsten van bestemmelingen en hun 'need-to-know'*.[48]

II.2.1. DE GEHEIME NOTA VAN 12 DECEMBER 2012 OVER DE SCIENTOLOGYKERK

II.2.1.1. De inhoud van de nota

De VSSE moet activiteiten opvolgen die een bedreiging (kunnen) vormen voor de veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde. Bij de uitoefening van deze opdracht, stootte de VSSE op namen van politieke mandatarissen die in verband konden gebracht worden met de Scientologykerk. Dit gaf aanleiding tot het opstellen van verschillende nota's. Zo ook van de gelekte nota van 11 december 2012 waarin de relatie van de vier hogervermelde politici met de Scientologykerk werd behandeld. De nota kan als volgt worden samengevat:

– een van de vier betrokkenen wordt benaderd door de Scientologykerk;
– een tweede onderhoudt relaties met de Scientologykerk;

---

47 Tevens werd het Comité belast met een 'transversale analyse' naar de wijze waarop de inlichtingendiensten informatie inwinnen over politieke mandatarissen (II.4).

48 Niet alleen het Vast Comité I opende een onderzoek. Ingevolge de verschillende lekken, diende de VSSE begin februari 2013 klacht in met burgerlijke partijstelling tegen onbekenden wegens inbreuk op artikel 11 van de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM). Het Comité kreeg geen inzage in het gerechtelijk onderzoek. Ook de Nationale Veiligheidsoverheid (NVO) opende bij de bestemmelingen van zowel de eerste nota als van de fenomeenanalyse een veiligheidsonderzoek. Ook de resultaten hiervan zijn bij het Vast Comité I niet gekend. Op 20 maart 2013 ten slotte, werd in naam van de Scientologykerk van België vzw, een klacht ingediend bij het Vast Comité I. Het onderzoek dat hierop volgde, werd afgerond begin 2014 (II.11.8). In het parlement werd ook een 'Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de gevallen waarin de Veiligheid van de Staat verkozen politici schaduwt' ingediend. (*Parl. St.* Kamer 2012-2013, nr. 53K2652/001 en *Parl. St.* Senaat 2012-13, nr. 5-2034/1).

– met betrekking tot de overige twee beweert de VSSE op basis van door de buitendiensten gemelde feiten dat ze zeer dicht staan bij de Scientologykerk of er zelfs lid van zijn.

Volgens het Comité handelde de VSSE bij het opstellen van deze eerste nota binnen het kader van haar wettelijke bevoegdheden zoals die staan omschreven in de Wet van 30 november 1998. Het Comité verwees meer bepaald naar artikel 8, 1° e) en g) dat betrekking heeft op 'schadelijke sektarische organisaties' en 'inmenging'. Het Comité beschikte over geen enkele aanwijzing dat er onregelmatigheden zouden hebben plaatsgevonden bij het vergaren van de inlichtingen die aan de basis lagen van de nota. Daarenboven was de nota genuanceerd in haar bewoordingen.

II.2.1.2. De bestemmelingen van de nota en hun need to know

De bewuste nota werd bezorgd aan zes bestemmelingen, te weten de ministers van Justitie en Buitenlandse Zaken, de Ambassadeur van België in Congo en de Voorzitter, het Hoofd Veiligheid en de Directeur Afrika van de FOD Buitenlandse Zaken. Ze waren allen houder van de vereiste veiligheidsmachtiging. Tevens maakte hun functie als minister, hoge functionaris of diplomaat en hun verantwoordelijkheid inzake diplomatie en internationale relaties dat voldaan was aan de vereiste van de *need to know*. De nota had namelijk betrekking op de infiltratie van de Congolese of van oorsprong Congolese gemeenschap in België door de Scientologykerk en haar vestiging in de Democratische Republiek Congo. Het Comité was de mening toegedaan dat deze inlichtingen belangrijk waren voor de overheden die belast zijn met het buitenlands beleid van België. Deze informatie moest dus bij toepassing van artikel 19 W.I&V[49] aan de betrokken overheden worden bezorgd.

II.2.1.3. De meldingsplicht

In de periode waarop het toezichtonderzoek betrekking had, bestonden er twee richtlijnen die een verplichting inhielden voor de VSSE om de minister van Justitie in kennis te stellen wanneer politici het voorwerp uitmaakten van inlichtingenactiviteiten: een ministeriële richtlijn van 25 mei 2009 – opgesteld naar aanleiding van de aanbevelingen van het Vast Comité I in het kader van een eerder toezichtonderzoek[50] – en een interne instructie van 27 maart 2012.[51]

---

49 '*De inlichtingen- en veiligheidsdiensten delen de inlichtingen bedoeld in artikel 13, tweede lid, slechts mee aan de betrokken ministers en de betrokken gerechtelijke en administratieve overheden, aan de politiediensten en aan alle bevoegde instanties en personen overeenkomstig de doelstellingen van hun opdrachten alsook aan de instanties en personen die het voorwerp zijn van een bedreiging bedoeld in de artikelen 7 en 11.*'

50 VAST COMITÉ I, *Activiteitenverslag 2008*, 22-33 (II.2. 'Gereserveerde dossiers' bij de Veiligheid van de Staat).

51 Zie hierover ook II.4.2.1.3.

De richtlijn van 25 mei 2009 stelt dat de minister van Justitie op de hoogte moet worden gebracht telkens de naam van een zetelend federaal parlementslid wordt vernoemd in een verslag. Geen van de vier betrokkenen bekleedde destijds een dergelijk mandaat. Er diende dus geen kennisgeving te gebeuren.

Het toepassingsgebied van de interne instructie van 27 maart 2012 is zowel enger als ruimer dan dat van de ministeriële instructie: ze heeft enerzijds alleen betrekking op vermeldingen in verslagen van de buitendiensten van de VSSE, maar anderzijds op alle ministers en politieke mandatarissen, ook deze van de Gemeenschappen en Gewesten.

Ten aanzien van Justine Kasa-Vubu diende ook ingevolge deze richtlijn geen kennisgeving te gebeuren aangezien zij geen Belgisch politiek mandataris was.

Ten aanzien van de drie anderen diende de minister wél te worden geïnformeerd. Met betrekking tot Bertin Mampaka had de VSSE reeds in juli 2012 een eerste nota bezorgd aan de minister van Justitie waarin gewag werd gemaakt van de contacten die hij had met de Scientologykerk. Deze nota kan dus als kennisgeving worden beschouwd. Met betrekking tot Pierre Migisha en Gisèle Mandaila kan alleen de nota van 11 december 2012 worden beschouwd als de vereiste kennisgeving. De VSSE had de minister wat deze twee laatsten betreft dus sneller moeten informeren.

II.2.2. DE FENOMEENANALYSE BETREFFENDE DE 'NIET-STAATSGESTUURDE INMENGINGSACTIVITEITEN[52]

II.2.2.1. De inhoud van de fenomeenanalyse

Het bewuste verslag vormt de vierde fenomeenanalyse die de VSSE opstelde. Het Vast Comité I benadrukte opnieuw[53] het nut van een dergelijk type van verslag dat *'expose un thème actuel qui relève des sphères d'intérêt et des missions dévolues à un service de renseignement et qui représente un défi politique et social majeur, tant aujourd'hui que pour les années à venir. Elle s'attache à décrire ce problème tant au niveau de ses origines historiques, qu'au plan de l'idéologie, de l'organisation, de la structure et des activités y relatives. Elle contextualise les défis et les risques, établit une 'évaluation de risque' à destination de nos responsables politiques, des autorités administratives concernées et des autorités judiciaires qui sont également confrontées à cette problématique […]'*.[54]

---

52 De problematiek van de verwittiging van de minister van Justitie in geval van inlichtingenactiviteiten ten aanzien van politieke mandatarissen werd opgenomen in het het onderzoek 'De opvolging van politieke mandatarissen door de inlichtingendiensten' (II.4).

53 VAST COMITÉ I, *Activiteitenverslag 2012*, 14-28 (II.2. De opvolging van buitenlandse inlichtingendiensten ten aanzien van hun diaspora in België).

54 Uit 'Extrémisme islamique en Belgique, Analyse du phénomène' van de VSSE.

Het Comité stelde echter vast dat de directie van de VSSE aan de opstellers ervan geen duidelijke richtlijnen had gegeven en had nagelaten de doelstellingen en de methodologie te definiëren. Het doel van deze fenomeenanalyse werd in de inleiding slechts kort toegelicht: '*de Veiligheid van de Staat tracht met deze fenomeenanalyse een beeld te schetsen van de inmengingsactiviteiten van groeperingen en/of organisaties in politieke en economische middens*'. Daarbij wees de VSSE erop dat elke organisatie het recht heeft te lobbyen om haar doelstellingen te promoten. Wordt er echter contact opgenomen met personen die verantwoordelijke functies bekleden om op die wijze beslissingsprocessen te beïnvloeden of om invloed uit te oefenen, dan wordt de grijze zone van het lobbyen overschreden en kan er sprake zijn van 'inmenging' in de zin van artikel 8, 1°g) W.I&V, aldus de VSSE.

Het Comité uitte voorts kritiek op het feit dat het rapport naliet op duidelijke wijze[55] de strategie te omschrijven die de Scientologykerk aanwendt om te trachten '*beslissingsprocessen te beïnvloeden met ongeoorloofde, bedrieglijke of clandestiene middelen*' (art. 8, 1° g) W.I&V). Evenmin werd er ingegaan op de werkelijke doelstellingen van de organisatie, noch op de wijze waarop contacten worden gelegd en onderhouden. Het Comité vond het dan ook aanbevelenswaard om in dergelijke analyse bij wijze van voorbeeld uiteen te zetten hoe een rekrutering kan verlopen: eerste contact(en) door een tussenpersoon, benaderen van parlementsleden, benadering via organisaties die hun relatie met de Scientologykerk niet onthullen, aanbieden van voordelen of hulp (bijvoorbeeld deelname aan cursussen of financiële hulp voor projecten)…

Maar het Comité was vooral kritisch voor de wijze waarop uitvoerig namen van (voormalige) politieke mandatarissen en hun medewerkers werden vermeld.[56] Ook al kwamen sommige namen meermaals voor en werd de betrokkenheid van sommige personen nader toegelicht, toch ontstond de indruk dat alle genoemde personen op eenzelfde niveau moesten worden geplaatst en dezelfde informatieve waarde bezaten. Het Comité wees er in deze op dat de vermelding bij naam in een verslag van de VSSE een 'stigmatiserend' effect heeft, zelfs indien dit verslag op beperkte schaal verspreid wordt.

Het Comité benadrukte dat, indien de opsomming van namen bedoeld was om aan te tonen wat de reikwijdte is van de contacten van de Scientologykerk en van diens activiteiten, het essentieel is te specifiëren wat de juiste band is tussen een welbepaald persoon en de Scientologykerk: zijn er één of meerdere pogingen tot toenadering geweest, waren deze pogingen succesvol, in welke context hebben ze plaatsgevonden, heeft de betrokkene op passieve of actieve wijze deelgenomen

55 Soms is wel op impliciete wijze duidelijk welke strategie wordt gevolgd. Mogelijk zijn de opstellers van de analyse te veel uitgegaan van de hypothese dat het voor de lezer om een evidentie ging.

56 Het Comité stelde vast dat de opstellers van de analyse zonder tussenkomst van de directie beslist hadden om namen te noemen. Het Vast Comité I plaatste vraagtekens bij deze beslissing.

aan activiteiten (bijvoorbeeld door een toespraak te houden op een conferentie), was de betrokkene zich bewust van het feit dat de activiteiten werden georganiseerd door de Scientologykerk… Met andere woorden, indien de VSSE het noodzakelijk acht om namen te noemen – en dat is haar verantwoordelijkheid – dan moet ze in het verslag de graad van betrokkenheid van elke persoon aangeven.

Indien het echter de bedoeling is om de ontwikkeling van de activiteiten van de Scientologykerk aan te tonen en op gedetailleerde wijze te illustreren dat er een welomschreven strategie van contactname en rekrutering wordt gevolgd (met andere woorden, indien men een fenomeen wil beschrijven), is het niet nodig om namen te noemen. In dat geval volstaan abstracte voorbeelden die aangeven hoe en waar de Scientologykerk leden rekruteert en netwerken uitbouwt.

II.2.2.2. De bestemmelingen van de fenomeenanalyse en hun need to know

Naast de verspreiding binnen de VSSE zelf, werd de fenomeenanalyse verzonden naar 33 personen.

De VSSE had vóór de verspreiding contact opgenomen met de Nationale Veiligheidsoverheid om na te gaan of de bestemmelingen houder waren van een veiligheidsmachtiging van het vereiste niveau. Dit bleek het geval, één uitzondering niet te na gesproken.[57] De VSSE liet zoals vereist een ontvangstbewijs tekenen door de bestemmeling of diens veiligheidsofficier. In een begeleidend schrijven bij de fenomeenanalyse wees de VSSE bovendien op de noodzaak tot strikte inachtneming van de Classificatiewet en op het ernstig nadeel dat kon voortvloeien uit een ongepast gebruik van het rapport.

Het Vast Comité I moest wel vaststellen dat er geen vooraf opgestelde lijst bestond van bestemmelingen voor dit soort van analyses: wie een rapport zou ontvangen en wie niet werd aan de appreciatie van de opstellers overgelaten. De hiërarchische overheid voegde er *in casu* wel enkele namen aan toe.

Het spreekt voor zich dat de ruime verspreiding die hiervan het gevolg was, het risico op lekken vergroot. Het Vast Comité I legde evenwel de nadruk op het feit dat vooreerst de perso(o)n(en) aan de oorsprong van de lekken verantwoordelijk is (zijn) (in de veronderstelling uiteraard dat er opzettelijk gelekt werd of de informatie bij de pers terecht kwam ingevolge een nalatigheid) voor de negatieve gevolgen hiervan voor de VSSE en de genoemde mandatarissen.

Bij het opstellen van de lijst met bestemmelingen was naar het oordeel van het Comité niet doordacht te werk gegaan. Ofwel werd door de VSSE in algemene termen verwezen naar de 'wettelijke bevoegdheid' van bepaalde personen (met name van de Eerste Minister, de Vice Eerste Ministers of de ministers die lid zijn van het Ministerieel Comité voor inlichting en veiligheid) ofwel, meer specifiek, naar hun veronderstelde *need to know*. Het probleem hierbij is evenwel dat de

[57] Eén bestemmeling beschikte niet over een veiligheidsmachtiging. Hij kreeg dan ook geen exemplaar van de fenomeenanalyse.

vraag wie een 'kennisnemingsbehoefte' heeft, afhankelijk is van de finaliteit van het product dat wordt verspreid. Ofwel wil het informeren over een algemeen fenomeen van inmenging, ofwel wil men de aandacht vestigen op precieze risico's waarmee een persoon of instantie in het kader van zijn of haar functie wordt of kan worden geconfronteerd. In dit laatste geval oordeelde het Comité dat het niet nodig is om het volledige verslag te bezorgen. Integendeel, op dat ogenblik is het aangewezen om de informatie te beperken tot wat nuttig is voor een welbepaalde bestemmeling. Indien het verslag echter bedoeld is om te informeren over een algemeen fenomeen, dan is het verzenden van een volledig verslag gerechtvaardigd. Maar op dat ogenblik stelt zich de vraag of het aan de VSSE zelf toekomt om dergelijk verslag te bezorgen aan veertien ambtenaren/diplomaten van de FOD Buitenlandse Zaken. Het Comité stelde zich de vraag of het niet meer aangewezen zou zijn mochten verslagen worden verzonden naar één enkele bestemmeling die als *point of contact* binnen dit departement de 'kennisnemingsbehoefte' van elk van zijn collega's kan beoordelen.[58]

Concreet wat betreft de fenomeenanalyse inmenging oordeelde het Comité dat het passender zou zijn geweest om het verslag op meer gerichte wijze te verspreiden, en dit in functie van de behoeften van elke bestemmeling. Hierdoor zouden mogelijks ook de negatieve gevolgen van het lek beperkt zijn gebleven.

II.3. EEN INFORMANT BINNEN HET VLAAMS BELANG?

Begin 2013 raken twee geheime rapporten van de Veiligheid van de Staat in de openbaarheid (zie II.2). In de parlementaire debatten die daarop volgen, verklaarde de minister van Justitie dat het '*niet de opdracht [van de VSSE] is om individuele parlementsleden te volgen. Dat is niet de opdracht van die dienst en het gebeurt in de praktijk ook niet*'.[59] Bart Debie, ex-politiecommissaris van Antwerpen en gewezen veiligheidsadviseur van Filip Dewinter (Vlaams Belang), meende dat tegen te moeten spreken. In een krantenartikel[60] liet hij optekenen: '*Wat ze met andere politici doen, weet ik niet. Maar de Staatsveiligheid heeft het Vlaams Belang jarenlang met héél véél aandacht gevolgd. En ik kan het weten, want ik was er zelf bij betrokken*'. Debie verklaart informant te zijn geweest van de VSSE van 2007 tot 2010 – periode tijdens dewelke hij woordvoerder/veiligheidsadviseur was van het Vlaams Belang. Er volgen hevige reacties van Filip Dewinter, de minister van Justitie en de administrateur-generaal van de VSSE.

---

58 Recent zou de VSSE beslist hebben om voortaan via een *point of contact* te werken.

59 *Hand.* Kamer 2012-13, 7 februari 2013, CRIV53COM666, 9 e.v. Verder: '*[…] ik herhaal ook dat het niet tot de opdracht van de Veiligheid van de Staat behoort om parlementsleden in de gaten te houden in hoofde van hun functie*'.

60 J. VAN DER AA en T. LE BACQ, *De Standaard*, 11 februari 2013 (Ik was de mol binnen Vlaams Belang).

Net daarvoor had het Vast Comité I over de thematiek van de opvolging van politieke mandatarissen een algemeen onderzoek opgestart.[61] Het Comité besliste evenwel in te gaan op deze specifieke *casus*, en een 'deelonderzoek' te voeren naar de contacten van de Veiligheid van de Staat met Bart Debie en de informatie die daaruit voortvloeide, in het bijzonder deze aangaande Filip Dewinter. Vooraf-gaand wordt overlopen of en in welke mate in de opvolging van het Vlaams Blok/ Belang werd voorzien doorheen de jaren.

II.3.1. DE OPVOLGING VAN HET VLAAMS BLOK, LATER VLAAMS BELANG

Op basis van de artikelen 7 en 8 W.I&V is de VSSE bevoegd om het extremisme[62] op te volgen wanneer dit een bedreiging vormt of zou kunnen vormen voor de interne of externe veiligheid van het land. De opvolging van politici of politieke partijen is dus mogelijk vanuit deze invalshoek. Wel moet bij de eventuele opvolging uiteraard rekening worden gehouden met de Grondwet, het EVRM en de rechtspraak van het Europees Hof voor de Rechten van de Mens inzake vrijheid van meningsuiting en vrijheid van vereniging.

Tot midden jaren '90 werd het Vlaams Blok systematisch opgenomen in de zogenaamde 'lijst met onderwerpen'. Op de lijsten van 1996 en 1999 kwam de partij niet meer voor.[63] In die periode diende er dus geen opvolging meer te gebeuren.

Daar kwam verandering in toen de minister van Justitie in 2001 de VSSE de instructie gaf om het Vlaams Blok opnieuw te beschouwen als een te behandelen onderwerp conform de Wet van 30 november 1998, met uitzondering van de activiteiten van de mandatarissen gesteld in het kader van hun parlementair mandaat. De uitoefening van een dergelijk mandaat werd daarbij gedefinieerd als '*de meningsuiting, de parlementaire vragen en interpellaties, het indienen van een wetsvoorstel, kortom wat zich in het parlementair halfrond afspeelt*'. In een interne richtlijn van juli 2001 werkte de VSSE de contouren van deze ministeriële richtlijn verder uit: de inlichtingen die over het 'Vlaams Blok' worden vergaard en verwerkt, moesten betrekking hebben op alle individuele en collectieve activiteiten die rechtstreeks verband houden met extremisme, zoals gedefinieerd in artikel 8, 1° W.I&V. Alle activiteiten zonder extremistisch karakter worden niet als dusdanig opgevolgd. De aandacht diende dus uit te gaan naar de actieve, extremistische militanten.

---

61 Zie *infra* 'II.4. De opvolging van politieke mandatarissen door die inlichtingendiensten'.

62 Extremisme wordt daarbij gedefinieerd als *'racistische, xenofobe, anarchistische, nationalistische, autoritaire of totalitaire opvattingen of bedoelingen, ongeacht of ze van politieke, ideologische, confessionele of filosofische aard zijn, die theoretisch of in de praktijk strijdig zijn met de beginselen van de democratie of de mensenrechten, met de goede werking van de democratische instellingen of andere grondslagen van de rechtsstaat* (art. 8, 1° c W.I&V).'

63 Er werd destijds niet noodzakelijk elk jaar een nieuwe lijst opgesteld.

In 2003 vraagt de VSSE – middels een bijzonder goed gemotiveerde nota – aan de Eerste Minister in zijn hoedanigheid van voorzitter van het Ministerieel Comité voor inlichting en veiligheid, om het Vlaams Blok van de lijst van op te volgen onderwerpen te verwijderen. Op deze vraag volgt geen antwoord. In 2004 wordt het Vlaams Blok het Vlaams Belang. Toch vormt dit geen aanleiding voor de VSSE om de bevoegde overheden opnieuw te bevragen omtrent hun standpunt inzake de al dan niet opvolging van de partij. Op de 'Lijst van onderwerpen' van 2006 komt het Vlaams Blok (*sic*) dan ook nog steeds voor.

Sinds 2009 maakt de VSSE geen 'lijst met onderwerpen' meer op. Vanaf dan wordt jaarlijks een zogenaamd 'actieplan' opgesteld dat door de minister van Justitie moet worden goedgekeurd. In dat plan worden de te volgen fenomenen en groeperingen[64] opgelijst en onderverdeeld in functie van een 'actieve opvolging'[65], een 'reactieve opvolging'[66] of 'geen opvolging'.[67] Zo wordt in het Actieplan 2010 onder de noemer 'reactieve behandeling' *'Extreme Rechts Nationalistische e/o identiteit bewegingen (…) nederlandstalig: Vlaams Belang'* vermeldt. De Actieplannen 2011 en 2012 maken onder meer melding van *'Vlaams Belang – interne partijwerking en nationale standpunten'*, maar dan onder de noemer 'geen opvolging'. In het Actieplan 2013 wordt de partij niet meer vernoemd. De rubriek 'geen opvolging' werd sindsdien niet meer opgenomen.

II.3.2. DE CONTACTEN TUSSEN BART DEBIE EN DE VSSE

Het eerste contact tussen Bart Debie en de VSSE kwam er op initiatief van Debie zelf. Halverwege augustus 2010[68] stuurde hij een e-mailbericht naar de VSSE om zijn diensten aan te bieden omdat hij van een *'heel bekend politicus opdrachten heeft gekregen die de grenzen van het strafrecht ver overschrijden'* en waarmee hij

64 Maar nooit individuele personen *as such*.

65 Dit betekent dat de VSSE actief activiteiten ontwikkelt om de informatiepositie te verwerven, uit te bouwen of te verstevigen.

66 'Reactieve opvolging' betekent dat de VSSE activiteiten ontwikkelt om de informatiepositie te verwerven, uit te bouwen of te verstevigen, maar slechts in reactie op een uitdrukkelijke vraag daartoe.

67 'Geen opvolging' betekent dat de VSSE de opvolging niet verzekert, of desgevallend niet aan een externe vraag om inlichtingen kan voldoen. Het betreft die problematieken waarvoor de dienst zich bewust is van de noodzaak tot opvolging en/of investering, maar waarvoor gelet op de onvoldoende capaciteit een adequate informatiepositie ontbreekt en geen acties kunnen worden gepland. Dit betekent dus niet dat de VSSE geen informatie over deze thema's kan ontvangen, verzamelen of opslaan, maar wel dat de VSSE deze niet verder uitdiept en dat de opvolging ervan louter incidenteel is.

68 In de pers werd initieel gesteld dat Bart Debie reeds in 2007 in contact was met de VSSE. Dit bleek echter niet uit het onderzoek van het Vast Comité I. Wellicht ging het om een misverstand: tijdens zijn contacten met de pers sprak betrokkene over zaken die zich in 2007 hadden afgespeeld, maar die hij pas in 2010 had gemeld. De journalisten erkenden nadien overigens zelf dat zij mogelijks onnauwkeurig waren geweest (T. NAEGELS, *De Standaard*, 27 februari 2013 (Welles-nietes-nieuws).

zich '*deontologisch niet langer mee [kon] verzoenen*'. Sindsdien vonden vijf ontmoetingen plaats en werden herhaaldelijk e-mails uitgewisseld, en dit tot juli 2012.

Bart Debie verschafte informatie over de buitenlandse contacten en geplande reizen van Filip Dewinter; over zijn positie binnen het Vlaams Belang en de machtsverhoudingen binnen de partij; over zijn 'sponsors' en deze van het Vlaams Belang; over een internationale conferentie waarvan het Vlaams Belang de praktische organisatie in handen had; over de verbanden tussen het Vlaams Belang en een aantal extreemrechtse organisaties; over de terreuraanval van de Noor Anders Breivik in 2011[69] en over het bezoek van Amerikaanse zakenlui en Senatoren aan Europa waarbij Filip Dewinter de delegatie in Antwerpen ontving. Uiteraard kwamen ook de feiten die aan de basis lagen van de contactname (vermeende illegale activiteiten) aan bod.

Er wordt ook sporadisch e-mailverkeer uitgewisseld waarin Bart Debie niets bijzonders te melden heeft. Na verloop van tijd stuurt geen van beide partijen nog aan op verdere ontmoetingen. In juli 2012 ten slotte meldt Bart Debie dat hij informatie heeft over 'een lek bij het Parket'. Er wordt een ontmoeting geregeld maar betrokkene daagt niet op. Nadien vonden er geen contacten meer plaats.

Het Vast Comité I oordeelde dat de VSSE met deze contacten binnen de perken van haar jaarlijkse actieplannen was gebleven. Het Actieplan 2010 voorzag in een 'reactieve' opvolging van extreemrechts en van het Vlaams Belang wat inhoudt dat de VSSE activiteiten mag ontplooien om te reageren op een specifieke gebeurtenis of ontwikkeling. Het Vast Comité I was van mening dat de informatie die betrokkene in eerste instantie leek te zullen geven – over '*opdrachten die de grenzen van het strafrecht ver overschrijden*' – dan ook rechtvaardigde dat werd ingegaan op het aanbod van Bart Debie. Ook gelet op zijn status binnen het Vlaams Belang en zijn kennis van het extreemrechtse veld kon dergelijke bron niet zomaar aan de kant worden geschoven. In het Actieplan 2011 werd het Vlaams Belang opgenomen onder de categorie 'geen opvolging'. Dit betekende evenwel niet dat de VSSE over dit thema geen informatie meer zou mogen ontvangen. Aangezien dat jaar via de bron weinig informatie werd opgetekend die rechtstreeks betrekking had op het Vlaams Belang, was ook deze opvolging conform het actieplan. In 2012 doofden de contacten met Bart Debie uit. In het actieplan van dat jaar was het Vlaams Belang nog steeds opgenomen onder de rubriek 'geen opvolging'.

Het Comité stelde eveneens vast dat de VSSE in haar relatie met Bart Debie de instructie van 15 mei 2001 had gerespecteerd: ze had geen inlichtingen ingewonnen die te maken hadden met de uitoefening van het parlementair mandaat *as such* (het uiten van de opinie en de werkzaamheden in het Parlement) van Filip Dewinter of van andere parlementairen.

---

[69] Deze had in zijn 'manifest' naar Belgische personen verwezen en het document was ook verzonden naar een aantal Belgen, waaronder een Volksvertegenwoordiger van het Vlaams Belang. De VSSE wilde weten of er linken waren tussen de Noorse dader en de geciteerde Belgische namen.

Het Vast Comité I was in het algemeen van mening dat de manier waarop de VSSE de contacten met Bart Debie had voorbereid en afgehandeld voor weinig of geen kritiek vatbaar was. Zo werden de doelstellingen van de inlichtingengaring (bijvoorbeeld inzake de intenties van Bart Debie, de vermeende illegale activiteiten van Filip Dewinter en 'verdoken' financieringskanalen van zijn partij) door de Analysedienst duidelijk uiteengezet en door de Buitendiensten ter harte genomen. Er werd meermaals uitdrukkelijk in herinnering gebracht dat de verzamelde informatie betrekking moest hebben op activiteiten die verband (kunnen) houden met extremisme. De informatie moest bijvoorbeeld kunnen bijdragen tot het detecteren en analyseren van extremistische (xenofobe of racistische) tendensen binnen het Vlaams Belang en niet op de uitoefening van het parlementair mandaat *as such* van Filip Dewinter of van andere parlementairen. Dit werd ook meermaals duidelijk gemaakt aan de bron. In de rapporten kwamen soms wel namen voor van Vlaams Belang-parlementsleden, maar niet in relatie tot hun parlementaire activiteiten. Er werd overigens zelden of nooit verwezen naar de hoedanigheid van parlementslid. Het Comité moest wel vaststellen dat de medewerkers van de VSSE de limieten van hun optreden wat betreft parlementaire mandatarissen, niet steeds adequaat konden omschrijven, al voelden ze deze misschien intuïtief wel goed aan. De grenzen gesteld in de richtlijn van de informatie die mag ingewonnen worden als het om een politicus gaat, waren niet erg duidelijk.

Ten slotte stelde het Comité ook vast dat de materiële omstandigheden waarin de bron werd ontmoet, normaal waren. Er werden hem geen financiële voordelen gegeven, slechts één kleine attentie. In de loop van de gesprekken had Bart Debie ook persoonlijke problemen aangekaart. Hij kreeg geen erkenning om cursussen te geven aan ambulanciers en vroeg zich tevens af of hij in aanmerking zou kunnen komen voor herstel in eer en rechten voor een vroegere veroordeling. De betrokken commissaris van de VSSE liet aan zijn bron weten dat er volgens de door hem gecontacteerde persoon geen uitzonderingen werden gemaakt. Verder verstrekte hij hem enkel informatie die ook publiek toegankelijk was.

II.3.3. FILIP DEWINTER IN DE DATABANK VAN DE VSSE[70]

Uiteraard beschikte de VSSE reeds vóór haar contacten met Bart Debie over informatie met betrekking tot Filip Dewinter.[71] Zijn naam was in het datasysteem

[70] Op 11 februari 2013 was in de media een lijvig dossier te zien dat tijdens een interview op het bureau van de administrateur-generaal van de VSSE lag. Op de kaft stond de naam van 'Dewinter Philip'. Het Comité stelde vast dat het enkel ging om een bundel met procedurestukken, briefwisseling en nota's in verband met de vele procedures die de betrokkene had gevoerd om toegang te krijgen tot zijn dossier bij de VSSE.

[71] Ook de ADIV beschikte over informatie en inlichtingen met betrekking tot Filip Dewinter, maar in veel geringere mate dan de VSSE. Het 'dossier' Dewinter bij de ADIV was oud, weinig systematisch bijgehouden en voornamelijk samengesteld uit informatie afkomstig van open bronnen.

van de VSSE, dat sinds 2001 operationeel is[72], 214 maal gelinkt met bepaalde materies zoals 'extreemrechts', maar ook bijvoorbeeld met 'salafisme' of 'radicale islam'.[73] Ook de verslagen die naar aanleiding van de contacten met Bart Debie waren opgemaakt[74], werden in de databank opgenomen en gekoppeld aan *in casu* 'Extremisme' en 'Extreemrechts Nederlandstalig'. In 156 gevallen ging het om een 'pertinente link'; in 55 gevallen betrof het een link 'ter info'; drie linken waren 'te bepalen'. Het Comité stelde vragen bij de juiste betekenis van deze concepten[75] én bij de concrete toepassing ervan op het terrein.

Naast de koppeling van een naam aan een materie, zijn er ook de zogenaamde 'operationele linken' waarbij een verband wordt gelegd tussen twee namen en de relatie tussen beiden een kwalificatie krijgt in de zin van 'bevriend met', 'tegenstander van', 'kennis van', 'sympathisant van' …

Het Comité meende uit zijn analyse niet te moeten afleiden dat de VSSE een overdreven aandacht voor de betrokkene aan de dag zou hebben gelegd. Uit het relatief kleine aantal operationele linken dat werd gelegd tussen Filip Dewinter en derden – in totaal 50 op twaalf jaar tijd – blijkt dat de VSSE zeer behoedzaam tewerk is gegaan en geen belangrijke 'informatiepositie' ten aanzien van betrokkene heeft uitgebouwd. Het Vast Comité I was van mening dat de VSSE zich ter zake eerder schroomvallig heeft gedragen.

II.3.4. RAPPORTERING AAN DE MINISTER VAN JUSTITIE

Wat betreft de melding aan de minister van Justitie wanneer bepaalde politieke mandatarissen opgevolgd worden door de VSSE, waren twee richtlijnen van belang.[76] Enerzijds was er de instructie van de minister van Justitie van 25 mei 2009 inzake de rapportering van vermeldingen van federale parlementsleden. Anderzijds was er de interne instructie van 27 maart 2012 die betrekking had op ministers, de Staatssecretarissen en de verkozenen van het federale, het gemeenschaps- en het gewestelijke niveau. Op 8 juli 2010 werd betrokkene Gemeenschapssenator wat betekent dat beide richtlijnen van toepassing waren op de informatie die voortvloeide uit de contacten met Bart Debie. Eén uitzondering niet te na gesproken, werden ze echter niet opgevolgd wat betreft de informatie over Filip Dewinter.

---

72 In het informaticasysteem dat vóór 2001 operationeel was, kwam de naam van Filip Dewinter voor in 459 documenten. Mede gelet op het feit dat het verouderde informatie betrof, nam het Comité deze documenten niet op in zijn onderzoek.

73 Een link kon zowel betekenen dat men betrokken was bij een fenomeen maar ook dat men er slachtoffer van was.

74 Omdat het om een menselijke bron ging en gelet op het delicate karakter van de zaak, werden de gegevens die voortvloeiden uit de contacten opgenomen in een zogenaamde 'operatie'. Op die manier krijgen slechts die personen die uitdrukkelijk gemachtigd zijn tot het kennisnemen van een welbepaalde operatie, toegang tot de informatie uit de databank van de VSSE.

75 Zie ook II.4.2.3.

76 Zie ook Hoofstuk II.2.1.3 en II.4.2.1.3.

II.4. DE OPVOLGING VAN POLITIEKE MANDATARISSEN DOOR DE INLICHTINGENDIENSTEN

Net zoals het onderzoek naar '*Geheime nota's over Scientology in de pers*' (II.2) en '*Een informant binnen het Vlaams Belang?*' (II.3.) is ook dit toezichtonderzoek het gevolg van dezelfde twee in de pers verspreide geclassificeerde nota's van de Veiligheid van de Staat. In de (parlementaire) debatten die op de bekendmaking volgden, werd veelvuldig de vraag gesteld of en in welke mate de Belgische inlichtingendiensten politieke mandatarissen (mogen) opvolgen en welke regels ze daarbij in acht moeten nemen. Het Comité besliste daarop een thematisch onderzoek te openen '*naar de wijze waarop de inlichtingendiensten informatie verzamelen over politieke mandatarissen, de wijze waarop ze met deze informatie omgaan en analyseren en de wijze waarop ze hierover rapporteren aan de bevoegde overheden*'.

Het was overigens niet voor het eerst dat het Vast Comité I de activiteiten van de inlichtingendiensten ten aanzien van politieke mandatarissen onderzocht.

Al in 1997 werd een onderzoek geopend '*naar de manier waarop de inlichtingendiensten het onderscheid maken tussen de activiteiten van parlementsleden als milieupacifisten en als parlementsleden*'.[77] Het onderzoek kwam er na een vraag van een Ecolo-parlementslid en spitste zich toe op de inlichtingen die de VSSE en de ADIV gebeurlijk over mandatarissen van Ecolo of Agalev (thans Groen!) zouden verzamelen. Het Comité kwam tot de conclusie dat de diensten dossiers hadden op de naam van een aantal parlementsleden van deze partijen, maar dat de activiteiten van deze personen sinds 1988 niet meer in het bijzonder gevolgd werden.

Een jaar later, in 1998, startte het Vast Comité I in het verlengde van voormeld onderzoek een meer algemene enquête over '*de verzameling van gegevens over parlementsleden door de inlichtingendiensten*'.[78] Dit onderzoek had betrekking op de mandatarissen van *alle* politieke partijen. Het Comité kwam in deze tot de conclusie dat '*noch de VSSE noch SGR onderzoek instellen naar handelingen die in het kader van de eigenlijke uitoefening van het parlementair mandaat worden gesteld*'.

In 2006 ten slotte kwamen de zogenaamde 'gereserveerde dossiers' bij de VSSE aan de oppervlakte.[79] Klaarblijkelijk werden sinds het eind van de jaren '80 een aantal dossiers met gegevens over verkozenen bijgehouden door de dienst 'Affaires Générales' van de VSSE, en dit buiten het 'normale circuit'. Sommige van deze dossiers werden zelfs exclusief op het secretariaat van de toenmalige administrateur-directeur-generaal van de Openbare Veiligheid bewaard. Het Comité besloot in dit onderzoek onder meer dat '*het actueel voorkomen van politieke mandatarissen en prominenten in de nu geïnformatiseerde rapporten van een inlichtingendienst een uiterst delicaat gegeven blijft. Het Comité was echter van mening dat de hoedanigheid van een prominent of politicus geen beletsel kan zijn voor een ade-*

77 VAST COMITÉ I, *Activiteitenverslag 1998,* 67 e.v.
78 VAST COMITÉ I, *Activiteitenverslag 1999*, 12 e.v.
79 VAST COMITÉ I, *Activiteitenverslag 2008*, 23 e.v.

quate opvolging en van een navenante beschikbaarheid van de rapportering hierover in het licht van de uitvoering van de wettelijke opdrachten van een inlichtingendienst. Deze activiteit dient immers te gebeuren 'zonder onderscheid des persoons'.'[80] In het verlengde hiervan deed het Comité volgende aanbeveling: *'Meer in het algemeen wenst het Vast Comité I dat de Veiligheid van de Staat klare en eenduidige richtlijnen uitwerkt met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen. Bij de uitwerking van deze richtlijnen en bij de concrete opvolging van de (gewezen) politieke mandatarissen dient de Veiligheid van de Staat rekening te houden met de krijtlijnen uitgetekend in het arrest van het Europees Hof voor de Rechten van de Mens in de zaak Segerstedt-Wiberg and others'.*[81]

II.4.1. ENKELE CIJFERGEGEVENS UIT HET NIEUWE ONDERZOEK

Op 1 maart 2013 waren er precies – dubbelmandaten buiten beschouwing gelaten – 479 personen die ofwel een ministerpost bekleedden in de federale of regionale regeringen of die verkozen waren als parlementslid van een regionale of federale, wetgevende vergadering. In zijn toezichtonderzoek vroeg het Comité aan beide inlichtingendiensten om na te gaan of en in welke mate de namen van deze personen in hun papieren dossiers en databanken voorkwamen.

Daaruit bleek dat de Buitendiensten van de VSSE vanaf juni 2010 (of met andere woorden, vanaf de start van de toenmalige federale legislatuur) tot begin 2013 727 documenten hadden opgesteld waarin telkenmale minstens één van de 479 mandatarissen werd vernoemd. In totaal werden 142 verschillende mandatarissen vernoemd.[82]

De Analysedienst van de VSSE telde over dezelfde periode 423 documenten waarin 93 verschillende politieke mandatarissen waren vermeld. Iets meer dan de helft van deze documenten waren afkomstig van externe bronnen (bijvoorbeeld

---

80 VAST COMITÉ I, *Activiteitenverslag 2008*, 30 e.v.

81 VAST COMITÉ I, *Activiteitenverslag 2008*, 110-111. In de zaak *Segerstedt-Wiberg and others* tegen Zweden van 6 juni 2006 problematiseerde het Hof het inwinnen en opslaan van gegevens over politieke opinie, verwantschap en lidmaatschap van personen en dit in het licht van artikel 8 EVRM. Het feit dat dergelijke gegevens, ook al betreffen het publiek gekende feiten, worden ingezameld of bijgehouden is een ernstige inmenging in het privéleven. Deze inmengingen kunnen – aldus het Hof – alleen gerechtvaardigd zijn wanneer zij proportioneel zijn vanuit het perspectief van de nationale veiligheid. Bij de beoordeling van deze proportionaliteit hechtte het Hof zeer veel belang aan het al dan niet gewelddadige karakter van een politieke partij. Dit karakter mag niet alleen afgeleid worden uit het politieke programma; het moet zich eveneens vertalen in de acties van de partijleiders en de posities die zij innemen.

82 Sommigen kwamen in meerdere documenten voor: 37% van de mandatarissen kreeg één vermelding, 35% twee tot vijf vermeldingen. Vier mandatarissen kwamen in meer dan 21 documenten voor. Eén verkozene werd in 91 documenten vermeld.

het OCAD, de politie of andere correspondenten); de andere helft vormde 'eigen productie'. Het betrof documenten voor intern gebruik (synthesenota's met een stand van zaken in een bepaald dossier en verslagen van vergaderingen), documenten bedoeld voor externen (nota's gericht aan Belgische autoriteiten en – slechts enkelen – aan buitenlandse overheden) en 'kantschriften' waarin de Analysedienst bepaalde vragen stelde aan de Buitendiensten.

Het Comité nam een steekproef van deze documenten[83] en bestudeerde ze om een zicht te krijgen op het collecte- en analysewerk van de VSSE ten aanzien van politieke mandatarissen (*infra*).

De ADIV[84] van zijn kant beschikte zowel over informatie op papieren als op digitale dragers. Zo bijvoorbeeld waren 115 steekkaarten beschikbaar die correspondeerden met een papieren dossier van politieke mandatarissen. Het grootste deel van de bijhorende dossiers was echter reeds vernietigd. In het zogenaamde 'levend' archief bevonden zich slecht 36 dossiers en in het 'dood' archief (omdat ze gedurende vijftien jaar niet meer waren geraadpleegd) nog 12.

In de databank van de ADIV werden de namen van 109 mandatarissen gevonden. Het Vast Comité I bestudeerde één vierde van deze dossiers. Daarbij bleek dat bijvoorbeeld nooit vermeld werd of een persoon al dan niet parlementslid was.

De ADIV had in de referteperiode van het toezichtonderzoek geen analysenota's opgesteld die specifiek op ministers of parlementaire mandatarissen betrekking hadden.

II.4.2. DE OPVOLGING VAN POLITICI DOORHEEN DE INLICHTINGENCYCLUS

Het Comité overliep bij zijn analyse van de geselecteerde dossiers alle aspecten van de inlichtingencyclus, te beginnen bij 'de sturing van de inlichtingenactiviteiten' over 'de collecte', 'de organisatie van de informatie' en 'de analyse' tot aan 'de verspreiding van de inlichtingen'.

II.4.2.1. Sturing van de inlichtingenactiviteiten

De activiteiten van de Belgische inlichtingendiensten worden op verschillende niveaus aangestuurd. Het meest algemene niveau is dat van de regelgeving – te weten wetten, besluiten en algemene instructies – waarbij bepaald wordt welke inlichtingenactiviteiten mogen worden uitgevoerd en op welke manier dit mag geschieden. Daaronder bevindt zich het niveau van de jaarlijkse actie- of inlichtingenplannen die – op voorstel van de diensten en goedgekeurd door de bevoegde

[83] Eén op de vier dossiers werd bestudeerd. Hierop werd één uitzondering gemaakt: de nota's die bestemd waren voor buitenlandse overheden werden allemaal in de analyse betrokken.

[84] Meer bepaald de Divisie C(ounter) I(ntelligence) die bevoegd is voor interne dreigingen.

minister – *in concreto* bepalen welke materies het komende jaar mogen of moeten bestreken worden. Ten slotte is er de *ad hoc* aansturing in concrete dossiers door het diensthoofd of de bevoegde minister. Deze drie niveaus worden hieronder besproken.

II.4.2.1.1. Regels van toepassing op het verzamelen van inlichtingen met betrekking tot politieke mandatarissen

De Wet van 30 november 1998 houdende regeling voor de inlichtingen- en veiligheidsdienst (W.I&V) bevat geen bepaling die aan een parlementslid een bijzonder statuut zou verlenen. In de wet wordt overigens geen verwijzing gemaakt naar politieke mandatarissen. Hetzelfde geldt voor de BIM-Wet van 4 februari 2010 die niet voorziet in een bijzondere bescherming voor politici, terwijl ze dat wél doet voor beroepsjournalisten, advocaten en artsen. Vanuit die optiek herhaalde het Comité zijn stelling uit 2008 dat de hoedanigheid van politicus geen beletsel kan zijn voor een adequate opvolging en rapportering. Het inlichtingenwerk dient immers te gebeuren 'zonder onderscheid des persoons'. Wel moet bij de eventuele opvolging rekening worden gehouden met de rechtspraak van het Europees Hof voor de Rechten van de Mens inzake vrijheid van meningsuiting en de vrijheid van vereniging. Er dient uiterst omzichtig te worden omgesprongen met een inmenging in deze grondrechten ten aanzien van (zelfs extreme) politieke partijen en mandatarissen.

Vanuit het besef dat de opvolging van politieke partijen of mandatarissen bijzonder gevoelig is, werd in 2001 een specifieke beperking ingebouwd voor de opvolging van parlementaire mandatarissen van het toenmalige Vlaams Blok[85]: in de ministeriële richtlijn van 15 mei 2001 waarbij de opdracht werd gegeven om die partij op te volgen, werd gesteld dat dit moet gebeuren met uitzondering van de activiteiten van de mandaterissen gesteld in het kader van hun parlementair mandaat. De VSSE definieerde deze beperking verder als volgt: '*een parlementair mandaat*' is '*de meningsuiting, de parlementaire vragen en interpellaties, het indienen van een wetsvoorstel, kortom wat zich in het parlementair halfrond afspeelt*'.

Sindsdien is deze definitie – waarvan men zich kan afvragen of ze (nog) voldoende gekend was, of ze van toepassing is buiten de mandatarissen van de betrokken partij om én of ze voldoende pertinent en duidelijk is – nooit expliciet herhaald, verfijnd of genuanceerd. Wel greep de minister van Justitie er in 2013 naar terug in haar antwoorden op enkele parlementaire vragen: activiteiten van een parlementslid '*binnen het parlement zelf*', in het kader van hun '*parlementaire functie*' of '*in hun optreden als parlementslid*' mogen niet opgevolgd worden door een inlichtingendienst.[86] Maar ook deze 'preciseringen', die dateerden van na de

85 Zie hierover Hoofdstuk II.3.

86 *Hand.* Senaat, 21 februari 2013, nr. 5-92, 16-18 en *Hand.* Senaat, 14 maart 2013, nr. 5-95, 17-19.

opstart van voorliggend toezichtonderzoek, namen volgens het Comité niet alle vragen weg. Immers, in de praktijk is het onderscheid tussen de activiteiten van een parlementaire mandataris binnen zijn of haar mandaat en erbuiten, moeilijk te handhaven. Daarenboven vallen bepaalde aspecten buiten de *scoop* van deze beperking (zoals bijvoorbeeld de rol van een parlementslid bij de interne partijwerking en de bepaling van de partijstrategie), terwijl ze net veel 'gevoeliger' zijn dan het louter stellen van een parlementaire vraag of het indienen van een wetsvoorstel (hetgeen informatie betreft die per definitie publiek is).

Het Comité herhaalde dan ook de aanbeveling uit zijn onderzoek 'gereserveerde dossiers'[87] om klare en eenduidige richtlijnen uit te werken met betrekking tot inlichtingenactiviteiten van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen.

Uiteraard geldt de noodzaak van een omvattende, duidelijke richtlijn ook voor de ADIV. Immers, deze dienst hanteerde ten tijde van het onderzoek nog steeds een instructie die dateerde van vóór de Wet van 30 november 1998. In een nota van 25 juni 1998 wordt uiteengezet dat politieke mandatarissen niet opgevolgd mogen worden uit hoofde van hun mandaat, maar dat ze, net zoals ieder ander burger, de aandacht van de ADIV kunnen weerhouden wanneer ze een veiligheidsmachtiging nodig hebben, wanneer ze deel uitmaken van een organisatie die een bedreiging vormt voor de opdrachten van Defensie of wanneer ze een militair domein trachten binnen te dringen of de activiteiten van Defensie trachten te belemmeren.

II.4.2.1.2. Opname van politieke partijen in de jaarlijkse actie- of inlichtingenplannen

In 2013 kwamen geen in het Parlement vertegenwoordigde politieke partijen meer voor in de jaarlijkse actie- of inlichtingenplannen van respectievelijk de VSSE en de ADIV. Voordien werden, wat de Veiligheid van de Staat betreft, bepaalde partijen systematisch vermeld als *target*, en dit soms op expliciet verzoek van de bevoegde minister (zie II.4.2.1.1).

Ook al werden er in 2013 geen in het Parlement vertegenwoordigde politieke partijen *as such* opgevolgd, toch was het Vast Comité I van oordeel dat ook hieromtrent klare en eenduidige richtlijnen zouden moeten worden uitgewerkt.

II.4.2.1.3. *Ad hoc*-sturing door minister van Justitie: een toepassingsmodaliteit van de richtlijn van 25 mei 2009

Op 2 mei 2009 had de toenmalige minister van Justitie in het Parlement aangekondigd dat '*de Veiligheid van de Staat hem telkens een waarschuwingsnota […] ter informatie zal sturen voor een actief federaal parlementslid dat werd vermeld of*

87 VAST COMITÉ I, *Activiteitenverslag 2008*, 110-111.

gelieerd is met een specifieke materie in een dossier als onderdeel van informatie of als persoon het voorwerp uitmaakt van bedreigingen ten overstaan van zijn persoon of als een buitenlandse inlichtingendienst interesse betoont in hem'.[88] In uitvoering hiervan gaf de minister op 25 mei 2009 zijn goedkeuring aan een instructie die gebaseerd was op een ontwerp van de VSSE. Deze richtlijn hield in dat de minister een '*note d'avertissement*' zou ontvangen '*pour tout parlementaire fédéral en activité cité pour information ou lié à une matière spécifique dans un rapport, en tant qu'élément d'information, ou qui fait l'objet de l'attention de la Sûreté de L'Etat comme personne menacée ou encore comme cible de l'intérêt d'un agent de renseignement étranger, ces citations ou liens réalisés dans l'exercice des compétences de la Sûreté de l'Etat. L'avertissement serait envoyé à Monsieur le Ministre sous la forme d'une note classifiée 'Secret – Loi 11.12.1998' pour tout parlementaire fédéral cité ou lié dans un rapport produit par la Sûreté de l'Etat. […] La Sûreté de l'Etat poursuivra son activité de surveillance de manière normale (silent procedure), sauf avis contraire de Monsieur le Ministre de la Justice.*'[89]

In 2013 stelde de toenmalige administrateur-generaal van de VSSE hierover het volgende: '*Grosso modo bevat de richtlijn drie aspecten. De belangrijkste vernieuwing betrof de onmiddellijke inkennisstelling van de minister van Justitie telkens de naam van een actief federaal parlementslid in een verslag van de VSSE voorkomt. De VSSE en de minister kwamen hiermee tegemoet aan de ongerustheid die bij sommige federale parlementsleden was gerezen naar aanleiding van het toezichtonderzoek van het Vast Comité I naar de zogenaamde 'gereserveerde dossiers'.*'[90] De administrateur-generaal wees er op dat deze werkwijze tevens toelaat dat de minister zijn verantwoordelijkheid kan opnemen door desgewenst bijkomende, punctuele bevelen aan de VSSE te geven. Ook kan hij toezicht houden op het inlichtingenonderzoek, eventueel via het Vast Comité I. Ten slotte laat een in kennisstelling de minister van Justitie toe te antwoorden op vragen van parlementsleden die gebruik maken van hun grondwettelijk controlerecht. Hierdoor wordt volgens de administrateur-generaal tegemoet gekomen aan de eisen van een parlementaire democratische rechtsstaat.

---

88 VAST COMITÉ I, *Activiteitenverslag 2009*, 3.

89 '*voor elk actueel, federaal parlementslid die 'ter informatie' of die gelinkt aan een specifieke materie vermeld wordt in een rapport, als informatief element, of die voorwerp uitmaakt van de aandacht van de VSSE, als bedreigd persoon of nog, als target van een buitenlandse inlichtingenagent, moeten deze vermeldingen of verbanden gerealiseerd worden in het kader van de uitoefening van de bevoegdheden van de VSSE. De verwittiging zal naar de minister van Justitie worden gezonden onder de vorm van een 'GEHEIM – Wet 11.12.1998' geclassificeerde nota en dit voor elk federaal parlementslid die geciteerd of gelinkt wordt in een verslag opgesteld door de VSSE. […] De VSSE zal zijn opvolgingsactiviteit op een normale manier verderzetten (silent procedure), behoudens anders beslist door de Heer minister van Justitie*' (vrije vertaling).

90 A. WINANTS, '*Control in the circus*. Interne controle bij de Veiligheid van de Staat' in *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, W. VAN LAETHEM en J. VANDERBORGHT (eds.), Antwerpen, Intersentia 2013, 137.

Naar het oordeel van het Vast Comité I verwoordde de administrateur-generaal zeer goed het belang van de richtlijn van 2009. Het Comité had deze instructie overigens reeds positief onthaald. In zijn *Activiteitenverslag 2009* stelde het dat '*op die wijze reeds ten dele tegemoet gekomen wordt aan de bekommernissen van het Vast Comité I*', geuit in het kader van het onderzoek 'gereserveerde dossiers'.[91]

Echter, sinds juni 2010 (met andere woorden, op een ogenblik dat de instructie ongeveer één jaar van kracht was) waren binnen de VSSE al een 350-tal[92] verslagen en nota's opgesteld waarin de naam werd vermeld van op dat ogenblik actieve federale parlementsleden, terwijl hiervan slechts uitzonderlijk melding was gemaakt op de voorgeschreven wijze … Dat de instructie nauwelijks werd nageleefd, werd blijkbaar ook nooit opgemerkt, gemeld, gecontroleerd en/of geproblematiseerd intern de dienst. Het Vast Comité I wees er in zijn toezichtonderzoek overigens op dat de richtlijn niet volledig *kon* worden nageleefd alleen al omwille van het feit dat de VSSE niet beschikte over een (permanent ge-update) lijst van alle politieke mandatarissen. Gevolg was onvermijdelijk dat soms verslagen werden opgesteld over parlementsleden, zonder dat men noodzakelijkerwijs weet had van hun statuut.

In de loop van het toezichtonderzoek stelde de VSSE een aantal wijzigingen voor aan zijn werkprocessen. Zo onder meer wat betreft de verwittiging van de vermelding van parlementsleden in zijn verslagen. In dit werkdocument stelde de VSSE voor om de minister maandelijks (en dus niet langer onmiddellijk) in kennis te stellen wanneer parlementsleden vermeld worden in documenten van de Analysedienst (en dus niet langer van de Buitendiensten). Dit werkdocument resulteerde na het afsluiten van het onderzoek van het Comité in een nieuwe instructie (zie Hoofdstuk I.1.3).

II.4.2.2. De collecte

Het Vast Comité I benadrukte dat het merendeel van de meldingen van parlementsleden in collecteverslagen van de VSSE ingegeven was ofwel door het feit dat de betrokken mandataris zelf het voorwerp was van een mogelijke bedreiging, ofwel omdat hij (toevallig) in contact kwam met een persoon of een groepering die wordt opgevolgd. Het Comité vond geen aanwijzingen dat de VSSE politieke mandatarissen viseerde om redenen buiten de wettelijke opgesomde belangen en bedreigingen om.

Wat de ADIV betreft, kon dezelfde conclusie getrokken worden: de dienst vertoonde geen interesse voor politieke mandatarissen *as such*. Wanneer de ADIV uitzonderlijk aandacht besteedde aan mandatarissen, dan gebeurde dit in relatie

---

91 VAST COMITÉ I, *Activiteitenverslag 2009*, 3.

92 Het in II.4.1 vermelde aantal van 727 documenten betreffen mandatarissen van zowel federale als regionale regeringen en assemblees, terwijl het *in casu* enkel federale mandatarissen betreft.

tot een militair belang of een militaire materie. Het merendeel van de ADIV-dossiers was overigens reeds geopend lang voordat de betrokken politicus een mandaat had opgenomen. Ook dit toonde aan dat het 'politieke mandaat' niet relevant was voor de aandacht van de ADIV.

Het Vast Comité I vond bij de VSSE op het niveau van de collecte in zijn steekproef slechts één dossier waaruit kon worden opgemaakt dat gegevens waren verzameld over elementen die mogelijks kaderden 'binnen het parlementair mandaat' zoals omschreven in de bovenvermelde richtlijn van 25 mei 2001 en zich 'binnen het parlement zelf' (*in casu* weliswaar een parlement van een deelstaat) afspeelde. Het betrof informatie die de VSSE had ontvangen over een vergadering die een politieke partij had georganiseerd met een buitenlandse politieke beweging dewelke een bedreiging zou kunnen uitmaken. Dit voorbeeld illustreerde voor het Comité opnieuw dat de in de richtlijn opgesomde criteria weinig nuttig en werkbaar zijn. Immers, enerzijds beperken politieke activiteiten zich niet tot het halfrond en anderzijds lijken er geen goede redenen voorhanden te zijn om dreigingen die zouden voorbereid worden vanuit het parlement, niet op te volgen. Het Vast Comité I was dan ook van oordeel dat deze criteria moesten herbekeken worden.

Dat het Comité geen elementen vond die wezen op een onrechtmatige opvolging van parlementsleden, betekende evenwel niet dat daarmee ook het nut van alle gecollecteerde data was aangetoond. Het Comité kon niet voorbij aan het feit dat een deel van de informatie eerder 'banaal' was: politicus A gaat eerst even persoon B groeten vooraleer weg te gaan; politicus C is aanwezig op een meeting waar duizend mensen aanwezig zijn; politicus D nam deel aan de manifestatie, maar kwam pas op het eind ervan toe… Soms is de link met een van de wettelijk omschreven belangen en dreigingen op het eerste zicht dan ook onduidelijk.

Het Comité is zich weliswaar bewust van het feit dat het in het inlichtingenwerk niet steeds evident is om op het moment van de collecte zelf, meteen uit te maken welke informatie al of niet relevant zal blijken. Dit neemt niet weg dat de eisen ter zake – zoals die omschreven zijn in de W.I&V en de Privacywet (doelbindingsprincipe, adequaatheid, correctheid…) – moeten nageleefd worden. Of en op welke wijze een bepaald feit in een collecteverslag wordt opgenomen, vormt dus een cruciaal gegeven. Het Comité was van oordeel dat de wijze waarop die *input* dient te gebeuren het voorwerp zou moeten zijn van permanente vorming alsook een reële kwaliteitsbewaking. In ditzelfde kader benadrukte het Comité dat uit een verslag duidelijk moet blijken of een persoon ten aanzien van een bepaalde dreiging bijvoorbeeld 'slachtoffer', 'actor' dan wel 'passant' is.

II.4.2.3. Organisatie van de informatie

De databank van de VSSE bevat uiteraard een bijzonder groot aantal gegevens over personen, groeperingen, plaatsen en gebeurtenissen (entiteiten). Om de exploitatie van deze gegevens mogelijk te maken, worden ze 'gelinkt' aan één of meerdere van de wettelijk op te volgen dreigingen zoals extremisme, proliferatie, inmenging… Dit worden 'motiveringen' genoemd. Er zijn vier soorten 'links' mogelijk: 'Voor info', 'Te bepalen', 'Pertinente link' of 'Operationele link'. Een 'Pertinente link' geeft aan dat het verband met één van de materies of dreigingen concreet en overduidelijk is.[93] De link is 'Te bepalen' wanneer nog niet werd uitgemaakt of er al dan niet een pertinente link is. De juiste draagwijdte van de twee andere links is echter minder duidelijk. 'Voor info' wordt nu eens omschreven als een *'link voor entiteiten die geen band hebben met één van de materies of dreigingen die de VSSE behandelt'* en dan weer als *'een link die duidt op een nog niet gekwalificeerde of op een passieve betrokkenheid (bijvoorbeeld als voorwerp van de dreiging)'*. Het Comité moest dan ook vaststellen dat deze concepten niet eenduidig worden omschreven en toegepast. Hierdoor dreigt het inlichtingenwerk aan doelmatigheid en doeltreffendheid te verliezen. Immers, het risico bestaat dat niet (al) de juiste verslagen 'aan de oppervlakte komen' wanneer dit nodig is met het oog op het analysewerk. Mogelijks worden zo verkeerde conclusies getrokken. Het Vast Comité I was dan ook de mening toegedaan dat de VSSE deze concepten dringend moet herbekijken. De dienst zou daarbij ook de mogelijkheid moeten inbouwen om de (vermoedelijke) rol van een in een verslag vernoemd persoon ten aanzien van de dreiging aan te duiden: is hij een 'voorbijganger', een 'mogelijk slachtoffer', een 'sleutelfiguur', een 'actor'…

II.4.2.4. De analyse

Het Vast Comité I vond geen indicaties dat de analysediensten van beide inlichtingendiensten op onwettige wijze aandacht zouden hebben besteed aan ministers en parlementairen.[94] In twee voorgaande onderzoeken (zie II.2 en II.3) werd

---

93 Volgens de richtlijn van 27 maart 2012 mogen ministers en politieke mandatarissen in functie alleen het voorwerp zijn van een 'pertinente link' wanneer uit de informatie van het verslag blijkt dat zij actief betrokken zijn bij een dreiging tegen het voortbestaan van de democratische en van de grondwettelijke orde. Zij kunnen het voorwerp zijn van een 'link voor info' wanneer uit de informatie van het verslag blijkt dat zij het voorwerp zijn van een dreiging of wanneer zij actief betrokken zijn bij een dreiging tegen een van de andere materies waarover de VSSE inlichtingen inwint. Wanneer de opsteller van een verslag meent dat er op basis van de informatie van het verslag voor een minister of een politiek mandataris in functie een pertinente link of een link ter info moet worden gelegd, dan overlegt hij daarover met zijn sectiechef.

94 Slechts in één dossier vond het Comité een verslag dat informatie bevatte die betrekking had op 'parlementaire activiteiten in het parlement'. De informatie was opgetekend door een medewerker van de VSSE die op uitnodiging aanwezig was op een gesloten vergadering in het

reeds aangetoond dat de VSSE zich bewust was van het delicate karakter van het inlichtingenwerk wanneer het politieke mandatarissen betreft. Hetzelfde gold voor de Dienst Analyse van de ADIV-CI.

Wel merkte het Comité op dat ook de analysediensten in hun rapportage de nodige aandacht moeten besteden aan de 'positie' van een in een verslag vermeld persoon ten aanzien van de dreiging ('slachtoffer', 'actor', 'passant'…).

II.4.2.5. De verspreiding van inlichtingen

Het Comité stelde vast dat de ADIV in de referteperiode geen documenten had verspreid naar andere diensten waarin de naam van een minister of een parlementair was vermeld.

De VSSE daarentegen had wel dergelijke nota's gezonden aan Belgische autoriteiten. Het Comité wees er evenwel op dat het net een kerntaak is van deze dienst om de bevoegde autoriteiten in kennis te stellen wanneer iemand het voorwerp is van een bedreiging of zelf aan een bedreiging meewerkt (art. 19 W.I&V), ook al betreft het een Belgisch politicus. Wel moeten bij de verspreiding van deze inlichtingen buiten de VSSE de *need to know* en de eisen van voornoemd artikel 19 W.I&V richtinggevend zijn. Het Vast Comité I had dit zo reeds gesteld in een eerder onderzoek.[95] Dit principe en deze wettelijke bepaling gelden ongeacht de bestemmeling: parket, federale overheidsdiensten, Eerste minister en vakministers, ministers uit de deelregeringen, de Koning als Staatshoofd… Maar uiteraard ook wanneer een buitenlandse dienst bestemmeling is. In dit kader kon het Comité vaststellen dat de VSSE de nodige terughoudendheid aan de dag legde waar het ging om het meedelen van bedoelde verslagen aan buitenlandse diensten. Deze terughoudendheid uitte zich op verschillende manieren: het beperkte aantal mededelingen, de aard van de informatie en de landen waaraan deze informatie werd meegedeeld. Desondanks benadrukte het Comité dat steeds zorgvuldig moet worden afgewogen of namen van Belgische politieke mandatarissen (maar ook van gewone burgers) kunnen vermeld worden in documenten die bestemd zijn voor buitenlandse diensten. Het principe van de *need to know* en de eis van artikel 19 W.I&V is daarbij eens te meer richtinggevend. Maar bij doorgifte van persoonsgegevens naar het buitenland spelen nog andere eisen, zoals bijvoorbeeld deze vermeld in de Privacywet. Het Vast Comité I benadrukte in dit kader opnieuw het belang van een nadere precisering door het Ministerieel Comité voor inlichting en veiligheid van de draagwijdte van artikel 19 W.I&V.

---

parlement. Het verslag was bestemd voor de minister van Justitie. Het Comité stelde zich opnieuw de vraag of het de bedoeling kon zijn dat dergelijke verslaggeving niet toegelaten zou zijn. Het Comité oordeelde dat het de bevoegde minister toekomt om hieromtrent een beslissing te nemen.

95 Zie Hoofdstuk II.2.'Geheime nota's over de Scientologykerk in de pers'.

II.5. DE INFORMATIEPOSITIE VAN DE VEILIGHEID VAN DE STAAT TEGENOVER EEN INTERNATIONALE TRANSACTIE VAN EEN BELGISCH BEDRIJF

II.5.1. EEN KLACHT OVER EEN GEWEIGERDE UITVOERVERGUNNING

Eind 2011 beklaagden vertegenwoordigers van een firma naar Belgisch recht, gespecialiseerd in de productie van hoogtechnologisch materiaal, zich over de weigering van de bevoegde minister om een uitvoervergunning toe te kennen voor een isostatische warmtepers.[96] Nochtans was het land van bestemming partij bij het non-proliferatieverdrag.[97] Daarenboven kreeg het bedrijf volgens de klagers eerder wél een uitvoervergunning voor hetzelfde product naar hetzelfde land. De weigering zou het gevolg zijn van de druk die een buitenlandse regering uitoefende op de Belgische instanties. Naar het oordeel van de klagers was er sprake van een inmenging die nefast was voor hun economische belangen.

Begin 2012 besliste het Vast Comité I een toezichtonderzoek te openen naar de informatiepositie van de VSSE met betrekking tot deze bewuste transactie zowel in het kader van de strijd tegen proliferatie als in het kader van de bescherming van het wetenschappelijk en economisch potentieel van het land.[98]

Het betrof overigens het derde toezichtonderzoek van het Comité waarin de firma betrokken was. Reeds in 2005 werd onderzocht hoe de VSSE informatie afkomstig van een buitenlandse dienst had verwerkt met betrekking tot de uitvoer van een isostatische warmtepers naar Iran.[99] Het Vast Comité I kwam toen tot het besluit dat de VSSE blijk had gegeven van een zekere nonchalance in de manier waarop ze deze informatie had behandeld, geanalyseerd en verspreid.

In 2011 werd een tweede onderzoek afgrond naar de manier waarop de bewuste firma werd opgevolgd door de VSSE.[100] De conclusie luidde dat de dienst

---

96 Een isostatische warmtepers is een machine die tot doel heeft de weerstand en duurzaamheid van sommige materialen te versterken door ze bij hoge warmte onder zeer hoge druk te plaatsen. Dergelijke persen worden gebruikt in de luchtvaartindustrie, maar kunnen ook dienen bij de productie van raketten en kernwapens. Het betreft een zogenaamd product 'voor tweeërlei gebruik' ('*dual use*'), te weten burgerlijk en/of militair, waarvan de uitvoer is onderworpen aan de controlemaatregelen zoals voorzien in de richtlijnen 1334/2000 en 428/2009 van de Raad van de Europese Unie.

97 'Treaty on the non-proliferation of nuclear weapons', zie: www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglishText.pdf.

98 Het Comité bevroeg hierbij niet alleen de VSSE, maar ook twee belangrijke actoren op het vlak van de uitvoering van het Belgische non-proliferatiebeleid, te weten Théo Van Rentergem, voorzitter van de Commissie van advies voor de niet-verspreiding van kernwapens (CANVEK) en Werner Bauwens, speciaal gezant voor ontwapening en non-proliferatie van de FOD Buitenlandse Zaken. Het eindverslag werd goedgekeurd in november 2013.

99 VAST COMITÉ I, *Activiteitenverslag 2005*, 8-27.

100 VAST COMITÉ I, *Activiteitenverslag 2011*, 37-40.

sommige transacties met één of meerdere gevoelige landen wel aandachtig had gevolgd, maar dat deze opvolging voornamelijk reactief en *ad hoc* was: ze vond slechts plaats in functie van informatie die door buitenlandse inlichtingendiensten werd aangeleverd. Positief was evenwel dat de VSSE niet alleen oog had voor de veiligheidsbelangen in verband met de ontwikkeling van chemische, bacteriologische of nucleaire wapens, maar ook voor de problematiek van de mededinging en voor signalen die wezen op mogelijke buitenlandse inmenging.[101] Hierbij was het Comité, net zoals de VSSE, van oordeel dat in de strijd tegen proliferatie het veiligheidsbelang voorrang moet krijgen op het economisch belang van een onderneming.

II.5.2. DE VASTSTELLINGEN

Via het secretariaat van de Commissie van advies voor de niet-verspreiding van kernwapens (CANVEK)[102], kreeg de VSSE op 1 februari 2011 kennis van de geplande uitvoer van een isostatische warmtepers. Het dossier stond immers geagendeerd op de eerstvolgende vergadering van de CANVEK, en daarin zetelt een analist van de VSSE. De VSSE verwonderde er zich over dat zij niet eerder door de firma zelf op de hoogte was gesteld van de voorgenomen uitvoer. Immers, in januari 2011 had de dienst tot tweemaal toe contact met een kaderlid van de firma en dit net met de bedoeling om informatie uit te wisselen over eventuele delicate dossiers die aan de CANVEK zouden worden voorgelegd. Deze contacten wezen er volgens het Comité op dat de VSSE ondertussen een meer proactieve houding had aangenomen tegenover de betrokken firma. Maar aangezien deze laatste *in casu* had nagelaten de VSSE in kennis te stellen, was de opvolging in dit dossier opnieuw reactief.

Onmiddellijk nadat de VSSE kennis had gekregen van de geplande transactie, werden enkele verificaties verricht bij buitenlandse partnerdiensten. De informatie van deze correspondenten alsook de contextuele elementen uit een open bronnenanalyse, resulteerden in een synthesenota over de situatie bij de firma. Deze nota werd begin 2011 verzonden naar de minister van Justitie.

In maart 2011 verzond de VSSE ook twee geclassificeerde nota's naar de CANVEK en naar de FOD Economie. Daarin zette de dienst de elementen uiteen die er op wezen dat de eindgebruiker van de warmtepers in verband kon worden

---

101 De analyses van de VSSE hebben doorgaans betrekking op zowel de bescherming van het wetenschappelijk en economisch potentieel als op proliferatie. Het is echter niet de taak van de CANVEK om rekening te houden met de economische aspecten verbonden aan de dossiers die haar worden voorgelegd.

102 Zie meer over de samenstelling en de bevoegdheden van deze Commissie: Koninklijk besluit van 12 mei 1989 betreffende de overdracht aan niet-kernwapenstaten van kernmaterialen, kernuitrustingen, technologische kerngegevens en hun afgeleiden (*BS* 15 juni 1989) en het Huishoudelijk reglement van de Commissie voor advies voor de niet-verspreiding van kernwapens (*BS* 8 februari 2010).

gebracht met een entiteit die in het verleden betrokken was bij een militair nucleair programma.

Op de vergaderingen van de CANVEK liet de VSSE verstaan dat het om een delicaat exportdossier ging. In haar voorzichtige en genuanceerde analyse formuleerde zij vooral hypothesen en vermoedens, en dit bij gebrek aan nauwkeuriger informatie.[103] Uit elementen die door andere commissieleden werden aangedragen, bleek dat de overheden van het land van bestemming terughoudend waren om bijkomende inlichtingen te verstrekken en om na de levering van de isostatische pers ter plaatse een inspectie te laten uitvoeren.

Gelet op de twijfels omtrent de definitieve bestemmeling van de warmtepers en de controle op het gebruik ervan, verleende de CANVEK op 16 juni 2011 weliswaar een gunstig exportadvies, maar onder de voorwaarde dat de klant bijkomende uitleg zou verschaffen en dat de overheden van het betrokken land garanties konden geven aangaande een inspectiebezoek.

Omdat hij eveneens van mening was dat de betrokken buitenlandse overheden onvoldoende garanties boden betreffende het bezoek ter plaatse, weigerde de bevoegde minister de uitvoervergunning. Hij zond zijn dossier – waarin hij ook het advies liet opnemen dat hij ontvangen had van een buitenlandse overheid – terug naar de CANVEK.

De VSSE vroeg de betrokken correspondent bijkomende inlichtingen over het advies dat de buitenlandse overheid bij de bevoegde minister had laten toekomen.[104] Het antwoord dat de dienst kreeg, was echter zeer 'minimalistisch'. Het liet de VSSE niet toe haar oorspronkelijke analyse aan te vullen of te verfijnen.

In augustus 2011 zou de buitenlandse klant alsnog hebben ingestemd met een onvoorwaardelijk recht van toegang tot de warmtepers. Maar aangezien geen enkele Belgische overheid zich ertoe kon verbinden dit inspectiebezoek ter plaatse uit te voeren, verleende de CANVEK op 17 oktober 2011 een ongunstig advies voor de uitvoer.

De VSSE verklaarde dat de informatie die de buitenlandse overheid rechtstreeks naar de bevoegde minister had gezonden, een doorslaggevende rol heeft gespeeld in de herziening van het advies van de CANVEK. Alhoewel de VSSE de mogelijkheid van een protectionistische reflex vanwege een buitenlandse overheid nooit uitsluit wanneer dat land concurrerende ondernemingen of industrieën heeft, zag ze *in casu* geen poging tot beïnvloeding van de economische

---

103 Volgens de directeur van de CANVEK bevatten de nota's die de VSSE aan de CANVEK overzendt, doorgaans voornamelijk hypothesen en vermoedens en slechts zelden vaststaande feiten. Het is dan ook vrij moeilijk om er formele motiveringen voor haar adviezen uit te puren. Dat er doorgaans geen zekerheden kunnen meegedeeld worden, heeft vele oorzaken. De VSSE wees op de zeer hoge techniciteit van de materie, de complexiteit van de bevoorradingsnetwerken, de moeilijkheid om precieze en actuele informatie over de lopende programma's te verkrijgen, het gebrek aan toegang tot de financiële gegevens van deze netwerken en dit tegenover de beperkte menselijke middelen die zij in deze kan inzetten.

104 Nadien omschreef de VSSE dit advies als '*laconiek en negatief*'.

mededinging. Het negatieve advies zou veeleer ingegeven zijn door een algemeen wantrouwen van deze buitenlandse regering ten aanzien van bepaalde exporttransacties naar het betrokken land en door het feit dat de Belgische overheden geen effectieve controle konden uitvoeren bij de eindgebruiker. Ook benadrukte de VSSE dat zij niet anders kan dan een beroep te doen op de betrokken buitenlandse inlichtingendienst, meer bepaald wanneer ze onderzoek voert naar een buitenlandse vennootschap in een gereputeerde hoogtechnologische sector. Voorts kwam de betrokken buitenlandse overheid voor op de '*Entity List*' van het Amerikaanse ministerie van Economische Zaken (*Department of Commerce*). Dit betekent dat, voor deze administratie, de export naar de betrokken entiteit onderworpen moet zijn aan strengere voorwaarden.

Het Vast Comité I concludeerde dan ook dat de VSSE in dit dossier geen disfunctie of onwettigheid kon aangewreven verweten worden.

Wel stelde het Comité zich de vraag of en hoe de invoering van een inspectiesysteem ter plaatse bij de eindgebruikers in het buitenland de analyse- en controlecapaciteiten zou kunnen versterken op het vlak van proliferatie van massavernietigingswapens in een internationale context. Ongeacht het bevoegdheidsniveau waar dit controlesysteem wordt ondergebracht (gewestelijk, federaal of zelfs Europees) mag een dergelijke opdracht niet worden verward met het bevorderen van de economische belangen van het land.

II.6. VERMEENDE STRAFBARE FEITEN VAN EEN BUITENLANDSE INLICHTINGENDIENST EN DE INFORMATIEPOSITIE VAN DE VSSE

In januari 2010 krijgt het Vast Comité I een korte mail. De auteur ervan – die een vreemde nationaliteit heeft – beweerde dat een buitenlandse regering de ontvoering van zijn gezin op buitenlands grondgebied had georganiseerd. Het Comité verklaarde zich evenwel onbevoegd omdat er geen aanknopingspunt bleek met zijn bevoegdheden. Wel bezorgde het een kopie van de mail aan de gerechtelijke overheden en de VSSE.

Begin december 2011 legt de man opnieuw klacht neer. Bij zijn aangifte voegt hij nu een klacht met burgerlijke partijstelling bij de onderzoeksrechter. Het Comité beslist nu wel een toezichtonderzoek te openen '*naar de informatiepositie van de VSSE ten aanzien van feiten aangegeven in een klacht van een buitenlands onderdaan aan de Belgische gerechtelijke overheden ten laste van agenten van een buitenlandse inlichtingendienst*'. Nieuwe elementen duidden immers op een link met zijn opdrachten. Het onderzoek werd opgestart in januari 2012 en begin februari 2013 afgerond.

De betrokkene was tewerkgesteld op een ambassade in het buitenland. In 2003 merkte hij, naar eigen zeggen, op dat verantwoordelijken van de ambassade

en personen die werkten voor de buitenlandse veiligheidsdiensten, geregeld contact hadden met figuren die een extremistische, zelfs gewelddadige, islam verdedigden. Omdat hij geen gehoor vindt bij zijn oversten, besluit hij de media in te lichten. Hij vraagt meteen ook politiek asiel aan en krijgt een verblijfsvergunning.

In oktober 2006 zouden hij en zijn gezin onder bedreiging naar Brussel zijn gebracht en van daaruit op een vlucht naar zijn vaderland zijn gezet.

De Veiligheid van de Staat was, via het Comité (*supra*), sinds midden januari 2010 op de hoogte van de beweerde feiten. Bovendien had de dienst eind januari ook een verslag ontvangen van de Belgische ambassadeur uit het vaderland van betrokkene, die kort daarvoor een contact met hem had. De ambassadeur sprak zich daarbij niet uit over de grond van de zaak, maar gaf te kennen dat het nuttig zou zijn dat de veiligheidsdiensten een onderzoek zouden instellen. De ambassadeur sloot immers niet helemaal uit dat het om een poging ging tot compromittering van de ambassade. De VSSE deed een aantal onderzoekverrichtingen[105] die resulteerden in een beknopt informatieverslag. Daarin werd geen conclusie getrokken over de geloofwaardigheid van het verhaal. Er werd ook niet geanalyseerd of deze zaak zou zijn opgezet om de Belgische diplomatie schade te berokkenen. De VSSE achtte het niet noodzakelijk een evaluatienota op te maken voor derden '*au vu de la maigreur et de la non pertinence en termes de renseignement des éléments récoltés*'. De ambassadeur in kwestie werd niet op de hoogte gehouden van het gevolg dat de VSSE aan zijn schrijven gaf. Volgens de VSSE was dit omdat de FOD Buitenlandse Zaken de dienst VSSE nooit 'officieel' bevraagd had.

Halverwege augustus 2011 weten betrokkene en zijn gezin het land te ontvluchten.

Eind oktober 2011 dient hij klacht in bij de onderzoeksrechter nopens feiten van ontvoering, vrijheidsberoving, slagen en verwondingen, gepleegd in het buitenland en voortgezet in België en dit tegen personen die vermoedelijk deel uitmaken van een buitenlandse inlichtingendienst. Wat later herhaalt hij zijn klacht, maar dan voor het Vast Comité I.

In de loop van februari 2012 en pas na door het Comité op de hoogte te zijn gebracht van de opening van een toezichtonderzoek en de klacht bij de onderzoeksrechter, nam de VSSE contact op met het bevoegde parket. Het parket bleek nog geen kennis te hebben van bewuste klacht.

In april 2012 ging de VSSE over tot nieuwe verificaties, die evenwel geen bewijs opleverden.

De VSSE beschouwde deze zaak in alle opzichten als zeer ongeloofwaardig. De documenten en informatie die de betrokkene bezorgde evenals de formulering ervan en de manier van verzending gaven aanleiding tot ernstige twijfel over hun waarachtigheid. Ook de vanwege de buitenlandse correspondent verkregen

[105] Raadpleging van open bronnen, een vraag om informatie naar een corresponderende buitenlandse dienst, een verificatie (die negatief bleek gezien betrokkene in 2010 nog niet bekend was bij de VSSE) …

informatie leverde volgens de VSSE geen relevante elementen op die een grondige analyse en het meedelen van informatie aan een Belgische of buitenlandse partner hadden gerechtvaardigd.

Bijgevolg besloot de VSSE dat deze zaak niet relevant was in het kader van inlichtingenwerk: "*En définitive, la dénonciation d'un enlèvement, comme le dépôt d'une plainte en justice sont des dossiers judiciaires et policiers qui ne relèvent pas de la compétence légale de la VSSE.*"

Het Vast Comité I trad de positie van de VSSE in die zin bij dat de behandeling van een gerechtelijk of politioneel dossier uiteraard niet behoort tot de bevoegdheid van de dienst. Maar wanneer de gelaakte feiten verband houden met een van de wettelijk op te volgen dreigingen (*in casu* inmenging) is de opvolging ervan wél pertinent in het kader van de inlichtingenopdracht. Het Comité was tevens van oordeel dat de VSSE – zelfs voorlopige – conclusies van haar analyses schriftelijk dient vast te leggen, en dit in het kader van elke reële of potentiële bedreiging waarvan ze, op welke wijze of van wie ook, kennis krijgt.

II.7. MOGELIJKE REPUTATIESCHADE DOOR UITLATINGEN VAN DE VSSE

Midden juli 2012 ontving het Vast Comité I een klacht van een particulier die actief was in de sector van de economische inlichtingengaring.[106] Hij beweerde dat de VSSE in de sector waar hij werkzaam was zijn reputatie besmeurde en dat dit nefaste gevolgen had bij de uitbouw van zijn professionele relaties. In september 2012 besliste het Vast Comité I hierop een toezichtonderzoek te openen '*naar de informatie die de VSSE eventueel heeft verspreid over een particulier*'.[107]

Het Comité stelde vast dat de klager en zijn handelsvennootschappen gekend waren bij de VSSE en dit in het kader van een algemeen onderzoek naar private inlichtingenbedrijven. Het onderzoek was gebeurd door de dienst die binnen de VSSE instaat voor de bescherming van het wetenschappelijk en economisch potentieel van het land (WEP). Het Comité oordeelde dat de belangstelling van de VSSE voor de activiteiten van economische inlichtingengaring van de klager, legitiem was. Het Comité zelf had de VSSE overigens eerder aanbevolen dergelijke activiteiten te bestuderen.[108]

Wel gaf de informatie waarover de VSSE beschikte geen aanleiding tot welke analyse dan ook die zou moeten aantonen welke bedreiging voor het WEP zou uitgaan van de activiteiten van de klager. De ingewonnen gegevens werden dus

106 Conform artikel 40 W.Toezicht vroeg de klager om zijn anonimiteit te waarborgen.
107 Het eindverslag werd goedgekeurd in april 2013.
108 VAST COMITÉ I, *Activiteitenverslag 2003*, 24 tot 115.

bewaard in het kader van algemene informatie die wordt ingezameld over private inlichtingenbedrijven die actief zijn in België. Er werd ook geen enkel informatierapport noch enige analyse betreffende de activiteiten van de klager bezorgd aan derden.

Het Comité besloot verder dat de elementen die aan de basis lagen van de klacht, geenszins konden aangetoond worden.

II.8. VERMEENDE ONRECHTMATIGE VERSPREIDING VAN PERSOONSGEGEVENS DOOR DE VSSE

II.8.1. DE AANLEIDING

Halverwege oktober 2012 dient een particulier een klacht in bij het Vast Comité I. De inhoud van diverse krantenartikels[109] deden betrokkene vermoeden dat de VSSE beschikte over 'een geheim dossier' over hem en hij stelde zich vragen bij de wijze waarop de journalisten hiervan in het bezit waren gekomen. De klager vroeg het Comité om een kopie van alle inlichtingen die de VSSE over hem zou hebben verzameld alsook om een onderzoek naar de leden van de VSSE, die volgens hem een misdrijf begingen door geclassificeerde informatie door te geven aan de media.

Het Comité besliste daarop in april 2013 een toezichtonderzoek te openen, dat begin september 2013 werd afgerond.

Het Vast Comité I was uiteraard niet bevoegd om aan de klager de inlichtingen te verstrekken waarover de VSSE eventueel zou beschikken. Hiervoor verwees het Comité naar de verschillende mogelijkheden zoals voorzien in de Wet van 11 april 1994 betreffende de openbaarheid van bestuur (WOB) en de Wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer (Privacywet).

Wel kon worden nagegaan of de VSSE daadwerkelijk een dossier had aangelegd over de betrokkene en of die informatie ter kennis van de pers was gekomen[110], of de VSSE daarmee afbreuk deed aan de rechten die de Grondwet en de wet aan de klager verlenen (meer bepaald het recht op eerbied voor het privéleven) en of de bekendmaking van de vermeende informatie afbreuk deed aan de efficiënte werking van de VSSE.

---

109 PLA, LVDK en GVV, *Het Laatste Nieuws*, 22 september 2012 (Niet te temmen); JDB en JVC, *Het Nieuwsblad*, 24 september 2012 (Kopstuk Sharia4Belgium werkte even op Vlaams Kabinet).

110 Bijvoorbeeld bij toepassing van artikel 19, 2de lid van de W.I&V die de voorwaarden bepaalt inzake mededeling aan de pers van inlichtingen door de administrateur-generaal van de VSSE of door een ongepaste mededeling die strijdig zou zijn met de classificatieregels (W.C&VM).

II.8.2. ONDERZOEKSVASTSTELLINGEN

Het onderzoek wees uit dat de VSSE inderdaad – meestal 'vertrouwelijk' geclassificeerde – inlichtingen over de klager had verzameld en bewaard. Hij was bij de VSSE gekend aangezien hij in februari 2006 de aandacht had getrokken. Bovendien deelde de klager zijn (extremistische) overtuigingen en engagement op zijn *blog*. De betrokkene maakte er geen geheim van dat hij actief was binnen *Sharia4Belgium*, waarvan hij zichzelf als woordvoerder profileerde. De VSSE was dan ook de mening toegedaan dat het zeer verontrustende gedrag van de klager moest worden opgevolgd.

Het Comité vond deze opvolging gerechtvaardigd vanuit de wettelijke opdracht van de dienst die er meer bepaald in bestaat inlichtingen in te winnen, te analyseren en te verwerken die betrekking hebben op elke activiteit die de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde bedreigt of zou kunnen bedreigen.[111]

De VSSE verklaarde over de klager geen inlichtingen aan de pers te hebben meegedeeld. Buiten de verklaringen van de klager zelf vond het Comité geen enkele aanwijzing op basis waarvan kon worden bewezen of verondersteld dat een dergelijke mededeling zou hebben plaatsgevonden. Aangezien de klager zelf naar buiten trad in de media en op sociale netwerken, was het voor de pers niet moeilijk om aanwijzingen te vinden van zijn engagement binnen Sharia4Belgium. Bij gebrek aan aanwijzingen over de eventuele onrechtmatige verspreiding van (persoons)gegevens, besloot het Vast Comité I dan ook dat de VSSE geenszins afbreuk had gedaan aan de rechten die de Grondwet en de wet aan de klager verlenen.

II.9. KLACHT OVER DE ONTVREEMDING VAN EEN LAPTOP

Begin 2013 ontving de voorzitster van de Senaat een e-mail van een persoon die meldde dat zijn laptop in de loop van 2007 was ontvreemd. Hij wenste te weten of de diefstal destijds mogelijks werd gepleegd door een Belgische inlichtingendienst. De voorzitster vroeg hierop aan het Vast Comité I om een onderzoek te openen.

De klager, die als journalist actief was, schreef in de periode 2006-2007 enkele artikels over de situatie in Congo. Naar eigen zeggen werden die publicaties hem niet in dank afgenomen; hij zou er meermaals over zijn aangesproken door diverse politici. Wanneer bij hem – maar ook bij een van de in zijn artikels vermelde personen – een computer verdwijnt, doet hij daarvan aangifte bij de politie.[112] Op dat

[111] In dit verband deed het Vast Comité I ook opmerken dat de klager op 29 augustus 2013 onder aanhoudingsbevel werd geplaatst wegens het uiten van 'schriftelijke bedreigingen' ten aanzien van meerdere personen. Begin januari 2014 werd hij veroordeeld door de correctionele rechtbank van Antwerpen.

[112] Naar alle waarschijnlijkheid werd dit strafonderzoek zonder gevolg geklasseerd.

moment uit hij evenwel geen enkele verdenking met betrekking tot de mogelijke dader(s). Pas veel later geraakt hij ervan overtuigd dat een Belgische inlichtingendienst mogelijks achter de diefstal zit: een verklaring van zijn advocaat en van een derde waarvan de klager vermoedde dat hij goede banden had met een buitenlandse inlichtingendienst, deden hem hiertoe besluiten. Wanneer de pers begin 2013 gewag maakt van de opvolging van politieke verantwoordelijken door de VSSE (zie Hoofdstuk II.2), sluit hij niet uit dat ook journalisten het voorwerp zouden kunnen zijn van een bijzondere aandacht vanwege de inlichtingendiensten…

Het Vast Comité I was niet bevoegd om zich te buigen over de strafrechtelijke kant van de zaak. Het is evenwel zijn taak om klachten en aangiften over de werking, het optreden, het handelen of het nalaten te handelen van de inlichtingendiensten te behandelen. Vandaar dat het Comité de ADIV en de VSSE bevraagd heeft.

De ADIV kende de klager alleen als auteur van de vermelde persartikels.

Ook de VSSE beschikte over de persartikels omdat ze handelden over een materie die tot haar wettelijke bevoegdheid behoort en die zij opvolgt. De klager zelf maakte echter nooit het voorwerp uit van bijzondere aandacht door deze dienst. Wel had de VSSE weet van het verdwijnen van de laptop. Er werd hieromtrent zelfs een kort rapport opgesteld, zonder verdere analyse en/of commentaar.

Het Comité besloot dat de klager eind 2007 door zijn artikels een beperkte, passieve aandacht had genoten van beide inlichtingendiensten. Tevens werd geen enkel element aangetroffen dat kon wijzen op enige betrokkenheid van de ADIV noch van de VSSE bij deze feiten.[113]

II.10. TUSSENTIJDSE VERSLAGEN IN DE ONDERZOEKEN NAAR AANLEIDING VAN DE SNOWDEN-ONTHULLINGEN

De onthullingen van de Amerikaanse klokkenluider Edward Snowden vormden het startschot van diverse toezichtonderzoeken (cf. II.11.11). Het Vast Comité I kon deze onderzoeken, gezien hun complexiteit en de impact van de onthullingen, in 2013 niet afronden.

Wel werd, in het kader van zijn toezichtonderzoek '*naar de informatiepositie van de Belgische inlichtingendiensten ten aanzien van de mogelijkheden van bepaalde staten tot massale data-captatie en –mining en van de wijze waarop deze staten aan politieke spionage zouden doen van zogenaamde 'bevriende landen*'', een uitgebreid tussentijds verslag afgerond en overgezonden naar de bevoegde overheden. Het tussentijds verslag bevat in essentie de open bronnen-analyse van drs. Mathias Vermeulen[114] die het Vast Comité I als deskundige had ingeschakeld op basis van arti-

113 Het toezichtonderzoek werd afgerond in oktober 2013.

114 *Research Fellow* aan het European University Institute (EUI) in Firenze en het Centre for Law, Science and Technology Studies aan de VU Brussel.

kel 48 § 3 W.Toezicht. Zijn werk resulteerde in de studie '*De Snowden-revelaties, massale data-captatie en politieke spionage*'. Het expertenverslag werd voorafgegaan door een inleiding van het Vast Comité I waarbij de Snowden-onthullingen in een breder kader werden geplaatst. Dit moest toelaten om het verslag van de expert beter te begrijpen. Omwille van het belang van het toezichtonderzoek werd het tussentijds verslag als Bijlage D van voorliggend activiteitenverslag opgenomen.

Een tweede toezichtonderzoek[115] naar aanleiding van de Snowden-onthullingen behandelt onder meer de in België geldende (inter)nationale rechtsregels ter bescherming van de privacy ten aanzien van middelen die toelaten om op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren. Ook in het kader van dit onderzoek deed het Vast Comité I beroep op de inbreng van een experte (Prof. Annemie Schaus, Université Libre de Bruxelles). Haar '*Advies over de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren*' werd eveneens opgenomen in bijlage van onderhavig activiteitenverslag.

II.11. TOEZICHTONDERZOEKEN WAAR IN DE LOOP VAN 2013 ONDERZOEKSDADEN WERDEN GESTELD EN ONDERZOEKEN DIE IN 2013 WERDEN OPGESTART

Dit onderdeel bevat een opsomming en een korte situering van alle in 2013 opgestarte onderzoeken alsook van die onderzoeken waaraan tijdens het werkingsjaar 2013 werd verder gewerkt maar die nog niet konden worden afgerond.

II.11.1. DE OPVOLGING VAN EXTREMISTISCHE ELEMENTEN IN HET LEGER

Naar aanleiding van briefings gegeven door de ADIV in de loop van 2012, nam het Vast Comité I kennis van de problematiek van militairen die zich binnen extremistische kringen bewegen en militairen die lid of sympathisant zijn van motorbendes. In diezelfde periode maakte de media gewag van de (tijdelijke) aan-

115 Toezichtonderzoek '*naar de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren*'. De onderzoeksresultaten werden midden februari 2014 voorgelegd aan de Senatoriële Begeleidingscommissie en aan de bevoegde ministers.

wezigheid van een militant-djihadist bij het Bataljon Ardense Jagers, die met de opgedane ervaring gevechtshandboeken zou hebben opgesteld. Het Comité besloot dan ook een toezichtonderzoek te openen naar '*de opsporing en de opvolging door de ADIV van extremistische elementen bij het personeel van Defensie en de Krijgsmacht*'. Het onderzoek wil nagaan of de ADIV deze problematiek op een efficiënte wijze aanpakt en of de dienst hierbij de rechten van de burgers respecteert.

In de loop van het onderzoek werd de regelgeving met betrekking tot de verificatie of zogenaamde *screening* van kandidaat-leden van Defensie gewijzigd. Er werd beslist het onderzoek uit te breiden tot die materie zodat de aandacht van het onderzoek komt te liggen op twee processen: het screeningsproces gedurende de rekruteringsfase en het detectieproces en de opvolging van radicale of extremistische elementen die reeds eerder werden gerekruteerd.

II.11.2. DE VSSE EN HAAR WETTELIJKE OPDRACHT VAN PERSOONSBESCHERMING

In de marge van het '*gemeenschappelijk toezichtonderzoek naar de dreigingsevaluaties van het OCAD inzake buitenlandse VIP's op bezoek in België*'[116], werden vragen gesteld met betrekking tot de beschikbaarheid van de VSSE bij het uitvoeren van bepaalde beschermingsopdrachten. De VSSE riep hiervoor meermaals dwingende redenen van overbelasting en gebrek aan middelen in.

Daarop besliste het Vast Comité I een toezichtonderzoek te openen waarin wordt bestudeerd of de Veiligheid van de Staat haar persoonsbeschermingsactiviteiten conform de wet invult en of zij daarbij doelmatig te werk gaat.

De als 'GEHEIM – Wet 11.12.1998' geclassificeerde versie van het eindrapport werd eind december 2013 aan de administrateur-generaal van de VSSE voorgelegd. Dit moest toelaten om bemerkingen en toevoegingen te maken die de volledigheid en duidelijkheid van de rapportage ten goede komen. Het onderzoek werd begin 2014 afgerond en besproken in de Begeleidingscommissie van de Senaat.

II.11.3. DE WIJZE VAN BEHEER, BESTEDING EN CONTROLE VAN DE SPECIALE FONDEN

In 2011-2012 werden door de gerechtelijke overheden twee strafonderzoeken opgestart naar het eventuele misbruik van gelden bestemd voor de vergoeding van informanten. De Dienst Enquêtes I werd vanuit zijn gerechtelijke opdracht ingeschakeld in beide onderzoeken (zie Hoofdstuk VI). Gezien de elementen

116 VAST COMITÉ I, *Activiteitenverslag 2012*, 35-37.

waarover het Vast Comité I kon beschikken op mogelijke structurele problemen wezen, werd begin september 2012 beslist een thematisch onderzoek te openen naar '*de wijze van beheer, besteding en controle van de fondsen bestemd voor de vergoeding van informanten van de VSSE en de ADIV*'.

Gelet op de lopende strafonderzoeken, werd het toezichtonderzoek echter meteen opgeschort. Eind maart 2014 werd besloten dat het toezichtonderzoek kon worden heropgestart.

II.11.4. TOEZICHTONDERZOEK NAAR DE JOINT INFORMATION BOX

De oprichting van een zogenaamde *Joint Information Box* (JIB) – goedgekeurd door het Ministerieel Comité voor inlichting en veiligheid – vormde volgens de initiatiefnemers het speerpunt van het 'Actieplan Radicalisme'. Het betreft een werkbestand dat werd ingeplant bij het OCAD, en dat de '*structurele verzameling van informatie over entiteiten die in het kader van het Actieplan Radicalisme worden opgevolgd*' tot doel heeft.

In een gezamenlijke vergadering van de Vaste Comités P en I van midden november 2012 werd beslist een toezichtonderzoek te openen '*over de wijze waarop het OCAD de informatie, opgeslagen in de Joint Information Box (JIB) beheert, analyseert en verspreidt, overeenkomstig de uitvoering van het Plan Radicalisme*'.

In 2013 werden door beide Enquêtediensten P en I diverse onderzoekverrichtingen gesteld en een eerste syntheserapport opgesteld.

II.11.5. INLICHTINGENAGENTEN EN SOCIALE MEDIA

Eind november 2012 berichtte de media over profielen van medewerkers van de inlichtingendiensten op sociale netwerksites als *Facebook* en *LinkedIn*. Dienvolgens verzocht de Senatoriële Begeleidingscommissie het Vast Comité I een toezichtonderzoek te openen naar '*wat de omvang is van het fenomeen dat medewerkers van de Veiligheid van de Staat, maar eventueel ook van de ADIV en OCAD, zich hun hoedanigheid van agent van die instellingen bekend maken op Internet via sociale media*'. Tevens diende het Comité na te gaan welke risico's dergelijke bekendmaking met zich kan brengen en in welke mate hiertegen maatregelen kunnen en mogen genomen worden.

Het Vast Comité I nam in december 2012 een aanvang met zijn toezichtonderzoek met betrekking tot de medewerkers van de ADIV en de VSSE. Diverse onderzoekdaden werden verricht. Het eindrapport zal in 2014 gefinaliseerd worden.

II.11.6. PERSONEELSLEDEN VAN HET OCAD EN SOCIALE MEDIA

Wat betreft het luik met betrekking tot de medewerkers van het OCAD en hun aanwezigheid op sociale netwerksites, werd begin 2013 ook een gemeenschappelijk toezichtonderzoek opgestart met het Vast Comité P. Immers, ingevolge artikel 56, 6° W.Toezicht wordt de externe controle op de werking van het OCAD waargenomen door beide Comités gezamenlijk.

Ook dit verslag kan in 2014 worden afgerond.

II.11.7. DE INFORMATIEPOSITIE VAN DE INLICHTINGENDIENSTEN EN VAN HET OCAD MET BETREKKING TOT EEN LEERLING-PILOOT

In juli 2012 verschenen diverse persartikels waarin geciteerd werd uit een toezichtonderzoek van het Vast Comité P naar '*informatiestromen op de luchthavens*'. Er werd onder meer verwezen naar een persoon die een pilotenopleiding kon volgen op een Belgische luchthaven, alhoewel hij een verleden had dat mogelijks wees op radicalisering. Dit voorbeeld kon wijzen op een gebrekkige informatie-uitwisseling tussen de diverse politiediensten op de luchthavens. Na kennisname van het rapport door het Vast Comité I, werd in juni 2013 beslist een gemeenschappelijk toezichtonderzoek te openen '*betreffende de informatiepositie en de opvolging door de ondersteunende diensten van het OCAD – alsook naar de evaluatie van de dreiging door het OCAD – betreffende een particulier X die toelating verkreeg om een cursus als vliegtuigpiloot te volgen in België*'.

Het onderzoek bevindt zich in de eindfase.

II.11.8. EEN KLACHT VAN DE SCIENTOLOGYKERK TEGEN DE VEILIGHEID VAN DE STAAT

In de loop van januari en februari 2013 verschenen diverse krantenartikelen waarin wordt vermeld dat de Veiligheid van de Staat zou nagaan of en wanneer politici contact hebben met organisaties zoals de Scientologykerk (zie II.2). Daarbij wordt geciteerd uit een geclassificeerde nota en uit de 'Fenomeenanalyse van niet-staatsgestuurde inmengingsactiviteiten' van de VSSE. In maart 2013 besluit de Scientologykerk klacht neer te leggen bij het Vast Comité I. Het Comité besliste een toezichtonderzoek te openen over de wijze waarop de Veiligheid van de Staat een rapport, haar betreffend, opgesteld en verspreid heeft. In 2013 werden de meeste onderzoeksverrichtingen afgerond. Het eindverslag werd gefinaliseerd midden 2014.

II.11.9. DE INTERNATIONALE CONTACTEN VAN HET OCAD

Een van de opdrachten van het Coördinatieorgaan voor de dreigingsanalyse bestaat er in contacten te onderhouden met 'gelijkaardige buitenlandse of internationale diensten' (art. 8, 3° W. OCAD). In zijn gezamenlijke vergadering van begin mei 2013 besloten de Vaste Comités I en P een onderzoek te voeren naar de wijze waarop het OCAD die opdracht invult.[117] In 2013 werden alle betrokken actoren uitvoerig bevraagd.

II.11.10. TOEZICHTONDERZOEK NAAR DE ELEMENTEN DIE DE VSSE VERSCHAFTE IN HET KADER VAN EEN NATURALISATIEDOSSIER

Een procureur des Konings verzette zich tegen de verlening van de Belgische nationaliteit van een particulier, daarbij verwijzend naar informatie van de VSSE aangaande '*gewichtige feiten eigen aan de persoon*'. Deze informatie zou een beletsel vormen voor zijn naturalisatie. De betrokkene was daarbij van oordeel dat hij het slachtoffer was van een misverstand dat leidde tot een inbreuk op zijn individuele rechten door de Veiligheid van de Staat. Eind juli 2013 diende de man klacht in bij het Vast Comité I. Het Comité opende daarop een toezichtonderzoek dat in februari 2014 werd gefinaliseerd.

II.11.11. KLACHT OVER DE WIJZE WAAROP DE VSSE EEN ZAAKVOERDER VAN EEN BELGISCH EXPORTBEDRIJF OPVOLGT

Naar aanleiding van een klacht, opende het Vast Comité I begin oktober 2013 een toezichtonderzoek '*naar de wijze waarop de VSSE een zaakvoerder van een Belgische onderneming, die over specifieke gegevens beschikt over uitvoer naar Iran, benadert en bejegent*'. Diverse onderzoekverrichtingen werden uitgevoerd; de klager alsook vertegenwoordigers van de betrokken inlichtingendienst werden verschillende malen gehoord. Het onderzoek zal in de loop van 2014 worden afgerond.

[117] 'Gemeenschappelijk toezichtonderzoek over de wijze waarop het OCAD internationale relaties onderhoudt met gelijkaardige buitenlandse of internationale diensten in toepassing van artikel 8, 3° van de W.OCAD van 10 juli 2006'.

II.11.12. VIER TOEZICHTONDERZOEKEN IN HET KADER VAN DE SNOWDEN-ONTHULLINGEN

Op 6 juni 2013 publiceerden *The Guardian*[118] en *The Washington Post*[119] informatie uit de tienduizenden (geclassificeerde) documenten die door Edward Snowden, die verschillende functies heeft vervuld in of voor Amerikaanse inlichtingendiensten, waren gelekt. Sindsdien volgden nieuwe onthullingen elkaar snel op.

De berichten gaven een inkijk in uitermate geheime programma's van voornamelijk de Amerikaanse *National Security Agency* (NSA). Ze onthulden onder meer het bestaan van het zogenaamde PRISM-programma waarbij de NSA (meta) data van telecommunicatie verkrijgt en brachten aan het licht dat Amerikaanse maar ook Britse diensten inlichtingenoperaties hebben opgezet ten aanzien van bepaalde internationale instellingen en samenwerkingsverbanden (VN, EU en G20) waarbij ook zogenaamde 'bevriende landen' werden geviseerd.

Deze onthullingen waren het startschot voor vele (parlementaire, gerechtelijke en inlichtingen) onderzoeken over heel de wereld. Zo ook in België. Op 1 juli 2013 vroeg de Begeleidingscommissie van de Senaat aan het Vast Comité I '*[…] een update van de bestaande informatie over de praktijken op het vlak van datamining. Niet alleen de Amerikaanse inlichtingendienst NSA zou dit doen, maar ook het Verenigd Koninkrijk zou massaal gegevens onderscheppen en analyseren. In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, en van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen.*'

Het Vast Comité I heeft daarop drie toezichtonderzoeken geopend die uiteraard nauw met elkaar verweven zijn. Dit geldt ook voor een vierde onderzoek[120] dat werd geïnitieerd na klacht van de voorzitter van de Nederlandse Orde van advocaten bij de Balie van Brussel.

Het eerste toezichtonderzoek[121] – dat begin 2014 in de Begeleidingscommissie van de Senaat werd besproken – biedt een antwoord op volgende vragen:

– over welke mogelijkheden beschikken grootmachten als de Verenigde Staten en Groot-Brittannië om op grote schaal gegevens van in België verblijvende

---

118 G. GREENWALD en E. MACASKILL, *The Guardian*, 6 juni 2013 (NSA Taps in to Internet Giant's Systems to Mine User Data, Secret files Reveals).

119 B. GELLMAN en L. POITRAS, *The Washington Post*, 6 juni 2013 (US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program).

120 'Toezichtonderzoek ingevolge een klacht van een stafhouder naar het gebruik van informatie afkomstig van massale buitenlandse data-captatie in Belgische strafzaken'.

121 'Toezichtonderzoek naar de informatiepositie van de Belgische inlichtingendiensten ten aanzien van de mogelijkheden van bepaalde staten tot massale data-captatie en –mining en van de wijze waarop deze staten aan politieke spionage zouden doen van zogenaamde 'bevriende lan-

personen, organisaties, ondernemingen of instanties (of die een link hebben met België) te onderscheppen en te exploiteren en over welke gegevens gaat het (zowel kwantitatief als kwalitatief)?
- in welke mate waren de Belgische inlichtingendiensten op de hoogte van de mogelijkheden van deze grootmachten (of in welke mate dienden ze er – gegeven hun wettelijke opdrachten – van op de hoogte te zijn)? Werden hierover inlichtingen gecollecteerd of werd dit niet wenselijk geacht? Bieden onze diensten voldoende bescherming ter zake?
- wat is de betekenis/waarde van de notie 'bevriende staat' in de context van inlichtingendiensten en in welke mate bepaalt die notie de houding van onze eigen inlichtingendiensten? Alhoewel dit aspect van de onthullingen (met name bepaalde operaties van inlichtingendiensten van zogenaamde 'bevriende landen' ten aanzien van internationale of supranationale instellingen waarin België vertegenwoordigd is of ten aanzien van Belgische belangen) niet expliciet in de vraagstelling van de Begeleidingscommissie was opgenomen, heeft het Vast Comité I beslist om ook hieraan aandacht te besteden, en dit gelet op het intrinsieke belang van deze vraag.

Het tweede toezichtonderzoek[122] – dat ook reeds werd besproken in de Senaatscommissie – behandelt de in België geldende (inter)nationale rechtsregels ter bescherming van de privacy ten aanzien van middelen die toelaten om op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren. Qua internationale regels was er daarbij uiteraard aandacht voor artikel 8 EVRM (waarbij zowel de 'horizontale werking' van deze bepalingen en de eventuele 'positieve verplichtingen' die eruit voortvloeien voor een Staat, belicht werden), artikel 17 van het Verdrag inzake burgerrechten en politieke rechter (BUPO-verdrag), Richtlijn 95/46/EC van 24 oktober 1995, Verdrag nr. 108 van 28 januari 1981 van de Raad van Europa en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie. Maar ook meer specifieke regels kwamen aan bod: de regels inzake *Passenger Name Record*, Swift, Safe Harbour … Ten slotte werden de interne rechtsregels die betrekking hebben op de privacybescherming en dataprotectie, belicht: de Wet Verwerking Persoonsgegevens en haar uitvoeringsbesluit en de bepalingen die specifiek zijn voor de werking van inlichtingendiensten. Daarnaast biedt dit tweede toezichtonderzoek ook een overzicht van de juridische mogelijkheden waarover Staten, burgers of bedrijven

den'. De onderzoeksresultaten werden midden april 2014 besproken met de Senatoriële Begeleidingscommissie en voorgelegd aan de bevoegde ministers.

122 Toezichtonderzoek 'naar de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren'. De onderzoeksresultaten werden midden februari 2014 voorgelegd aan de Senatoriële Begeleidingscommissie en aan de bevoegde ministers.

beschikken om actie te ondernemen tegen (mogelijke) inbreuken op (grond)rechten.

Het derde toezichtonderzoek[123] – dat nog niet werd gefinaliseerd – behandelt de mogelijke implicaties van data-mining op de bescherming van het wetenschappelijk en economisch potentieel van het land. Het wil nagaan of de Belgische inlichtingendiensten:

- aandacht hebben besteed aan dit fenomeen;
- een reële of mogelijke bedreiging hebben gedetecteerd voor het Belgische wetenschappelijk en economisch potentieel;
- er de bevoegde overheden van in kennis hebben gesteld en beschermingsmaatregelen hebben voorgesteld; en
- over voldoende en adequate middelen beschikken om deze problematiek op te volgen.

Het vierde onderzoek, opgestart na aangifte van een stafhouder, betreft voornamelijk het eventuele gebruik in strafzaken van gegevens die op massale (en illegale) wijze zijn gecapteerd.

123 Toezichtonderzoek 'over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgisch wetenschappelijk en economisch potentieel uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie- en informatiesystemen'.

HOOFDSTUK III
CONTROLE OP DE BIJZONDERE INLICHTINGENMETHODEN

Artikel 35 § 1, 1° W.Toezicht bepaalt dat het Comité in zijn jaarlijks activiteitenverslag *'specifiek aandacht [moet besteden] aan de specifieke en de uitzonderlijke methoden voor het verzamelen van gegevens, zoals bedoeld in artikel 18/2 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdiensten [en] aan de toepassing van hoofdstuk IV/2 van dezelfde wet'*.[124] Dit hoofdstuk behandelt dan ook de inzet van bijzondere inlichtingenmethoden door de beide inlichtingendiensten en de wijze waarop het Vast Comité I zijn jurisdictionele rol in deze waarneemt. Het vormt de verkorte weergave van de twee zesmaandelijkse verslagen die het Comité ten behoeve van zijn Begeleidingscommissie moet opstellen.[125] In deze zesmaandelijkse verslagen moet naast een aantal kwantitatieve gegevens (aantal machtigingen, duur van de methoden, betrokken personen), ook worden ingegaan op de door de BIM-methoden 'behaalde resultaten'. Omwille van het belang ervan hield het Comité er aan zijn analyse in dit verband verkort weer te geven in dit activiteitenverslag.

III.1. BEHAALDE RESULTATEN

'Although the financial costs of an intelligence operation are often tangible, the benefits that it produces are often intangible … This is especially true when the object of an operation is the non-occurrence of an event, such as a terrorist attack'.[126] Dit citaat vat meteen samen hoe moeilijk het is om in een inlichtingencontext te meten wat het behaalde resultaat is van een welbepaalde operatie of methode. Het probleem van het meten van 'resultaten' is trouwens niet eigen aan de inlichtingenwereld. Het geldt ook voor de gerechtelijke wereld wanneer die de resultaten van haar bijzondere opsporingsmethoden (BOM) wil meten. We stel-

124 Zie voor een bespreking van de bijzondere inlichtingenmethoden en de controle hierop: VAST COMITÉ I, Activiteitenverslag 2010, 51-63 en W. VAN LAETHEM, D. VAN DAELE en B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

125 Art. 35 § 2 en 66*bis* § 2, derde lid, W.Toezicht.

126 H. BORN en A. WILLS, *Overseeing Intelligence Services – A Toolkit*, DCAF, 2012.

len dan ook vast dat de gerechtelijke overheden dergelijke analyse niet opmaakt, ondanks de bewoordingen van artikel 90*decies* Wetboek van Strafvordering.[127]

Ondanks deze moeilijkheid heeft het Comité getracht een zicht te krijgen op het 'nut' van de ingezette BIM-methoden, vooreerst door een eenvoudige bevraging te houden bij de twee inlichtingendiensten zelf en vervolgens door een diepgaande analyse van vier omvangrijke casussen.

De bevraging bij de inlichtingendiensten had betrekking op 238 BIM-beslissingen en -machtigingen uit de periode van september 2010 tot december 2012, of met andere woorden op iets meer dan 9% van het totale aantal toelatingen.[128] Beide diensten werd de vraag gesteld hoe ze de doeltreffendheid van uitgevoerde methoden evalueerden in functie van de in de toelating beoogde doelstellingen. De VSSE was van mening dat in 84% van de gevallen alle beoogde doelstellingen bereikt werden, in 8,5% een deel van de doelstellingen, en in 7,5% geen van de doelstellingen. De ADIV gaf volgend antwoord: in 72% van de gevallen was de dienst van mening dat de alle beoogde doelstellingen bereikt werden, in 16% een deel van de doelstellingen, in 12% geen van de doelstellingen.

Voortbouwend op deze zelfevaluatie voerde het Comité een inhoudelijk onderzoek waarbij alle methoden die werden ingezet ten aanzien van vier verschillende 'targets' (zijnde een persoon of organisatie) in detail werden onderzocht. Voor elke target werd bekeken welke BIM-methoden opeenvolgend werden ingezet en wat dit inhoudelijk opleverde, dit in functie van de finaliteit van de methode (bijv. het netwerk van een persoon blootleggen of zekerheid bekomen over zijn betrokkenheid bij een dreiging). In totaal werden op de vier targets 160 methoden toegepast.

De eerste target was in totaal 18 maal het voorwerp van een BIM-methode. De behaalde resultaten lieten evenwel niet toe het vermoeden van de dienst te bevestigen, wel om het te versterken, onder andere omdat de dienst een beter zicht kreeg op het netwerk van de persoon. Dit was trouwens ook het vooropgestelde doel. De BIM-methoden leverden ter zake informatie op die met 'gewone' inlichtingenmethoden niet konden worden verkregen. Deze casus toonde ook aan dat de opvolging van de betrokkene werd gestart op aangeven van een buitenlandse inlichtingendienst. De bekomen informatie werd, overeenkomstig artikel 20 Wet I&V, met deze inlichtingendienst gedeeld.

---

127 *'Tot slot moet nog een opmerking gemaakt worden bij de weging van het 'resultaat' van de diverse maatregelen. In de praktijk blijkt het zeer moeilijk om 'het resultaat' van de diverse maatregelen enerzijds voldoende adequaat te definiëren en anderzijds het resultaat 'geïsoleerd' (per maatregel) na te gaan, gezien er (veelal) sprake is van parallel gebruik van verscheidene opsporings- en onderzoeksmethoden. Bovendien is het onmogelijk om het "resultaat" correct of minstens op afdoende wijze weer te geven zonder enige bijkomende informatie betreffende de context waarin de maatregelen aangewend werden en zonder informatie over de beoordeling door de bodemrechter.'* (Dienst voor het Strafrechtelijk beleid, *Verslag 2013 in uitvoering van artikel 90decies Wetboek van Strafvordering (2012), s.l.*, 6).

128 Waarvan voor de VSSE 94 specifieke en 71 uitzonderlijke methoden en voor de ADIV 48 specifieke en 25 uitzonderlijke methoden.

Een tweede target – een organisatie – was het voorwerp van 47 methoden. Om bloot te leggen wie met wie in contact staat, werd veelvuldig gewerkt met de identificatie van abonnees van elektronische communicatiemiddelen. Tevens hanteerde men de mogelijkheid om personen te lokaliseren aan de hand van hun telecommunicatie en werden ze geschaduwd. In deze casus kan gesteld worden dat globaal genomen de door de BIM-methoden vooropgestelde doelstellingen bereikt werden. Bovendien illustreerde deze casus ook zeer goed de samenhang tussen de 'gewone' methoden en de BIM-methoden, en de tussen de diverse BIM-methoden onderling waarbij de ene methode voortbouwde op de andere.

In een derde casus werden 79 BIM-methoden toegepast. Het merendeel betrof ook hier identificaties en lokalisaties. En ook hier werd de target door een partnerdienst 'aangebracht' bij de Belgische inlichtingendienst. De methoden hebben echter niet toegelaten te bevestigen dat deze persoon ook effectief een bedreiging vormde. Wel bleek hij contacten te hebben met personen die een reële bedreiging uitmaakten. Bovendien kon, via toegang tot bankgegevens, aangetoond worden dat bepaalde financiële stromen in de tijd samenvielen met sommige activiteiten van personen die eveneens in de kijker van de inlichtingendiensten liepen. Het Comité moest in dit dossier vaststellen dat de informatiepositie van de betrokken dienst al bij al niet in grote mate was versterkt, ondanks de inzet van 79-methoden.

De laatste casus berustte op 16 BIM-methodes die werden ingezet ten aanzien van een bepaalde organisatie. Het betrof voornamelijk de (langdurige) observatie met behulp van technische middelen en de inzage van bankgegevens. Het onderzoek had tot doel na te gaan wie tot het netwerk van de organisatie kon gerekend worden. Het Comité stelde vast dat de technische middelen die ingezet waren, soms defecten vertoonden, zodat de resultaten ontbraken. Daarenboven kon een deel van de bekomen gegevens (beeldmateriaal) bij gebrek aan tijd en mensen slechts gedeeltelijk worden verwerkt. De gegevens die wél geanalyseerd konden worden, werden verwerkt in vele tientallen inlichtingenrapporten. De studie van het Comité leerde dat de observaties en de analyse van de financiële gegevens zeker hebben bijgedragen tot de realisatie van het vooropgestelde doel.

III.2. CIJFERS MET BETREKKING TOT DE SPECIFIEKE EN UITZONDERLIJKE METHODEN

Tussen 1 januari en 31 december 2013 werden door de twee inlichtingendiensten samen 1378 toelatingen verleend tot het aanwenden van bijzondere inlichtingen-

methoden, 1224 door de VSSE (waarvan 1102 specifieke en 122 uitzonderlijke) en 154 door de ADIV (waarvan 131 specifieke en 23 uitzonderlijke).

Onderstaande tabel maakt een vergelijking met de cijfers van 2011 en 2012. Daarbij moet opgemerkt worden dat het Comité sinds januari 2013 een andere telling hanteert voor één welbepaalde bijzondere methode. Voorheen werden het aantal 'Kennisnames van identificatiegegevens van elektronisch communicatieverkeer' in voetnoot vermeld maar niet als dusdanig meegeteld in de totalen. Hiervoor werd geopteerd omdat (de meeste) 'Kennisnames van identificatiegegevens' door de diensthoofden van de inlichtingendiensten werden toegelaten in eenzelfde document waar ook bijvoorbeeld een 'Kennisname van de oproepgegevens' of een 'Kennisname van lokalisatiegegevens' werd toegelaten. Omdat het strikt genomen om andere methoden gaat, heeft het Vast Comité I geoordeeld dat het apart meetellen van dergelijke 'Kennisnames van identificatiegegevens' een juister beeld oplevert van het effectief aantal ingezette specifieke methoden. Met andere woorden: wanneer het in dit rapport vermelde aantal bijzondere methoden hoger ligt dan dezelfde periode van vorig jaar dan is dit grotendeels te wijten aan een andere manier van tellen en dus niet aan het feit dat er zoveel meer methoden werden aangewend. De impact van die nieuwe telwijze wordt meteen duidelijk in onderstaande tabel.

	ADIV		VSSE		TOTAAL
	Specifieke methode	Uitzonderlijke methode	Specifieke methode	Uitzonderlijke methode	
2011	60	7	731	33	831
2012	67	24	655	102	848
2013	131	23	1102	122	1378

De op het eerste gezicht uitgesproken stijging moet dus worden genuanceerd. Op basis van de telling zoals die gevoerd werd in de voorgaande jaren zou 2013 slechts 960 methoden hebben geteld. Er werden dus ten opzicht van 2012 ongeveer 13% meer BIM-methoden ingezet. Onderstaande tabellen maken duidelijk waar die stijging te situeren is.

In wat volgt, worden per dienst drie grote rubrieken onderscheiden: cijfers over de specifieke methoden, cijfers over de uitzonderlijke methoden en cijfers inzake de dreigingen en te verdedigen belangen die door de methoden geviseerd worden.

III.2.1. TOELATINGEN MET BETREKKING TOT DE ADIV

III.2.1.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	7	8	14
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	0	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	0	0	0
Kennisnemen van identificatiegegevens van elektronisch communicatieverkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	23 dossiers	25 dossiers	66 methoden[129]
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	17	30	15
Kennisnemen van lokalisatiegegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	13	4	36
TOTAAL	60	67[130]	131[131]

Wat betreft de specifieke methoden ingezet door de ADIV, toont de vergelijking met voorgaande jaren twee opvallende tendensen: het aantal observaties en lokalisaties is sterk toegenomen.

III.2.1.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	1	1
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	0	0	0

129 In vergelijking met vorige jaren is er een daling te noteren: de 66 toelatingen hebben immers betrekking op 16 dossiers.

130 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

131 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

AARD UITZONDERLIJKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	0	0	0
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	5	7	5
Binnendringen in een informaticasysteem	0	2	0
Afluisteren, kennisnemen en opnemen van communicaties	2	14	17
TOTAAL	7	24[132]	23[133]

III.2.1.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[134]

De ADIV mag de specifieke en de uitzonderlijke methoden aanwenden in het kader van drie van zijn opdrachten die elk op zich specifieke te vrijwaren belangen behelzen:

- de inlichtingenopdracht die gericht is op dreigingen tegen onder meer de onschendbaarheid van het nationaal grondgebied, de militaire defensieplannen en het wetenschappelijk en economisch potentieel op vlak van defensie (art. 11, 1° W.I&V);
- de opdracht inzake de militaire veiligheid die bijvoorbeeld gericht is op het behoud van de militaire veiligheid van het defensiepersoneel, van de militaire installaties en de militaire informatica- en verbindingssystemen (art. 11, 2° W.I&V);
- de bescherming van militaire geheimen (art. 11, 3° W.I&V).

AARD VAN DE OPDRACHT	AANTAL 2011	AANTAL 2012	AANTAL 2013
Inlichtingenopdracht	38	63	183
Militaire veiligheid	8	7	26
Bescherming geheimen	19	21	50

132 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

133 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

134 Per toelating kunnen meerdere belangen en dreigingen aan de orde zijn.

Anders dan voor de VSSE, staan de dreigingen waaraan de ADIV aandacht mag of moet besteden, niet in de wet omschreven. Toch vermeldt deze dienst in zijn toelatingen systematisch welke bedreiging wordt geviseerd. Dergelijke transparantie verdient inderdaad aanbeveling. De cijfers tonen aan dat, wat betreft de inzet van bijzondere methoden, de strijd tegen spionage de eerste prioriteit van de militaire inlichtingendienst is gebleven.

AARD DREIGING	AANTAL 2011	AANTAL 2012	AANTAL 2013
Spionage	54	78	157
Terrorisme (en radicaliseringsproces)	10	3	11
Extremisme	3	3	42
Inmenging	0	2	2
Criminele organisatie	0	1	28
Andere	0	5	29

III.2.2. TOELATINGEN MET BETREKKING TOT DE VSSE

III.2.2.1. De specifieke methoden

AARD SPECIFIEKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren op of in publiek toegankelijke plaatsen met een technisch middel	89	75	109
Betreden en doorzoeken van publiek toegankelijke plaatsen met een technisch middel	0	1	0
Kennisnemen van identificatiegegevens van postverkeer en vorderen medewerking postoperator	4	2	0
Kennisnemen van identificatiegegevens van elektronisch communicatie-verkeer; het vorderen van de medewerking van een operator; of de rechtstreekse toegang tot gegevensbestanden	355 dossiers	254 dossiers	613[135] methoden
Kennisnemen van oproepgegevens van elektronisch communicatieverkeer en het vorderen van de medewerking van een operator	237	147	136

[135] In vergelijking met vorige jaren is er een daling te noteren: de 613 toelatingen hebben immers betrekking op 243 dossiers.

AARD SPECIFIEKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Kennisnemen van lokalisatiegegevens van elektronisch communicatie-verkeer en het vorderen van de medewerking van een operator	46	176	244
TOTAAL	**731**	**655**[136]	**1102**[137]

Wat betreft de specifieke methoden, ingezet door de VSSE, toont de vergelijking met voorgaande jaren twee opvallende tendensen: het aantal observaties en lokalisaties is sterk toegenomen.

III.2.2.2. De uitzonderlijke methoden

AARD UITZONDERLIJKE METHODE	AANTAL 2011	AANTAL 2012	AANTAL 2013
Betreden van en observeren in niet publiek toegankelijke plaatsen met of zonder een technisch middel	2	8	6
Betreden en doorzoeken van niet publiek toegankelijke plaatsen met of zonder een technisch middel	3	6	6
Oprichten en gebruiken van een fictieve rechtspersoon	0	0	0
Openmaken en kennisnemen van al dan niet aan een postoperator toevertrouwde post	4	12	6
Verzamelen van gegevens betreffende bankrekeningen en bankverrichtingen	10	16	11
Binnendringen in een informaticasysteem	3	10	12
Afluisteren, kennisnemen en opnemen van communicaties	11	50	81
TOTAAL	33	102[138]	122[139]

De cijfers tonen opnieuw een opvallende stijging van het aantal tapmaatregelen: van 11 in 2011 over 50 in 2012 tegenover 81 in 2013. Voor de andere uitzonderlijke methoden werden geen significante verschillen vastgesteld.

136 In zeventien gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist. Vorig jaar betroffen het negen gevallen.

137 In negen gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist. Vorig jaar betroffen het negen gevallen.

138 In vijf gevallen had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

139 In één geval had de toelating betrekking op een van de beschermde beroepscategorieën, te weten een advocaat, arts of beroepsjournalist.

III.2.2.3. De belangen en dreigingen die de inzet van de bijzondere methoden rechtvaardigen[140]

De VSSE mag slechts optreden ter vrijwaring van volgende belangen:
- de inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde;
- de uitwendige veiligheid van de Staat en de internationale betrekkingen;
- de vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel.

AARD BELANG	AANTAL 2011	AANTAL 2012	AANTAL 2013
De inwendige veiligheid van de Staat en het voortbestaan van de democratische en grondwettelijke orde	694	704	1994
De uitwendige veiligheid van de Staat en de internationale betrekkingen	571	693	1965
De vrijwaring van de essentiële elementen van het wetenschappelijk of economisch potentieel	24	15	18

Volgende tabel geeft een beeld van de (potentiële) dreigingen die de VSSE viseerde bij de inzet van specifieke en uitzonderlijke methoden. Uiteraard kan één methode gericht zijn tegen meerdere dreigingen. De VSSE kan de specifieke methoden aanwenden in het kader van alle dreigingen die tot haar bevoegdheid behoren (art. 8 W.I&V). Uitzonderlijke methoden mogen niet ingezet worden in het kader van het extremisme en de inmenging. Zij zijn wel toegelaten in het kader van het aan het terrorisme voorafgaande radicaliseringsproces (art. 3, 15° W.I&V).

AARD DREIGING	AANTAL 2011	AANTAL 2012	AANTAL 2013
Spionage	193	243	561
Terrorisme (en radicaliseringsproces)	371	288	1086
Extremisme	319	177	602
Proliferatie	17	28	27
Schadelijke sektarische organisaties	4	7	15
Inmenging	3	10	27
Criminele organisaties	3	5	18

140 Per toelating kunnen meerdere belangen en dreigingen aan de orde zijn.

Deze cijfers tonen aan dat terrorisme en extremisme, maar ook spionage dé aandachtspunten blijven van de VSSE, minstens qua inzet van BIM-methoden.

III.3. DE ACTIVITEITEN VAN HET VAST COMITÉ I ALS JURISDICTIONEEL ORGAAN EN ALS PREJUDICIEEL ADVIESVERLENER INZAKE BIM-METHODEN

III.3.1. DE CIJFERS

Het Vast Comité I kan op vijf manieren worden gevat om zich uit te spreken over de wettelijkheid van bijzondere inlichtingenmethoden (art. 43/4 W.I&V):
- op eigen initiatief;
- op verzoek van de Commissie voor de bescherming van de persoonlijke levenssfeer;
- op klacht van een burger;
- van rechtswege als de BIM-Commissie een specifieke of een uitzonderlijke methode wegens onwettigheid heeft geschorst en de exploitatie van de gegevens heeft verboden;
- van rechtswege als de bevoegde minister een toelating heeft verleend op basis van artikel 18/10 § 3 W.I&V.

Daarnaast kan het Comité ook gevat worden in zijn hoedanigheid van 'prejudicieel adviesverlener' (art. 131*bis*, 189*quater* en 279*bis* Sv.). Desgevraagd geeft het Comité een advies over de al dan niet rechtmatigheid van aan de hand van specifieke of uitzonderlijke methoden ingewonnen inlichtingen die in een strafzaak worden gebruikt. De beslissing om een advies te vragen berust bij de onderzoeksgerechten of de strafrechters. Strikt genomen treedt het Comité alsdan niet op als jurisdictioneel orgaan.

WIJZE VAN VATTING	AANTAL 2011	AANTAL 2012	AANTAL 2013
1. Op eigen initiatief	13	19	16
2. Privacycommissie	0	0	0
3. Klacht	0	0	0
4. Schorsing door BIM-Commissie	15	17	5
5. Toelating minister	0	2	2
6. Prejudicieel adviesverlener	0	0	0
TOTAAL	28	38	23

De cijfers tonen aan dat de daling van het aantal vattingen toe te schrijven is aan het lagere aantal schorsingen uitgesproken door de BIM-Commissie.

Eens gevat, kan het Comité verschillende soorten (tussen)beslissingen nemen. In twee gevallen (1. en 2. hieronder) wordt evenwel een beslissing genomen vóór de eigenlijke vatting.

1. Nietigheid van de klacht wegens vormgebrek of afwezigheid van een persoonlijk en rechtmatig belang (art. 43/4, eerste lid, W.I&V).
2. Beslissing om geen gevolg te geven aan een klacht die kennelijk niet gegrond is (art. 43/4, eerste lid, W.I&V).
3. Schorsing van de betwiste methode in afwachting van een definitieve beslissing (art. 43/4, laatste lid, W.I&V).
4. Vordering tot bijkomende informatie ten aanzien van de BIM-Commissie (43/5 § 1, eerste tot derde lid, W.I&V).
5. Vordering tot bijkomende informatie ten aanzien van de betrokken inlichtingendienst (43/5 § 1, derde lid, W.I&V).
6. Onderzoeksopdracht voor de Dienst Enquêtes I (art. 43/5 § 2 W.I&V). In deze rubriek wordt zowel verwezen naar de veelvuldige bijkomende informatie die door de Dienst Enquêtes I op eerder informele wijze wordt ingewonnen vóór de eigenlijke vatting en naar informatie die op verzoek van het Comité wordt ingewonnen na de vatting.
7. Horen van de BIM-Commissieleden (art. 43/5 § 4, eerste lid, W.I&V).
8. Horen van het diensthoofd of de leden van de betrokken inlichtingendienst (art. 43/5 § 4, eerste lid, W.I&V).
9. Beslissing over geheimen die betrekking hebben op een lopend opsporings- of gerechtelijk onderzoek waarvan de leden van de inlichtingendiensten drager zijn, na overleg met de bevoegde magistraat (art. 43/5 § 4, tweede lid, W.I&V).
10. Uitspraak door de voorzitter van het Vast Comité I, na het diensthoofd te hebben gehoord, indien het lid van de inlichtingendienst meent het geheim waarvan hij drager is te moeten bewaren omdat de onthulling ervan nadelig is voor de bescherming van de bronnen, de bescherming van de persoonlijke levenssfeer van derden of de vervulling van de opdrachten van de inlichtingendienst (art. 43/5 § 4, derde lid, W.I&V).
11. Stopzetting van een methode indien ze nog steeds in uitvoering is of indien zij werd geschorst door de BIM-Commissie en bevel dat de gegevens die met deze methode werden verkregen niet mogen worden geëxploiteerd en dienen te worden vernietigd (art. 43/6 § 1, eerste lid, W.I&V).
12. Gedeeltelijke stopzetting van een toegelaten methode. Hier wordt de situatie bedoeld waarbij bijvoorbeeld één methode in tijd wordt beperkt, niet de situatie waarbij in één toelating van een diensthoofd meerdere methoden worden gemachtigd en het Comité slechts één ervan stopzet.
13. Gehele of gedeeltelijke opheffing van de schorsing en het verbod die door de BIM-Commissie was uitgesproken (art. 43/6 § 1, eerste lid, W.I&V). Dit houdt in dat de door het diensthoofd toegelaten methode door het Comité wel (gedeeltelijk) wettelijk, proportioneel en subsidiair werd bevonden.

14. Onbevoegdheid van het Vast Comité I.
15. Ongegrondheid van de aanhangige zaak en geen stopzetting van de methode.
16. Advies als prejudicieel adviesverlener (artt. 131*bis*, 189*quater* en 279*bis* Sv.).

Het Vast Comité I moet binnen een termijn van een maand volgend op de dag waarop het werd geadieerd een definitieve uitspraak doen (art. 43/4 W.I&V). In alle dossiers werd die termijn gerespecteerd.

AARD VAN DE BESLISSING	**2011**	**EIND-BESLISSING 2011**	**2012**	**EIND-BESLISSING 2012**	**2013**	**EIND-BESLISSING 2013**
1. Nietige klacht	0		0		0	
2. Kennelijk ongegronde klacht	1		0		0	
3. Schorsing methode	3		1		0	
4. Bijkomende informatie van BIM-Commissie	4		0		0	
5. Bijkomende informatie van inlichtingendienst	9		6		**0**	
6. Onderzoeksopdracht Dienst Enquêtes	17		11		50	
7. Horen BIM-Commissieleden	0		0		0	
8. Horen leden inlichtingendiensten	1		0		0	
9. Beslissing mbt geheim van onderzoek	0		0		0	
10. Gevoelige informatie tijdens verhoor	0		0		0	
11. Stopzetting methode	12		4		9	
12. Gedeeltelijke stopzetting methode	7		18		5	
13. (Gedeeltelijke) opheffing verbod van BIM-Commissie	5	**39**	13	**38**	2[141]	**23**
14. Onbevoegd	0		0		0	
15. Wettige toelating / Geen stopzetting methode / Ongegrond	15		3		7	
16. Prejudicieel advies	0		0		0	

[141] Eigenlijk besliste het Comité dat de schorsing van de BIM-commissie zonder voorwerp was (zie dossier 2013/1728).

III.3.2. DE RECHTSPRAAK

Hieronder wordt de essentie weergegeven van de 23 eindbeslissingen die het Vast Comité I in 2013 nam. De samenvattingen zijn ontdaan van operationele gegevens. Alleen die elementen die van belang zijn voor het juridische vraagstuk worden opgenomen.[142]

De beslissingen werden gegroepeerd onder vijf rubrieken:

- Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode;
- Motivering van de toelating;
- De proportionaliteits- en de subsidiariteitseis;
- Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van dreiging;
- De gevolgen van een onwettig(e) (uitgevoerde) methode.

Indien relevant werden sommige beslissingen onder meerdere rubrieken opgenomen.

III.3.2.1. Wettelijke (vorm)vereisten voorafgaandelijk aan de uitvoering van een methode

Geen bijzondere methode mag aangewend worden zonder voorafgaande schriftelijke toelating van het diensthoofd. In geval van een uitzonderlijke methode dient er daarenboven een ontwerp van machtiging en een eensluidend advies van de BIM-Commissie voor te liggen. Indien methoden worden ingezet zonder schriftelijke toelating of eensluidend advies, kan het Comité uiteraard optreden.

III.3.2.1.1. Geen bevoegdheid voor de inlichtingendienst

Een inlichtingendienst wil overgaan tot de opsporing van de in- en uitgaande oproepen van een bepaald gsm-nummer (dossier 2013/1835). Immers, uit een andere BIM-methode was eerder toevallig gebleken dat de target wellicht betrokken was bij een internationale smokkel of zwendel. De dienst wou hierover zekerheid. Hij wenste ook na te gaan of de buitenlandse overheid waarvan de target deel uitmaakte, bij de zaak betrokken was. Bij de omschrijving van de bedreiging maakte dienst enkel gewag van de '*schade aangericht door criminele organisaties en het clandestien karakter van de beschreven zwendel die ten minste een potentiële bedreiging vormen voor de economische belangen van België*'. Het Comité merkte echter op dat de bevoegdheid tot opvolging van criminele organisaties, zich beperkt tot die organisaties '*die wezenlijk betrekking hebben op de activiteiten van*

[142] Alle beslissingen van het Comité in deze materie worden gemerkt met de vermelding 'beperkte verspreiding'. Eén beslissing werd als 'vertrouwelijk' geclassificeerd en één als 'geheim'.

spionage, terrorisme, extremisme, proliferatie, schadelijke sektarische organisaties en inmenging' (art. 8, 1°, f W.I&V.). Aangezien dit niet genoegzaam aannemelijk werd gemaakt in de machtiging, werd de methode onwettelijk bevonden.

III.3.2.1.2. Toelating door de bevoegde minister

Net zoals vorig jaar[143] vatte de inlichtingendienst tweemaal zijn minister op basis van artikel 18/10 § 3, derde lid, W.I&V omdat de BIM-commissie omwille van de vakantieperiode niet rechtsgeldig kon vergaderen (dossiers 2013/2327 en 2013/2328). Het wetsartikel laat toe dat, indien de commissie geen advies uitbrengt binnen de termijn van vier dagen na ontvangst van het ontwerp van machtiging voor een uitzonderlijke methode, de inlichtingendienst zijn minister kan vragen de methode alsnog toe te laten. Het Comité had reeds beslist dat het, gelet op de concrete omstandigheden en op de noodzaak voor de dienst om zijn wettelijke opdrachten te kunnen blijven uitoefenen, geen bezwaar had tegen het feit dat de minister onmiddellijk werd gevat. In de twee nieuwe dossiers had de minister het ontwerp van machtiging gehandtekend, maar niet gedagtekend. Eveneens ontbrak een aanduiding van het tijdstip waarop het diensthoofd verslag had moeten uitbrengen over het verloop van de methode en liet de minister na de beslissing mee te delen aan het Comité. Beide verplichtingen zijn nochtans opgenomen in artikel 18/10 § 3, derde en vierde lid, W.I&V. Het Comité oordeelde evenwel dat de methode geldig was. Het herhaalde dat, gezien de omstandigheden en gelet de noodzaak om de inlichtingendienst toe te laten zijn wettelijke opdrachten naar behoren te vervullen, er geen bezwaar is om een beroep te doen op artikel 18/10 § 3, derde lid, W.I&V. Daarenboven merkte het Comité op dat deze bepaling eenvoudigweg de toelating van de bevoegde minister vereist zonder daarbij andere verplichtingen op te leggen dan deze voorzien in artikel 18/10 § 1 W.I&V. Het Comité voegde hieraan toe dat het '*niet-bestaan van dergelijke vermelding* [bedoeld wordt de vermelding van het tijdstip waarop het diensthoofd verslag moet uitbrengen, nvda] *de wettigheid van de beslissing niet aantast, noch afbreuk doet aan de toelating van de Minister*'.

III.3.2.1.3. Methode niet gedekt door de (vereiste) toelating of machtiging

Wanneer een observatie met een technisch middel voor de tweede maal wordt verlengd, merkt het Comité dat die verlenging bij vergissing zeven dagen te laat is aangevraagd (dossier 2013/2653). Met andere woorden: de camera draaide gedurende die korte periode verder zonder de vereiste toelating. De inlichtingendienst ging er van uit dat het Comité niet moest ingrijpen aangezien hij de opgenomen beelden niet zou opslaan in zijn bestanden en dus ook niet zou kunnen exploiteren. Het Comité stelde evenwel dat de beslissing van de dienst om de beelden niet

143 VAST COMITÉ I, *Activiteitenverslag 2012*, 55.

op te slaan '*ne peut avoir pour effet de priver le Comité des prérogatives que la loi lui a octroyées quant au sort à réserver aux données qui ont été recueillies et enregistrées sans une autorisation légale*.'[144] De beelden dienden dus te worden vernietigd.

In een ander dossiers was net hetzelfde aan de hand: tussen de tweede en de derde verlenging van de methode in had de camera gedurende 25 dagen gedraaid zonder de vereiste toelating (dossier 2013/2663). Ook hier kon het Comité niet ingaan op het verzoek om de gegevens niet te vernietigen omdat ze toch niet konden/zouden geëxploiteerd worden. Het Comité benadrukte ook dat '*la mise en œuvre illégale d'une méthode visée par l'article 18/17 L. R&S est susceptible de constituer une infraction visée à l'article 259bis du code pénal*.'[145]

In een derde dossier (2013/1760) besliste het hoofd van de betrokken inlichtingendienst een korte observatie te verrichten met een camera op de toegangspoort van een voor het publiek toegankelijke zaal waar een bepaald evenement zou plaatsgrijpen. De inlichtingendienst was de mening toegedaan dat het om een specifieke methode ging. Maar uit bijkomende informatie die door de BIM-Commissie was ingewonnen, bleek dat de toegangspoort '*est séparée de la voie publique par une bande de terrain pourvue d'une grille pouvant être fermée, et qu'elle est par conséquent située dans un lieu privé qui n'est pas accessible au public*.'[146] Het betrof met andere woorden een uitzonderlijke methode waarvoor de vereiste procedure niet was gevolgd. Het Comité onderschreef dan ook het oordeel van de BIM-Commissie en verklaarde de methode onwettelijk.

III.3.2.2. Motivering van de toelating

In 2013 trof het Comité vijf beslissingen die wezen op een gebrek aan (afdoende of coherente) motivering van de toelating.

Een inlichtingendienst wil overgaan tot de opsporing, identificatie en lokalisatie van de oproepgegevens van drie toestellen (dossier 2013/2618). Nochtans wordt in de toelating alleen de lokalisatie van één toestel expliciet gemotiveerd. Desgevraagd meldt de inlichtingendienst aan de BIM-Commissie dat het de bedoeling was slechts één van de drie toestellen te lokaliseren. De vermelding van de lokalisatie van de drie toestellen zowel in de toelating zelf als in de vordering naar de operator zou een administratieve vergissing zijn geweest. De BIM-Commissie sprak dan ook een gedeeltelijke schorsing uit. Het Comité dat was '*saisi*

144 '*niet voor gevolg kan hebben om het Comité de prerogatieven te ontnemen die de wet hem heeft verleend met betrekking tot het lot dat moet worden verbonden aan gegevens die verzameld en opgenomen zijn zonder wettelijk mandaat.*' (vrije vertaling).

145 '*de illegale uitvoering van een methode voorzien in artikel 18/17 W.I&V kan de inbreuk uitmaken bedoeld in artikel 259bis van het Strafwetboek.*' (vrije vertaling).

146 '*is gescheiden van de openbare weg door een stuk terrein voorzien van een hek dat kan gesloten worden, en dat de zaal bijgevolg gesitueerd is op een niet voor het publiek toegankelijke plaats.*' (vrije vertaling).

d'office de l'ensemble de la décision'[147] oordeelde echter anders. Het was immers niet mogelijk uit te maken of het werkelijk om een administratieve vergissing ging. Daarom werd de aanvraag voor de lokalisatie van de twee nummers waarvoor geen motivering werd opgegeven, als onwettelijke beschouwd.

In een ander dossier (2013/1912) wil de inlichtingendienst de titularis van een gsm-nummer identificeren. Hij zou immers zeer regelmatig contact hebben met een actief lid van een welbepaalde buitenlandse extremistische organisatie die onder meer tegen de NATO zou gericht zijn. Maar volgens het Comité '*l'examen des pièces ne fait pas apparaître que la condition de légalité de la méthode ainsi que les principes de subsidiarité et de proportionnalité, comme déterminés dans l'article 18/3, § 1 premier alinéa de la L. R&S, ont été respectés*.'[148] Immers, de dreiging die zou uitgaan van de organisatie werd door geen enkel concreet element gepreciseerd in de beslissing. Met het oog op bijkomende informatie vatte het Comité zich in deze zaak. Het wou meer aanduidingen over '*le caractère potentiellement menaçant de la cible de la méthode spécifique concernée*'[149] en '*le degré de priorité qu'occupe la (les) problématique(s) […] dans son Plan d'action*.'[150] Aangezien de betrokken dienst op beide vragen concrete antwoorden kon geven, oordeelde het Comité dat de toegelaten methode wettelijk, proportioneel en subsidiair was.

Een inlichtingendienst wil via een observatie te weten komen wie er zal deelnemen aan een vergadering waarin vermoedelijk zal gesproken worden over een nieuw politiek initiatief en een nieuw bewind in een bepaald land (dossier 2013/2420). Tevens verwacht men dat er leden van de betrokken buitenlandse inlichtingendienst zullen aanwezig zijn. In zijn toelating stelt de dienst dat volgende belangen bedreigd zijn: '*de uitwendige veiligheid van de Staat en de internationale betrekkingen, spionage, inmenging.*' De motivering van de ernst van de bedreigingen blijft beperkt tot het volgende: '*een reële mogelijkheid [dat] inlichtingenofficieren clandestiene activiteiten ontplooien op Belgisch grondgebied'. 'Considérant qu'à défaut de constituer une mission en soi [du service de renseignement], la surveillance des activités que déploient les services de renseignement étrangers sur le territoire national ne se justifie que par une menace concrète pour la sûreté de l'Etat belge et ses relations internationales*'[151], aldus het Comité. Aangezien ook uit

147 '*van rechtswege gevat voor het geheel van de beslissing*' (vrije vertaling).

148 '*liet het onderzoek van de stukken niet blijken dat de voorwaarde van de wettelijkheid van de methode evenals de principes van subsidiariteit en proportionaliteit zoals bepaald in artikel 18/3, § 1, eerste lid W.I&V, werden nageleefd.*' (vrije vertaling).

149 '*het potentieel bedreigend karakter uitgaand van het voorwerp van de betrokken specifieke methode*' (vrije vertaling).

150 '*de graad van prioriteit die de problematiek(en) inneemt (innemen) in zijn Actieplan.*' (vrije vertaling).

151 '*Overwegende dat de opvolging van de activiteiten die buitenlandse inlichtingendiensten ontplooien op het nationale grondgebied alleen gerechtvaardigd is in geval van een concrete dreiging voor de veiligheid van de Belgische Staat en zijn internationale relaties, aangezien dergelijke opvolging op zich geen eigenlijke taak is van de inlichtingendiensten.*' (vrije vertaling).

de bijkomende informatie niet blijkt hoe die eventuele clandestiene activiteiten een bedreiging kunnen zijn voor de veiligheid van de Staat en de internationale betrekkingen, is de methode niet wettig.

In een laatste dossier oordeelde het Comité dat de methode niet kon toegelaten worden omdat '*la motivation de la méthode, est incohérente d'une part et insuffisante d'autre part et ne permet pas au Comité d'en apprécier la légalité*'[152] (dossier 2013/2447). De inlichtingendienst had voorgenomen een observatie te verrichten met '*bewakingscamera's gericht op niet-besloten en voor het publiek toegankelijke besloten plaatsen, zoals luchthavens of treinstations.*' De dienst verwees hiervoor naar artikel 18/4 W.I&V dat voorziet in de observatie met technische middelen in publieke plaatsen of in private plaatsen die toegankelijk zijn voor het publiek. Uit de motivering van de beslissing bleek echter dat het de bedoeling was om na te gaan welke personen er woonden of bezoek brachten aan een woonst waarvan de eigenaar op dat ogenblik van zijn vrijheid was beroofd. Aangezien de woonst deel uitmaakte van een complex van woningen, vroeg het Comité bijkomende uitleg over de wijze waarop de observatie *in concreto* zou gebeuren. Daaruit bleek duidelijk dat het geenszins de bedoeling was om plaatsen zoals stations en luchthaven te observeren. '*Les renseignements fournis au Comité, suite à sa demande, vont au-delà d'une simple explication complémentaire, mais révèle l'objectif réel de la méthode*'.[153] De gewraakte methode was namelijk bedoeld om een andere methode (met name de observatie van de personen die toegang hadden tot de woonst) voor te bereiden.

III.3.2.3. De proportionaliteits- en de subsidiariteitseis

Er werden zes beslissingen genomen waarbij de proportionaliteits- en/of de subsidiariteitseis bepalend was.

In twee dossiers (die op eenzelfde operatie betrekking hadden) wenste een inlichtingendienst over te gaan tot de opsporing en de identificatie van de oproepgegevens van de telefoonnummers van vier personen (dossier 2013/2067) en tegelijkertijd tot hun lokalisatie (dossier 2013/2068). De nummers waren op dat ogenblik echter nog niet gekend. Zij zouden verkregen worden via een andere methode. Het Comité stelde dat '*en l'absence d'informations obtenues par cette première méthode, il n'est pas permis de juger du respect des principes de subsidiarité et de proportionnalité et donc de la légalité de la présente méthode*'.[154] Het Comité beveelt dan ook de stopzetting.

---

152 '*de motivering van de methode enerzijds incoherent is en anderzijds onvoldoende en het Comité niet toelaat er de wettelijkheid van te beoordelen.*' (vrije vertaling).

153 '*de op verzoek van het Comité meegedeelde inlichtingen overstijgen een eenvoudige bijkomende uitleg maar onthullen de ware finaliteit van de methode.*' (vrije vertaling).

154 '*bij gebrek aan inlichtingen verkregen door deze eerste methode, kan geen oordeel gevormd worden over de naleving van de principes van subsidiariteit en proportionaliteit en dus over de wettelijkheid van de huidige methode.*' (vrije vertaling).

In een later dossier (2013/2337) kwam het Comité tot hetzelfde oordeel. De betrokken inlichtingendienst wou overgaan tot het afluisteren van een aantal gsm-nummers. Maar een aantal nummers waren op het moment van de toelating nog onbekend. De dienst wou immers ook een aantal nummers afluisteren die gelinkt waren of zouden kunnen zijn aan een welbepaald en gekend gsm-toestel. Om hoeveel en om welke nummers het uiteindelijk precies zou gaan, kon pas geweten zijn op het ogenblik dat de methode effectief werd aangewend. Aangezien de methode aldus sloeg '*sur un nombre indéterminé de numéros de GSM; qu'en l'absence d'information sur le nombre de ces numéros et sur les numéros eux-mêmes qui devraient être écoutés*'[155] was het onmogelijk om de subsidiariteit of de proportionaliteit te beoordelen. De methode werd dan ook stopgezet met betrekking tot de ongekende nummers.

Wanneer een inlichtingendienst wil overgaan tot de opsporing van de oproepgegevens van de gsm van een specifiek persoon en tegelijkertijd de lokalisatiegegevens wil bekomen (dossier 2013/2417), schorts de BIM-Commissie de methoden: '*Men beschikt evenwel over geen verdere informatie over deze [persoon]. Zijn profiel en zijn activiteiten blijken moeilijk te evalueren … Ook wordt in de beslissing niet aannemelijk gemaakt dat er een effectieve bedreiging van deze persoon zou uitgaan.*' In haar toelating had de inlichtingendienst een aantal overwegingen opgenomen die betrekking hadden op de persoon zelf maar ook een aantal meer algemene aspecten van geopolitieke aard. Het Comité vroeg de dienst om bijkomende informatie. Daaruit bleek dat er een zekere tegenspraak bestond tussen verklaringen die de persoon destijds had afgelegd voor een Belgische overheid en zijn activiteiten. '*Attendu que ce comportement étrange et ambigu permet de le considérer comme constituant une menace potentielle pour la sécurité intérieure et extérieure du pays*'.[156] Maar anderzijds stelde het Comité dat '*en l'absence de renseignements plus précis sur ses activités effectives, la demande de données de localisation apparait à ce stade disproportionnée.*'[157] De eerste methode (opsporing oproepgegevens) werd daarom wettelijk verklaard, terwijl de tweede methode (lokalisatie) werd vernietigd.

Ter ondersteuning van een filature wil de inlichtingendienst gedurende één jaar beelden kunnen maken tijdens de observaties (dossier 2013/2446). Het Comité stelde zich vragen bij de duur van deze specifieke methode. Het Comité had reeds toelatingen gehonoreerd voor het gebruik van camera's gedurende één jaar maar toen betrof het een vaste camera die bijvoorbeeld gericht was op een aan de openbare weg gelegen ingang. *In casu* betrof het echter een filature. '*Attendu que même si la filature est une mesure ordinaire, non susceptible de contrôle juri-*

155 '*op een onbepaald aantal gsm-nummers; dat bij gebrek aan informatie over het aantal nummers en over de nummers zelf die zouden moeten beluisterd worden*' (vrije vertaling).

156 '*Overwegende dat dit vreemde en ambigue gedrag toelaat hem te beschouwen als een potentiële bedreiging voor de in- en externe veiligheid van het land.*' (vrije vertaling).

157 '*bij afwezigheid van meer precieze inlichtingen over zijn effectieve activiteiten, lijkt het verzoek om lokalisatiegegevens op dit ogenblik disproportioneel.*' (vrije vertaling).

dictionnel par le Comité permanent R, l'utilisation d'une méthode spécifique pendant une période d'un an doit être justifiée, eu égard aux principes de légalité en ce compris les principes de proportionnalité et de subsidiarité; Attendu que la seule explication fournie quant à la durée, dans ce cas précis, est que pour des raisons pratiques, sur le plan opérationnel, une période longue permet la planification de filatures (et donc des observations au moyen d'une caméra) en tenant compte d'autres opérations de filatures en cours ou à venir'.[158] Het Comité oordeelde dat dergelijke motivering niet beantwoordt aan de principes van proportionaliteit en subsidiariteit en dat de observatie die accessoir is aan de filature moet beperkt worden tot een redelijke termijn van vier maanden.

In een laatste dossier (2013/2662) wenste een inlichtingendienst over te gaan tot de observatie met technische middelen van verschillende leden van een welbepaalde buitenlandse organisatie die actief is in België. De observatie was bedoeld voor de duur van één jaar. De dienst wou niet alleen de medewerkers observeren die in België verblijven maar ook personen die af toe naar België komen en die deel uitmaken van de directe omgeving van de beweging. De bedoeling van de methode bestond er in '*identifier les contacts et activités des membres influents de* [mouvement surveillé] *présents en Belgique.*'[159] Zo gesteld, werden personen die niet in België verblijven, niet gevat door de toelating. Bovendien bleek niet duidelijk of de personen die deel uitmaken van de directe omgeving, tevens invloedrijke personen zijn. Daar bovenop was gebleken dat de methode nog niet in uitvoering was, alhoewel dit volgens de toelating van het diensthoofd reeds bijna een volledig jaar mogelijk was. Ten slotte oordeelde het Comité dat de toelating om de personen die soms in België verbleven gedurende één jaar te kunnen observeren, niet proportioneel. Wat hen betreft, moet de duur van de toelating beperkt blijven tot de tijd die zij in België doorbrengen.

III.3.2.4. Wettelijkheid van de methode met betrekking tot de aangewende technieken, de ingewonnen gegevens, de duur van de maatregel en de aard van de dreiging

III.3.2.4.1. De controle over de uitvoering van de BIM-methode

De Wet van 30 november 1998 bepaalt dat alleen een Belgische inlichtingenagent zoals die omschreven wordt in artikel 3, 2° W.I&V, effectief een specifieke of uit-

158 '*Overwegende dat ook al vormt de filature een gewone methode die niet onderworpen is aan de jurisdictionele controle door het Vast Comité I, dan nog moet de aanwending van een specifieke methode gedurende een periode van één jaar gerechtvaardigd zijn gelet op de wettigheidsprincipes waaronder begrepen de principes van proportionaliteit en subsidiariteit; Overwegende dat de enige uitleg die in deze casus verschaft wordt wat betreft de duur van de methode, is dat dit nodig is vanuit praktische overwegingen op operationeel vlak aangezien een lange periode de planning van de filatures (en dus van de observaties met een camera) toelaat rekening houdend met andere lopende of toekomstige schaduwingsoperaties*'. (vrije vertaling).

159 '*de contacten en activiteiten identificeren van de invloedrijke leden van de opgevolgde beweging die aanwezig zijn in België*' (vrije vertaling).

zonderlijke methode mag uitvoeren. Wel voorziet artikel 13/1 § 2, vijfde lid W.I&V in de mogelijkheid om de hulp of bijstand van andere personen in te roepen. Zolang een of meerdere Belgische inlichtingenagenten *'gardant le contrôle direct de la méthode'*[160] is er geen probleem. Dit criterium werd tweemaal *in concreto* getoest door het Comité.

In het eerste dossier (2013/1950) wenste de dienst een observatie te houden in een private plaats. De methode zou uitgevoerd worden door een agent van een buitenlandse inlichtingendienst en een particulier. Aangezien de dienst *'n'a pas le contrôle direct de cette méthode comme voulu par le législateur'*[161], wordt de methode stopgezet.[162]

Het tweede dossier (2013/2226) was in dit opzicht anders. De inlichtingendienst riep de hulp in van drie buitenlandse inlichtingenagenten om een toestel uit een wagen te verwijderen. Dat toestel was via een eerdere methode geplaatst. Aangezien er slechts bijstand werd verleend door de buitenlandse agenten die over de nuttige technische ervaring beschikten en de eigen agenten dus de directe controle bewaarden, was de methode wettelijk.

III.3.2.4.2. Schorsing van een stopgezette methode

In dossier 2013/1728 was een andere problematiek aan de orde. De dag zelf waarop een tapmaatregel wordt toegelaten, beslist het hoofd van de betrokken inlichtingendienst de maatregel stop te zetten. Er was immers gebleken dat het gsm-nummer dat men wou afluisteren, niet aan de target toebehoorde. Daarop schorste de BIM-Commissie de betrokken methode en beval ze de stopzetting ervan. Het Comité oordeelde echter dat *'la constatation du fait que l'un des numéros de GSM interceptés n'est pas utilisé par la cible de la méthode concernée, n'est pas de nature, en soi, à rendre illégale la dite méthode, celle-ci ayant été décidée et exécutée en parfaite conformité avec la loi'*.[163] Het diensthoofd reageerde correct door de methode stop te zetten vanaf het ogenblik dat ze niet meer nuttig is vanuit de vooropgestelde finaliteit. Dit vormt een toepassing van artikel 18/10 W.I&V. Het Comité oordeelde dat de bevoegdheid van de BIM-Commissie om een methode te schorsen of stop te zetten (art. 18/10, § 6 W.I&V) alleen betekenisvol was geweest indien het diensthoofd zou nagelaten hebben de maatregel stop te zetten. Volgens het Comité was de beslissing van de commissie dan ook zonder voorwerp.

---

160 '*de dienst controle over de methode behouden*' (vrije vertaling).

161 '*niet de directe controle heeft over deze methode zoals gewild door de wetgever*' (vrije vertaling).

162 Daarenboven had de dienst nagelaten te onderzoeken of de locatie waar de observatie zou plaatsvinden niet aan een bijzonder juridisch statuut was onderworpen op basis van het internationaal recht.

163 '*de feitelijke vaststelling dat een van de geïntercepteerde gsm-nummers niet door de target wordt gebruikt is op zich niet van die aard dat de methode die in volledige conformiteit met de wet tot stand is gekomen en uitgevoerd, onwettelijk zou zijn*' (vrije vertaling).

III.3.2.4.3. Het statuut van advocaat

In drie dossiers (2013/2518, 2013/2519 en 2013/2536) beslist een inlichtingendienst om een uitzonderlijke methode aan te wenden ten aanzien van een advocaat die als dusdanig actief is in een niet-EU-land maar op het ogenblik van de aanwending van de methoden in België aanwezig was. Het Comité stelde zich de vraag of de betrokkene de bescherming kon genieten voorzien in de artikelen 2 § 2[164] en 18/2 § 3 W. I&V.[165] Het Comité stelde, zich baserend op de artikelen 428 en 428*bis* van het Gerechtelijk Wetboek.[166] dat de bescherming niet van toepassing kan zijn op betrokkene die '*het beroep van advocaat in België niet kan uitvoeren, noch de titel van advocaat dragen*'.

III.3.2.4.4. De duur van een uitzonderlijke methode

De BIM-commissie verleende een eensluidend advies voor de doorzoeking van bagage op een private plaats die niet toegankelijk is voor het publiek (dossier 2013/2520). Ze formuleerde evenwel een voorbehoud: de machtiging mocht niet langer duren dan vijf dagen, en niet twee maanden zoals in het ontwerp van machtiging vermeld. Die drempel is voorzien in artikel 18/12 § 1 W.I&V. Toch werd hiermee geen rekening gehouden in de machtiging zelf; die was twee maan-

164 *'Het is de inlichtingen- en veiligheidsdiensten verboden gegevens die worden beschermd door ofwel het beroepsgeheim van een advocaat of een arts, ofwel door het bronnengeheim van een journalist te verkrijgen, te analyseren of te exploiteren.*
Bij uitzondering en ingeval de betrokken dienst vooraf over ernstige aanwijzingen beschikt dat de advocaat, de arts of de journalist persoonlijk en actief meewerkt of heeft meegewerkt aan het ontstaan of aan de ontwikkeling van de potentiële bedreiging, zoals bedoeld in de artikelen 7, 1°, 8, 1° tot 4°, en 11, kunnen deze beschermde gegevens worden verkregen, geanalyseerd of geëxploiteerd worden.'

165 *'Als een in §§ 1 en 2 bedoelde methode aangewend wordt ten opzichte van een advocaat, een arts of een journalist, of van hun lokalen of communicatiemiddelen die zij voor beroepsdoeleinden gebruiken, of van hun woonplaats of verblijfplaats, mag deze methode niet uitgevoerd worden zonder dat, naargelang het geval, de voorzitter van de Orde van de Vlaamse balies, van de Ordre des barreaux francophone et germanophone, van de Nationale Raad van de Orde van Geneesheren of van de Vereniging van Beroepsjournalisten hiervan vooraf op de hoogte is gebracht door de voorzitter van de commissie bedoeld in artikel 3, 6°. De voorzitter van de commissie is verplicht om de nodige inlichtingen te verstrekken aan de voorzitter van de Orde of van de Vereniging van Beroepsjournalisten, waarvan de advocaat, de arts of de journalist deel uitmaakt. De betrokken voorzitter is tot geheimhouding verplicht. De straffen bepaald in artikel 458 van het Strafwetboek zijn van toepassing voor inbreuken op deze verplichting tot geheimhouding.'*

166 *Art. 428. 'Niemand kan de titel van advocaat voeren of het beroep van advocaat uitoefenen indien hij geen Belg of onderdaan van een lidstaat van de Europese Unie is, niet in het bezit is van het diploma van doctor of licentiaat in de rechten, niet de eed heeft afgelegd bedoeld in artikel 429 en niet is ingeschreven op het tableau van de Orde of op de lijst van de stagiairs. Er kan afgeweken worden van de voorwaarde van nationaliteit in de gevallen die de Koning bepaalt op advies van de Orde van Vlaamse balies en de Ordre des barreaux francophones et germanophone. Behoudens de afwijkingen die de wet vaststelt, mag geen nadere bepaling aan de titel van advocaat worden toegevoegd'.*

den geldig. De BIM-Commissie ging dan ook over tot de gedeeltelijke schorsing. Het Comité bevestigde het oordeel van de BIM-Commissie.

III.3.2.5. De gevolgen van een onwettig(e) (uitgevoerde) methode

In dossier 2013/1728 besliste het Comité dat de tapmaatregel op een gsm die niet aan de target toebehoorde, wettig was (zie III.3.2.4.2). Nochtans was duidelijk dat het niet de bedoeling was die gegevens te verzamelen. Toch oordeelde het Comité dat het *'n'est pas compétent pour apprécier l'utilité pour un service de renseignement de conserver ou non des données recueillies au moyen d'une méthode exceptionnelle légalement mise en œuvre; que ce pouvoir d'appréciation appartient au service de renseignement lui-même en vertu de l'art. 13 L. R&S et de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel'*.'[167]

In dossier 2013/1835 werd de opsporing van de communicatie van een bepaald gsm-nummer onwettelijk bevonden (zie II.3.2.1.1). Het Comité beval de stopzetting van deze methode voor zover ze nog in uitvoering was. Tevens oordeelde het ze dat '*de gegevens, verkregen en gebeurlijk nog te verkrijgen ingevolge de onwettig bevonden methoden*' niet mochten worden geëxploiteerd en dienden te worden vernietigd.

In dossier 2013/2446, waar de methode disproportioneel werd bevonden (zie II.3.2.3), stelde het Comité dat de gevraagde observatie, die accessoir was aan de filature, moet beperkt worden tot een redelijke termijn van vier maanden en *'que la méthode est illégale pour la période de temps au délà des 4 mois'*.[168]

Wanneer de inlichtingendienst in zijn machtiging geen rekening houdt met het feit dat een bepaalde uitzonderlijke methode maximaal voor vijf dagen kan worden ingezet (dossier 2013/2520 – zie ook II.3.2.4.4), stelt het Comité de onwettigheid vast van de methode '*DOCH SLECHTS voor zover zij zou zijn uitgevoerd NA het verstrijken van een periode van vijf dagen, te rekenen vanaf de machtiging van het diensthoofd*'. Met andere woorden: alleen de '*de gegevens, verkregen en gebeurlijk nog te verkrijgen op basis van het onwettig bevonden gedeelte van de methode, […] mogen [niet] worden geëxploiteerd en moeten worden vernietigd*.'

In een laatste dossier (2013/2662 – zie ook II.3.2.3) wenste een inlichtingendienst over te gaan tot de observatie met technische middelen van verschillende leden van een welbepaalde buitenlandse organisatie die actief is in België. De observatie was bedoeld voor de duur van één jaar. Het Comité oordeelde dat dit niet proportioneel was ten aanzien van de targets die zich slechts sporadisch in België bevonden en *'qu'il conviendrait dès lors de limiter leur observation à la*

167 *'niet bevoegd is om het nut te beoordeelden voor een inlichtingendienst om ja dan neen via een wettelijk uitgevoerde uitzonderlijke methode ingezamelde gegevens, te bewaren; dat die appreciatie toekomt aan de inlichtingendienst zelf en dit in functie van artikel 13 W.I&V en van de wet verwerking persoonsgegevens van 8 december 1992'* (vrij vertaling).

168 '*dat de methode onwettelijk is voor de periode boven de vier maanden*' (vrij vertaling).

durée de leur séjour en Belgique et d'utiliser la procédure d'urgence si nécessaire […] Déclare la méthode illégale en ce qu'elle concerne les "anciens responsables" qui ne résident plus en Belgique mais qui reviennent "parfois" [et] les personnes faisant "partie de l'entourage direct" du mouvement ciblé; La méthode n'ayant pas encore été mise en œuvre, il n'y a pas lieu d'en ordonner la cessation ni la destruction des données recueillies sur ces dernières personnes.'[169]

III.4. CONCLUSIES

Wat betreft het werkingsjaar 2013, formuleert het Comité volgende conclusies:
- het aantal ingezette methoden is in vergelijking met 2011 en 2012 gestegen. Men mag echter niet gewagen van een groei die zou wijzen op een ongebreidelde inzet van bijzondere methoden;
- de stijging is grotendeels het gevolg van het feit dat het aantal observaties en lokalisaties door de VSSE sterk toegenomen is;
- voor het derde jaar op rij viel er een stijging te noteren van het aantal gemachtigde tapmaatregelen;
- uit het onderzoek naar de behaalde resultaten blijkt dat één bepaalde target het voorwerp kan zijn van zeer veel methoden;
- voor de ADIV blijft de strijd tegen 'spionage' de meeste bijzondere methoden opeisen. Ook wat betreft de VSSE nam de aandacht voor deze dreiging (althans wat betreft de BIM) toe. Anderzijds werden beide diensten minder methoden gemachtigd in de strijd tegen het terrorisme;
- twaalf specifieke en uitzonderlijke methoden werden ingezet ten aanzien van een advocaat, arts of beroepsjournalist. Vorig jaar waren dit er nog 24. Aangezien op één persoon meerdere BIM-methoden kunnen worden toegepast, zegt dit cijfer niets over het aantal beroepsbeoefenaars dat het voorwerp was van een BIM-methode;
- het Vast Comité I werd in 2013 23 keer gevat in plaats van 38 het jaar voordien. Deze daling is toe te schrijven is aan het lagere aantal schorsingen uitgesproken door de BIM-Commissie.

169 '*dat het dus vereist is hun observatie te beperken tot de duur van hun verblijf in België en indien noodzakelijk de hoogdringendheidsprocedure te hanteren. […] Verklaart de methode onwettelijk wat betreft de "vroegere verantwoordelijken" die niet meer in België verblijven maar die "soms" terugkeren [en] de personen die "deel uitmalen van de directe omgeving" van de geviseerde beweging; Aangezien de methode nog niet ten uitvoer werd gelegd dient de stopzetting, noch de vernietiging van de ten aanzien van deze personen verzamelde gegevens te worden uitgesproken*' (vrij vertaling).

HOOFDSTUK IV

HET TOEZICHT OP DE INTERCEPTIE VAN COMMUNICATIE UITGEZONDEN IN HET BUITENLAND

Sinds begin 2011 kunnen zowel de VSSE als de ADIV onder zeer strikte voorwaarden communicaties afluisteren, er kennis van nemen en ze registreren (art. 18/17 § 1 W.I&V).

Deze zogenaamde 'BIM-intercepties' moeten evenwel duidelijk worden onderscheiden van '*het zoeken, het onderscheppen, het afluisteren, het kennisnemen of het opnemen door de Algemene Dienst inlichting en veiligheid van de Krijgsmacht van elke vorm van communicatie uitgezonden in het buitenland*.' Deze vorm van afluisteren was al langer mogelijk en kan worden ingezet om redenen van militaire aard in het kader van de opdrachten gedefinieerd in artikel 11 § 2, 1° en 2°, W.I&V als om redenen van veiligheid en bescherming van Belgische en van geallieerde troepen tijdens opdrachten in het buitenland alsook van onze onderdanen die in het buitenland gevestigd zijn (art. 11 § 2, 3° en 4° W.I&V). Ook dit worden klassiek 'veiligheidsintercepties' genoemd, maar zij kennen een volkomen ander controlekader. Het externe toezicht erop is namelijk uitsluitend opgedragen aan het Vast Comité I, en dit zowel voor, tijdens als na de intercepties (art. 44*bis* W.I&V). Het Comité heeft hierbij de bevoegdheid om lopende intercepties te doen stopzetten wanneer blijkt dat de voorwaarden waarin ze uitgevoerd worden, de wettelijke bepalingen en/of de ministeriële toelating niet respecteren (art. 44*ter* W.I&V). Elk jaar, begin december, dient de ADIV immers aan de minister van Landsverdediging zijn gemotiveerde lijst voor te leggen met organisaties of instellingen, van wie de communicatie het komende jaar mag onderschept worden. Dit gebeurt met het oog op de ministeriële toelating van deze intercepties. De minister dient zijn beslissing te nemen binnen tien werkdagen en moet ze vervolgens meedelen aan de ADIV. Nadien moeten zowel de lijst als de ministeriële toelating door de ADIV worden overgezonden aan het Vast Comité I.

In 2013 heeft het Vast Comité I de door de wetgever vereiste verificaties verricht. Daarenboven werd eind december 2013 een omstandige brief gericht naar de ADIV en dit in verband met het Afluisterplan voor het werkingsjaar 2014. Daarin heeft het Comité vragen tot verduidelijk gesteld met betrekking tot de limieten die zowel art. 259*bis* § 5 Strafwetboek als art. 44*bis* W.I&V stellen aan het

intercepteren in het buitenland. De vragen hadden onder meer betrekking op de keuze en de omschrijving van mogelijks te intercepteren 'organisaties of instellingen' en op de motivering ervan vanuit de wettelijke opdrachten van de militaire inlichtingendienst zoals omschreven in artikel 11 W.I&V. Het Vast Comité I ontving in maart 2014 een omstandig antwoord dat werd geanalyseerd met het oog op eventueel verder onderzoek.

HOOFDSTUK V
ADVIEZEN, STUDIES EN ANDERE ACTIVITEITEN

V.1. TWINTIG JAAR DEMOCRATISCH TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

Het Vast Comité I vierde in 2013 zijn twintigjarig bestaan. Ter gelegenheid van deze verjaardag werden een feestbundel uitgegeven en een academische zitting georganiseerd.

Voor de jubileumuitgave '*Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*'[170] werden niet minder dan 38 binnen- en buitenlandse academici, politici en practici bereid gevonden om – ieder vanuit zijn of haar ervaring, expertise en interesses – te schrijven over het toezicht op inlichtingendiensten. Daarbij werden alle behandelde thema's in vijf hoofdstukken ondergebracht: (1) Democratische controle op de inlichtingendiensten van 1830 tot 2013; (2) De controle op de inlichtingendiensten in een breder kader; (3) Het Vast Comité I voor het voetlicht; (4) Het Vast Comité I en zijn relatie met de gecontroleerde diensten en de vier machten; en (5) Het gras is (niet altijd) groener aan de overkant (waarin een aantal buitenlandse auteurs hun licht werpen op het Belgische controlesysteem). Er werd afgesloten met een epiloog van de hand van professor emeritus Cyrille Fijnaut.

Het boek werd op 24 mei 2013 in het Federaal parlement voorgesteld tijdens een plechtige zitting. Talrijke vertegenwoordigers uit de hoogste gezagsinstanties van het land, uit de inlichtingengemeenschap, de media, de academische wereld en enkele buitenlandse toezichtorganen tekenden present.

V.2. INFORMATIEDOSSIERS

Naast toezichtonderzoeken (zie hierover uitvoerig Hoofdstuk II), opent het Vast Comité I ook zogenaamde 'informatiedossiers' die moeten toelaten om een

170 W. VAN LAETHEM en J. VANDERBORGHT (eds.), *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, Intersentia, Antwerpen, 2013, 565 p.

gestructureerde respons te bieden op vragen met betrekking tot de werking van de inlichtingendiensten en het OCAD.[171] Indien dergelijke dossiers aanwijzingen van disfuncties aan het licht brengen of van aspecten van de werking van inlichtingendiensten die nader onderzoek behoeven, kan het Comité overgaan tot het initiëren van een toezichtonderzoek. Indien echter duidelijk is dat een dergelijk onderzoek geen meerwaarde ressorteert vanuit de doelstellingen van het Vast Comité I, wordt het informatiedossier gesloten.

In 2013 werd bijvoorbeeld een informatiedossier geopend naar de problematiek van de naleving van de classificatiewetgeving bij de verzending van documenten, naar de plannen om bepaalde (buiten)diensten van de ADIV te centraliseren en naar de mogelijke inlichtingenactiviteiten van het recent opgerichte ISTAR-Bataljon binnen de Krijgsmacht. Wat betreft ISTAR werd de Begeleidingscommissie van de Senaat in kennis gesteld van het juridisch standpunt van het Comité.

V.3. EXPERT OP DIVERSE FORA

Vertegenwoordigers van het Vast Comité I werden in 2013 diverse malen als expert geconsulteerd door binnen- en buitenlandse publieke en private instellingen.

Zo werd de voorzitter van het Comité op 20 februari 2013 uitgenodigd in de Kamercommissie voor de Binnenlandse Zaken waar hoorzittingen werden georganiseerd over de Wet van 19 juli 1991 houdende regeling van het beroep van privédetective. De voorzitter lichtte de positie van het Comité toe ten aanzien van de vraag welke rol het toezichtorgaan kan spelen bij de controle op de private inlichtingensector.[172]

De voorzitter werd op 18 juni 2013 ook gehoord door de Commissie Binnenlandse Zaken en Administratieve Aangelegenheden van de Senaat. Eerder was in de Senaat een voorstel van resolutie ingediend met betrekking tot het snel ontwikkelen van een federale strategie voor de beveiliging van informatie- en communicatiesystemen.[173] Het voorstel vond zijn oorsprong in de vaststellingen en conclusies van het toezichtonderzoek dat het Comité voerde naar de houding van de Belgische inlichtingendiensten tegenover de noodzaak om informatie- en

---

171 De aanleiding voor het opstarten van informatiedossiers is zeer divers: er wordt een klacht neergelegd en het Vast Comité I wil via een snelle verificatie de manifeste ongegrondheid zo snel als mogelijk uitsluiten; de directie van een inlichtingendienst maakt melding van een incident en het Comité wil nagaan hoe het werd afgehandeld; de media melden een voorval en het Comité wil weten of dit strookt met de realiteit en of er een meer algemene problematiek achter schuilgaat…

172 *Par. St.* Kamer 2012-13, 53-2711/001, 7-9.

173 Parl. St. *Senaat* 2010-11, 4 oktober 2011, nr. 5-1246/1 en Parl. St. Senaat 2012-13, 28 november 2012, nr. 5-1855/1.

communicatiesystemen te beschermen tegen intercepties en cyberaanvallen uit het buitenland. De hoorzittingen kaderden in dit thema.

Begin juni 2013 nam een vertegenwoordiger van het Vast Comité I deel aan de door het *Democratic Centre of Armed Forces* (DCAF) in Tunis georganiseerde rondetafel over 'La transition démocratique et la réforme des services de renseignement'.[174] Door zijn expertise ter beschikking te stellen in dergelijke fora, tracht het Comité een bijdrage te leveren aan het democratiseringsproces van bepaalde landen. De bijeenkomst mondde uit in de oprichting van een interministeriële werkgroep onder leiding van de premier om tot nieuwe wettelijke regelingen te komen voor de Tunesische inlichtingendiensten. In het verlengde hiervan brachten de voorzitter van de 'Instance Nationale de la Protection des Donées Personnelles' en een magistraat verbonden aan het 'Tribunal Administratif' een werkbezoek aan het Vast Comité I.

Op de Litouwse ambassade in Brussel vond een ontmoeting plaats tussen de voorzitters van het *Comité de la Défense et de la Sécurité* enerzijds en van het Vast Comité I anderzijds. Ook hier stond de organisatie van de democratische controle op de inlichtingendiensten en een kennismaking met het Belgische model centraal.

Zoals hierboven aangegeven (Hoofdstuk II.10 en II.11.12), vormden de Snowden-onthullingen het startschot voor vele onderzoeken over heel de wereld. Zo ook in het Europees Parlement. Naar aanleiding van de Resolutie van het Europees Parlement van 4 juli 2013 organiseerde de Commissie burgerlijke vrijheden, justitie en binnenlandse zaken van het Europees Parlement, kortweg de LIBE-Commissie, een reeks hoorzittingen om informatie te verzamelen en om de weerslag van de spionageactiviteiten op de grondrechten en gegevensbeschermingsregels te beoordelen. De voorzitter van het Vast Comité I, Guy Rapaille, werd samen met Senator en lid van de Senatoriële Begeleidingscommissie, Armand De Decker, midden november 2013 in dit kader uitgenodigd. De lopende Belgische onderzoeken werden er kort toegelicht.[175]

Sinds 2011 oefent de voorzitter van het Vast Comité I het voorzitterschap uit van het *Belgian Intelligence Studies Centre (BISC)*. Dit centrum voor inlichtingenstudies wil de inlichtingen- en veiligheidsdiensten en de wetenschappelijke wereld dichter bij elkaar brengen en een bijdrage leveren aan de reflectie over inlichtingenvraagstukken.[176] In 2013 organiseerde het BISC drie studiedagen: 'Kroniek van mijn verborgen oorlog, 1941-1944' (maart 2013), 'Spionage tijdens de Koude Oorlog revisited' (juni 2013) en 'Open source and social media intelligence' (december 2013).

---

174 www.dcaf-tunisie.org.

175 European Parliament, LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, The role of parliamentary oversight of intelligence services at national level in an era of mass surveillance, Statement by Mr Guy Rapaille, Chair of the Belgian Intelligence Services Oversight Committee, 14 november 2013 (www.europarl.europa.eu).

176 www.intelligencestudies.be.

In 2013 werd de frequentie van de werkzaamheden van de zogenaamde 'Werkgroep Analyse', waarin vertegenwoordigers van de twee inlichtingendiensten én het Vast Comité zetelen, opgevoerd. Deze werkgroep trof de voorbereidingen voor de verdere ontwikkeling van de *Belgian Intelligence Academy* (BIA)[177], een academie die opleidingen voor analisten uit zowel de burgerlijke als de militaire inlichtingendienst zal organiseren. Ten behoeve van deze inlichtingenacademie werden ondertussen ook de beheersorganen opgericht: een Directiecomité, een Uitvoerend Comité met aanstelling van een directeur en een secretariaat en een Wetenschappelijk Comité. De voorzitter van het Vast Comité I treedt op als waarnemer bij het Directiecomité en ook minstens één vertegenwoordiger van het Comité maakt deel uit van het Wetenschappelijk Comité. Een eerste 'test case Intelligence and Analysis Course (IAC)' die liep van half juni tot half juli 2013, werd geëvalueerd en een protocolakkoord tussen de betrokken ministers voorbereid. Tevens werd begin juni 2013 door vertegenwoordigers van de VSSE, ADIV en het Vast Comité I in Parijs een werkbezoek gebracht aan de 'Académie française du Renseignement'.

Ten slotte werd het Vast Comité I in 2013 ook vanuit de academische wereld geconsulteerd. De voorzitter van het Comité maakte deel uit te maken van een jury van het Franse 'Centre des Hautes Etudes du Ministère de l'Intérieur' voor een thesisverdediging.[178] Verder neemt het Comité als expert deel aan een onderzoek over de 'nieuwe uitdagingen voor het inlichtingenbeleid in Frankrijk' dat wordt uitgevoerd door Prof. Sébastien Laurent, verbonden aan de Universiteit van Bordeaux. Ook werden gastcolleges gegeven aan de universiteiten van Luik en Louvain-la-Neuve, werd deelgenomen aan de Jobday van de faculteit Rechten, Politieke Wetenschappen en Criminologie van de universiteit van Luik alsook aan een panelgesprek van de Vlaamse Liga voor Mensenrechten over privacy en veiligheid.

V.4. LID VAN EEN SELECTIECOMITÉ

De voorzitter van het Vast Comité I werd, samen met de voorzitter van de Cel voor Financiële Informatieverwerking (CFI) en de directeur van het Coördinatieorgaan voor de dreigingsanalyse (OCAD), aangesteld als lid van het selectiecomité belast met het geven van een omstandig advies aan de ministers van Binnenlandse Zaken en Justitie omtrent de kandidaturen voor de post van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse.[179]

---

177 De missie van de academie luidt als volgt: *'La Belgian Intelligence Academy vise à être le moteur et la référence en matière de formation professionnelle dans le renseignement civil et militaire, et à être reconnue pour son expertise et ses compétences. Elle a pour mission de dispenser des formations communes et structurées, de qualité, au personnel des services de renseignement'.*

178 De thesis had betrekking op 'L'action des services de renseignement à l'épreuve du droit: quelles insuffisances, quelles améliorations?'.

179 M.B. van 29 maart 2013 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 8 april 2013.

V.5. ONTWERP VAN WETSVOORSTEL TOT WIJZIGING VAN DE CLASSIFICATIEWET

De Begeleidingscommissie van de Senaat droeg het Comité midden 2013 op om een wetsvoorstel uit te werken om de Wet van 11 december 1998 betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen (W.C&VM) aan te passen. Dit met het oog op een *overruling*-procedure of een automatische declassificatie wanneer een bepaalde classificatie niet voldoende verantwoord lijkt. De vraag van de Senaat kaderde in eerdere aanbevelingen van het Comité.[180] Gelet op andere prioriteiten, kon het Comité dit voorstel niet finaliseren. Een voorstel zal worden uitgewerkt en overgezonden aan de nieuwe Begeleidingscommissie van de Kamer van Volksvertegenwoordigers.

V.6. CONTROLE SPECIALE FONDSEN ADIV

Het Rekenhof houdt namens de Kamer van Volksvertegenwoordigers toezicht op het gebruik van de financiële middelen door overheidsdiensten. Het moet daarbij de wettigheid en de rechtmatigheid van alle uitgaven controleren. Dat geldt in principe ook voor alle uitgaven van de inlichtingendiensten. Echter, omwille van de gevoeligheid van de materie wordt een deel van het budget van de VSSE en de ADIV (met name de 'speciale fondsen' met uitgaven voor bijvoorbeeld operaties en informanten) niet onderzocht door het Rekenhof. Voor de VSSE wordt de controle van deze uitgaven verricht door de Kabinetschef van de minister van Justitie. Sinds 2006 wordt de controle van de speciale fondsen van de ADIV echter alleen uitgevoerd door het hoofd van de Krijgsmacht en dit vier maal per jaar. Op suggestie van het Rekenhof gebeurt dit sinds 2010 in aanwezigheid van de voorzitter van het Vast Comité I.

V.7. AANWEZIGHEID IN DE MEDIA

Steeds vaker wordt het Vast Comité I gesolliciteerd door de geschreven en gesproken media om toelichting te geven over zijn werkzaamheden dan wel deze van de inlichtingendiensten. Het Vast Comité I ging een aantal maal op deze verzoeken in.

180 VAST COMITÉ I, *Activiteitenverslag 2006*, 137.

Datum	Onderwerp/titel	Forum
Voorjaar 2013	Interview met Guy Rapaille, voorzitter van het Vast Comité I	Diplomatic World nr. 38
4 april 2013	'Filip Dewinter et le Vlaams Belang visés par la Surêté'	L'Echo
4 april 2013	'Staatsveiligheid stak dossier Dewinter niet in doofpot'	De Tijd
6 mei 2013	'Nieuw gezicht in controlecomité inlichtingendiensten'	MO*
24 mei 2013	'De cultuur van het geheim neemt toe'	MO*
25 mei 2013	'Leger in opspraak over 'geheime' geheime dienst'	De Tijd
6 juni 2013	'Staatsveiligheid gecontroleerd'	VRT, Radio 1, Joos
10 juni 2013	'Les renseignements belges'	RTBF, Radio Première, Face à l'info
27 juni 2013	'Des renseignements plus professionnels'	Le Soir
5 augustus 2013	'Controlecomité inlichtingendiensten start groot Prism-onderzoek'	MO*
18 september 2013	'NSA kreeg blanco cheque in België'	De Morgen
22 september 2013	'Vision stratégique de la cyber-sécurité: un désintérêt général'	RTBF-TV, Mise au point
23 oktober 2013	'Staatsveiligheid leeft meldingsplicht aan minister niet na'	De Morgen
23 oktober 2013	'142 namen van politici in dossiers Staatsveiligheid'	MO*
31 oktober 2013	'A quoi sert l'espionnage?'	RTBF, Radio Première, Le forum du midi

HOOFDSTUK VI
DE OPSPORINGS- EN GERECHTELIJKE ONDERZOEKEN

Naast zijn medewerking aan de toezichtonderzoeken, voert de Dienst Enquêtes I van het Comité ook onderzoeken naar leden van de inlichtingendiensten die verdacht worden van een misdaad of wanbedrijf. Dit doet de enquêtedienst in opdracht van de gerechtelijke overheden. Deze bevoegdheid staat omschreven in artikel 40, derde lid van de Wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse. Met de Wet van 10 juli 2006 betreffende de analyse van de dreiging werd deze bevoegdheid uitgebreid tot misdaden of wanbedrijven gepleegd door de leden van het Coördinatieorgaan voor de dreigingsanalyse (OCAD). Wat betreft de leden van de andere 'ondersteunende diensten' geldt deze bepaling alleen ten aanzien van de verplichting om relevante inlichtingen aan het OCAD mee te delen (art. 6 en 14 W.OCAD).

Wanneer zij een opdracht van gerechtelijke politie vervullen, staan de leden en de directeur van de Dienst Enquêtes I onder het toezicht van de procureur-generaal bij het hof van beroep of van de federaal procureur (art. 39 W.Toezicht). Op dat ogenblik heeft het Vast Comité I geen zeggenschap over hen. De voorzitter van het Vast Comité I moet er echter zorg voor dragen dat de uitvoering van de opdrachten van gerechtelijke politie de uitvoering van de toezichtonderzoeken niet hindert. De reden daarvoor ligt voor de hand: het controleorgaan staat in de eerste plaats ter beschikking van het parlement. Die opdracht zou in het gedrang kunnen komen indien een te aanzienlijk deel van de tijd zou besteed worden aan gerechtelijke dossiers. De voorzitter kan in dat geval overleg plegen met de gerechtelijke autoriteiten over de inzet van de leden van de Dienst Enquêtes I in strafonderzoeken (art. 61*bis* W.Toezicht). Van deze mogelijkheid werd nog nooit gebruik gemaakt.

In de gevallen waarin de Dienst Enquêtes I strafonderzoeken voert, moet de directeur na het afronden van dit onderzoek verslag uitbrengen bij het Vast Comité I. In dat geval '*beperkt het verslag zich evenwel tot de informatie die nuttig is voor de uitoefening door het Vast Comité I van zijn opdrachten*' (art. 43, derde lid, W.Toezicht).

In 2013 voerde de Dienst Enquêtes I een aanzienlijk aantal onderzoeksdaden uit in het kader van twee belangrijke onderzoeken. Zo werden bijvoorbeeld 56 processen-verbaal opgesteld.

Een eerste onderzoek, opgestart eind 2011 en uitgevoerd in opdracht van het Federaal Parket naar mogelijke geldverduistering door inlichtingenagenten, werd afgerond in 2013. Het dossier werd door het Federaal Parket zonder gevolg geklasseerd. Niettemin heeft het toegelaten om de noodzaak te benadrukken om werk te maken van een fundamentele aanpassing van het fondsenbeheer bestemd voor de uitbetaling van bronnen van inlichtingendiensten.

Het tweede dossier, waaraan gelijkaardige feiten ten grondslag lagen en dat in handen was van het parket van Antwerpen, kon niet worden afgerond in 2013.

Deze twee gerechtelijke dossiers toonden de noodzaak aan om in detail de geldende regels en praktijk te analyseren met betrekking tot het beheer van fondsen voor de uitbetaling van informanten, en dit bij beide inlichtingendiensten. Het Comité besliste dan ook hieromtrent een toezichtonderzoek te openen (zie II.10.3).

HOOFDSTUK VII

DE GRIFFIE VAN HET BEROEPSORGAAN INZAKE VEILIGHEIDSMACHTIGINGEN, -ATTESTEN EN -ADVIEZEN

De voorzitter van het Vast Comité I neemt ook het voorzitterschap van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en -adviezen waar. De griffiefunctie wordt uitgeoefend door de griffier (of zijn plaatsvervanger) en door de administratie van het Vast Comité I.

Het Beroepsorgaan is bevoegd voor geschillen die betrekking hebben op beslissingen in vier domeinen: de veiligheidsmachtigingen, de veiligheidsattesten die toegang moeten verlenen tot plaatsen waar zich geclassificeerde documenten bevinden, de veiligheidsattesten die toegang moeten verlenen tot welbepaalde plaatsen waar zich een dreiging voordoet en, ten slotte, de veiligheidsadviezen. Daarnaast treedt het Beroepsorgaan ook op als 'annulatierechter' tegen beslissingen van publieke of administratieve overheden om in een bepaalde sector of voor een bepaalde plaats of evenement veiligheidsattesten of -adviezen aan te vragen.[181]

Deze activiteiten van het Beroepsorgaan hebben een directe impact op zowel de budgettaire als personele middelen van het Vast Comité I. Immers worden alle werkingskosten gedragen door het Vast Comité I, dat daarnaast niet enkel én de voorzitter én de griffier levert, doch ook het nodige administratief personeel dat moet instaan voor de tijdsintensieve voorbereiding, de behandeling en de afhandeling van de beroepen.

In dit hoofdstuk worden de aard van de bestreden beslissingen, de hoedanigheid van de bevoegde overheden en van de verzoekers en de aard van de beslissingen van het Beroepsorgaan binnen de verschillende beroepsprocedures cijfermatig weergegeven. Om enige vergelijking mogelijk te maken, werden de cijfers van de afgelopen twee jaar eveneens opgenomen.

In 2013 kende het aantal beroepen en beslissingen een spectaculaire groei in vergelijking met 2012: 189 beroepen tegenover 91 en 187 beslissingen tegenover 81. Deze stijging is vooral toe te schrijven aan het feit dat er in de loop van 2013 veel beroepen werden aangetekend door kandidaat-militairen die een negatief veilig-

181 Zie hierover uitgebreid het *Activiteitenverslag 2006* van het Vast Comité I (91-119).

heidsadvies kregen van de ADIV, die in deze optreedt als veiligheidsoverheid in een nieuwe procedure van selectie en aanwerving.[182] Daarnaast viel er ook een sterke aangroei te noteren van het aantal beroepen tegen negatieve veiligheidsadviezen in het kader van de toekenning van luchthavenidentificatiebadges.

Tabel 1. Betrokken veiligheidsoverheid

	2011	2012	2013
Nationale Veiligheidsoverheid	21	40	98
Veiligheid van de Staat	2	0	1
Algemene Dienst inlichting en veiligheid	39	27	78[183]
Crisiscentrum van de Regering	0	0	0
Federaal Agentschap voor Nucleaire Controle	7	11	9
Federale politie	1	1	1
Lokale politie	0	2	2
Lokale luchthavencommissie	1	10	–[184]
TOTAAL	**71**	**91**	**189**

Tabel 2. Aard van de bestreden beslissing

	2011	2012	2013
Veiligheidsmachtigingen			
Vertrouwelijk	14	7	5
Geheim	31	29	56
Zeer geheim	9	9	5
Totaal veiligheidsmachtigingen	54	45	66

182 Zie art. 9 Wet 28 februari 2007 tot vaststelling van het statuut van de militairen van het actief kader van de Krijgsmacht en tot wijziging van sommige bepalingen betreffende het statuut van het militair personeel zoals gewijzigd bij art. 24 Wet 31 juli 2013 (*BS* 20 september 2013).

183 Zoals uiteengezet in de inleiding bij dit hoofdstuk is de sterke stijging van het aantal dossiers komende van de ADIV te wijten aan het systeem waarbij kandidaat-militairen kunnen onderworpen worden aan een veiligheidsverificatie.

184 Sinds 2013 worden de adviezen in het kader van de veiligheidsbadges voor de toegang tot de beveiligde zones van luchthavens niet meer verleend door de lokale luchthavencommissies maar door de Nationale Veiligheidsoverheid. Vandaar ook de stijging van het aantal dossiers komende van de NVO in vergelijking met vorige jaren.

	2011	2012	2013
Weigering	32	33	41
Intrekking	21	12	5
Weigering en intrekking	–	–	4
Machtiging voor beperkte duur	0	0	1
Machtiging voor lager niveau	1	1	0
Geen beslissing binnen termijn	0	1	15
Geen beslissing binnen verlengde termijn	0	0	0
Totaal veiligheidsmachtigingen	54	45	66
SUBTOTAAL VEILIGHEIDSMACHTIGINGEN	**54**	**45**	**66**
Veiligheidsattesten geclassificeerde documenten			
Weigering	0	23	0
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Weigering	14	0	15
Intrekking	0	0	0
Geen beslissing binnen termijn	0	0	0
Veiligheidsadviezen			
Negatief advies	3	23	106
Geen advies	0	0	2
'Herroeping' van een positief advies	0	0	0
Normatieve rechtshandelingen	0	0	0
Beslissing van publieke overheid om attesten te eisen	0	0	0
Weigering NVO om verificaties voor attesten te verrichten	0	0	0
Beslissing van administratieve overheid om adviezen te eisen	0	0	0
Weigering NVO om verificaties voor adviezen te verrichten	0	0	0
SUBTOTAAL ATTESTEN EN ADVIEZEN	**17**	**46**	**123**
TOTAAL BESTREDEN BESLISSINGEN	**71**	**91**	**189**

Tabel 3. Hoedanigheid van de verzoeker

	2011	2012	2013
Ambtenaar	4	5	4
Militair	37	26	26
Particulier	29	54	159
Rechtspersoon	1	6	0

Tabel 4. Taal van de verzoeker

	2011	2012	2013
Franstalig	32	51	92
Nederlandstalig	39	40	97
Duitstalig	0	0	0
Anderstalig	0	0	0

Tabel 5. Aard van de door het Beroepsorgaan genomen voorbereidende beslissingen[185]

	2011	2012	2013
Volledig dossier opvragen (1)	68	90	187
Aanvullende informatie opvragen (2)	5	5	12
Horen lid overheid (3)	4	10	3
Beslissing voorzitter (4)	0	0	0
Informatie uit dossier halen door Beroepsorgaan (5)	24	44	68
Informatie uit dossier halen door inlichtingendienst (6)	0	0	0

185 Het 'aantal genomen voorbereidende beslissingen' (tabel 5), de 'wijze waarop de verzoeker zijn rechten van verdediging gebruikt' (tabel 6) of nog, de 'aard van de beslissingen van het beroepsorgaan' (tabel 7) is niet noodzakelijkerwijs gelijklopend met het aantal ingediende verzoeken uit de tabellen 1 tot en met 4. Immers, sommige dossiers werden bijvoorbeeld al opgestart in 2012, terwijl de beslissing pas viel in 2013.

(1) Het Beroepsorgaan beschikt over de mogelijkheid het gehele onderzoeksdossier bij de veiligheidsoverheden op te vragen. Aangezien dit dossier meer gegevens bevat dan het onderzoeksverslag alleen, wordt dit verzoek systematisch gedaan.
(2) Het Beroepsorgaan heeft de mogelijkheid om tijdens de procedure aanvullende informatie die het nuttig acht, op te vragen.
(3) Het Beroepsorgaan kan beslissen om de leden van de inlichtingen- en politiediensten of van de veiligheidsoverheden die aan het veiligheidsonderzoek of de -verificatie hebben meegewerkt, te horen.
(4) De voorzitter van het Beroepsorgaan kan beslissen dat het lid van de inlichtingendienst bepaalde gegevens geheim houdt tijdens zijn verhoor.
(5) Indien de betrokken inlichtingendienst hierom verzoekt, kan het Beroepsorgaan beslissen dat bepaalde informatie uit het dossier dat aan de verzoeker ter inzage zal worden voorgelegd, wordt gehaald.
(6) Indien het informatie betreft die afkomstig is van een buitenlandse inlichtingendienst, beslist de Belgische inlichtingendienst zelf of de informatie ter inzage is. Dit is een aspect van de toepassing van de zogenaamde 'derdenregel'.

Tabel 6. Wijze waarop de verzoeker zijn rechten van verdediging gebruikt

	2011	2012	2013
Dossierinzage door klager / advocaat	48	54	103
Horen van de klager / advocaat[186]	55	65	138

Tabel 7. Aard van de beslissingen van het beroepsorgaan

	2011	2012	2013
Veiligheidsmachtigingen			
Beroep onontvankelijk	5	0	2
Beroep zonder voorwerp	1	1	3
Beroep ongegrond	29	19	20
Beroep gegrond (volledige of gedeeltelijke toekenning)	19	23	35
Bijkomende onderzoeksdaden door overheid	1	1	0
Bijkomende termijn voor overheid	0	0	14[187]

186 In bepaalde dossiers wordt de klager/advocaat meermaals gehoord.
187 Deze dossiers hadden in hoofdzaak betrekking op de toekenning van veiligheidsmachtigingen voor personeelsleden van de SHAPE. Aangezien de Belgische veiligheidsoverheid hierbij soms tevergeefs wachtte op informatie vanuit Frankrijk, werden de wettelijke termijnen regelmatig overschreden. Het Beroepsorgaan besloot in 14 gevallen de NVO een bijkomende termijn te verlenen om alsnog een beslissing te nemen.

	2011	2012	2013
Veiligheidsattesten geclassificeerde documenten			
Beroep onontvankelijk	0	0	0
Beroep zonder voorwerp	0	0	0
Beroep ongegrond	0	0	0
Beroep gegrond (toekenning)	0	0	0
Veiligheidsattesten plaats of gebeurtenis			
Beroep onontvankelijk	1	3	1
Beroep zonder voorwerp	0	1	0
Beroep ongegrond	7	8	6
Beroep gegrond (toekenning)	4	6	11
Veiligheidsadviezen			
Beroep onbevoegd	0	5	0
Beroep onontvankelijk	0	1	4
Beroep zonder voorwerp	0	0	1
Bevestiging negatief advies	0	9	25
Omvorming in positief advies	3	4	65[188]
Beroep tegen normatieve rechtshandelingen	0	0	0
TOTAAL	**70**	**81**	**187**

[188] Zoals uiteengezet in de inleiding bij dit hoofdstuk is de stijging van het aantal dossiers inzake veiligheidsadviezen toe te schrijven aan de beroepen van kandidaat-militairen en aan personen die een luchthavenidentificatiebadge moeten bekomen.

HOOFDSTUK VIII
DE INTERNE WERKING VAN HET VAST COMITÉ I

VIII.1. SAMENSTELLING VAN HET VAST COMITÉ I

Tijdens zijn plenaire vergadering van 2 mei 2013 is de Senaat overgegaan tot de benoeming van twee werkende leden, van twee plaatsvervangende voorzitters en van vier plaatsvervangende leden van het Vast Comité I.[189] Gérald Vande Walle werd opnieuw verkozen tot Franstalig werkend lid. Pieter-Alexander De Brock, gedetacheerd expert bij het Coördinatieorgaan voor de dreigingsanalyse, werd verkozen tot Nederlandstalig raadsheer. Zij legden op 8 mei 2013 de eed af in handen van de voorzitster van de Senaat. Guy Rapaille, advocaat-generaal bij het hof van beroep te Luik, werd reeds eerder herbenoemd.

Ook bij de Dienst Enquêtes I vielen er verschuivingen te noteren. Een Nederlandstalige en Franstalige commissaris-auditor besloten de dienst te verlaten. Zij werden respectievelijk in maart 2013 en januari 2014 vervangen. Eind 2013 besloot ook directeur Pierre Nivelle de Dienst Enquêtes I te verlaten. Hij werd op 2 december 2013 vervangen door Frank Franceus, die tot dan werkzaam was als commissaris-auditor. Hij werd benoemd voor een termijn van vijf jaar met aanvang op 1 januari 2014. Het personeelsbestand van deze dienst viel terug op vijf *fulltime* equivalenten.

De administratieve staf van het Vast Comité I, onder leiding van griffier Wouter De Ridder, kende geen wijzigingen en bleef op een totaal van 16 personeelsleden.

VIII.2. VERGADERINGEN MET DE BEGELEIDINGSCOMMISSIE(S)

In de loop van 2013 vonden zes vergaderingen plaats met de Senatoriële Begeleidingscommissie aan wie het Vast Comité I rapporteert. Tijdens deze vergaderingen werden – achter gesloten deuren – de toezichtonderzoeken besproken. Ook het

189 *BS* 21 mei 2013. Pierre Vanderheyden, advocaat-generaal bij het hof van beroep van Luik, werd aangeduid als eerste plaatsvervangend voorzitter; Emile Dejehansart, raadsheer bij het hof van beroep van Bergen, werd tweede plaatsvervangend voorzitter. Carmelo Zaïti, Philippe Meire, Herman Daens en Frank Franceus, werden aangesteld als plaatsvervangende leden.

'zesmaandelijkse verslag over de toepassing van de specifieke en uitzonderlijke methoden door de inlichtingen- en veiligheidsdiensten en de controle hierop door het Vast Comité I voor het werkingsjaar 2012', kwam aan bod. Tevens vond er in oktober 2013 een vergadering plaats met de Begeleidingscommissies van zowel de Kamer van Volksvertegenwoordigers als van de Senaat. Tijdens deze vergadering werd het *Activiteitenverslag 2012* van het Vast Comité I besproken[190] en stond een gemeenschappelijk toezichtonderzoek van de Vaste Comités I en P geagendeerd.

De samenstelling van de Senaatscommissie onderging een wijziging. Sabine de Bethune (CD&V) nam het voorzitterschap van de commissie waar. Verder maakten Dirk Claes (CD&V), Armand De Decker (MR), Philippe Mahoux (PS) deel uit van de commissie. Danny Pieters (N-VA) werd op 17 juli 2013 vervangen door Karl Vanlouwe (N-VA).[191]

Ingevolge de Wet van 6 januari 2014[192], verhuisde de begeleiding van het Vast Comité I van de Senaat naar een ééngemaakte 'Commissie belast met de begeleiding van het Vast Comité P en het Vast Comité I' in de Kamer, die zowel de politie- als de inlichtingendiensten zal controleren.

VIII.3. GEMEENSCHAPPELIJKE VERGADERINGEN MET HET VAST COMITÉ P

De artikelen 52 tot 55 W.Toezicht bepalen de gevallen waarin en de wijze waarop het Vast Comité I en het Vast Comité P gemeenschappelijke vergaderingen dienen te organiseren. Het doel van deze vergaderingen is tweeërlei: het uitwisselen van informatie en het bespreken van gemeenschappelijke toezichtonderzoeken. In 2013 vonden vijf gemeenschappelijke vergaderingen plaats.

VIII.4. FINANCIËLE MIDDELEN EN BEHEERSACTIVITEITEN

Voor het werkingsjaar 2013 werd aan het Vast Comité I een dotatie toegekend van 3,86 miljoen euro tegenover 3,93 miljoen euro in 2012.[193] In 2013 kon het Vast Comité I ten volle zijn voordeel halen uit de kostenbesparing door schaalvergroting als uitloper van zijn verhuis naar het FORUM-gebouw van de Kamer van Volksvertegenwoordigers. Inzake werkingskosten werden bovendien nieuwe synergiën met de Kamer ontwikkeld.

---

190 *Parl. St.* Senaat 2013-14, nr. 5-2426/1 en *Parl. St.* Kamer 2013-14, nr. 53K3496/1.
191 *Hand.* Senaat 2012-13, 17 juli 2013, nr. 5-113, 7.
192 *B.S.* 31 januari 2014.
193 Wet van 4 maart 2013 houdende de algemene uitgavenbegroting voor het begrotingsjaar 2013, *BS* 15 maart 2013 en *Parl. St.* Kamer 2012-2013, nr. 53K2578/001.

VIII.5. VORMING

Omwille van het belang voor de organisatie, moedigt het Vast Comité I zijn medewerkers aan tot het volgen van algemene (informatica, management…) of sectoreigen opleidingen. Wat betreft deze laatste categorie werden onderstaande studiedagen door een of meerdere (personeels)leden van het Vast Comité I bijgewoond.

DATUM	TITEL	ORGANISATIE	PLAATS
2012-2013 2013-2014	Hogere Studies Veiligheid en Defensie	KHID	Brussel
14 januari 2013	Le renseignement en réseaux	Métis	Parijs
17 januari 2013	Renseignement de sources ouvertes: sommes-nous tous des capteurs?	KHID	Brussel
1 maart 2013	Cybercriminalité – Enjeux et actualités	Université de Namur – B-CCentre – CRIDS	Namen
19 maart 2013	Kroniek van mijn verborgen oorlog, 1941-1944	BISC	Brussel
26 maart 2013	De conflicten tussen het Belgische recht en het lokaal recht	Studiecentrum voor Militair recht en Oorlogsrecht	Brussel
26 maart 2013	Le paysage nucléaire militaire en mutation	Académie royale de Belgique	Brussel
27 maart 2013	Cybercrime – Risks to Operative Derived from Smart Phones, the Internet en Social Media	Ambassade Verenigd Koninkrijk	Brussel
4 april 2013	Modernisation et cadre juridique du renseignement en France	Université de Lille	Rijsel
29 april 2013	Le renseignement en question: les sources ouvertes	Métis	Parijs
22-23 mei 2013	Changing Intelligence Challenges	GFF – CATS – Swedish National Defence College – SUPO	Stockholm
3 juni 2013	Rencontre coordination du renseignement	BIA	Parijs
10 juni 2013	Spionage tijdens en na de Koude Oorlog revisited	BISC	Brussel

DATUM	TITEL	ORGANISATIE	PLAATS
13 juni 2013	L'action des services de renseignement à l'épreuve du droit	Centre des hautes études du Ministère de l'Intérieur	Paris
13 juni 2013	Intelligence stratégique	HEC Liège – BISC	Seraing
21 juni 2013	Diplomatic security conference	ECSA	Brussel
24 juni 2013	Le renseignement en question: les sources ouvertes	Métis	Parijs
27 juni 2013	Security & Defence Day Conference	Security & Defence– SDA – CEIS – KAS	Brussel
10 juli 2013	Le rapport Urvoas: quel contrôle des services de renseignement?	HCFDC	Parijs
19 september 2013	Beyond the security vs privacy debate	Security & Defence	Brussel
20 september 2013	Single table lunch meeting (Mr Leonard H. Schrank)	ECSA	Brussel
30 september 2013	Ethique et renseignement	GERER	Parijs
16 oktober 2013	TIGFI Finance Lunch	The Institute for Global Financial Integrity	Luxemburg
21 oktober 2013	De Belgische wapenhandel	Vlaams Vredesinstituut – GRIP	Brussel
24 oktober 2013	Single table lunch meeting (Mr André Vandoren)	ECSA	Brussel
15 november 2013	Les Assises de l'Intelligence Stratégique	Agence de Stimulation économique – Université Louvain-la-Neuve	Louvain-la-Neuve
21 november 2013	Avonddebat 'Privacy'	Liga voor Mensenrechten	Brussel
27 november 2013	10 jaar BOM – balans en uitdagingen	Federale politie (DJO/BTS)	Brussel
6 december 2013	Open source & social media intelligence	BISC	Brussel
16 december 2013	Ethique et renseignement	GERER	Parijs

VIII.6. EVALUATIE VAN DE INTERNE WERKPROCESSEN

Het Vast Comité I heeft – net zoals in 2009 – zijn interne werkprocessen grondig geëvalueerd. Het betreft meer specifiek de werkstromen in het kader van de uitvoering van toezichtonderzoeken, de afhandeling van BIM-dossiers of nog, de behandeling van de dossiers van het Beroepsorgaan inzake veiligheidsmachtigingen, -attesten en –adviezen. Aan de hand van de bevindingen hieromtrent kon het Vast Comité I zijn interne werking optimaliseren.

HOOFDSTUK IX
AANBEVELINGEN

Op basis van de in 2013 afgesloten toezichtonderzoeken en de behandelde BIM-dossiers, formuleert het Vast Comité I onderstaande aanbevelingen. Zij hebben in het bijzonder betrekking op de bescherming van de rechten die de Grondwet en de wet aan de personen verlenen (IX.1), op de coördinatie en de efficiëntie van de inlichtingendiensten, het OCAD en de ondersteunende diensten (IX.2) en – ten slotte – op de optimalisatie van de toezichtmogelijkheden van het Vast Comité I (IX.3).

IX.1. AANBEVELINGEN IN VERBAND MET DE BESCHERMING VAN DE RECHTEN DIE DE GRONDWET EN DE WET AAN PERSONEN WAARBORGEN

IX.1.1. UITVOERING VAN DE ARTIKELEN 19 EN 20 W.I&V[194]

Het Comité herhaalt opnieuw dat het, conform artikelen 19 en 20 W.I&V, aan de bevoegde ministers en aan het Ministerieel Comité voor inlichtingen en veiligheid toekomt om te bepalen onder welke voorwaarden de Belgische inlichtingendiensten moeten of kunnen samenwerken met buitenlandse inlichtingendiensten. Het Vast Comité I acht het hiertoe noodzakelijk dat de beide inlichtingendiensten ten laatste midden 2015 gezamenlijk een voorstel zouden formuleren aan het Ministerieel Comité waarin alle aspecten van de problematiek aan bod komen.

Specifiek aan de ADIV beveelt het Vast Comité I aan dat een studie zou worden uitgevoerd over de eventuele verantwoordelijkheid wanneer de dienst informatie en/of inlichtingen met een buitenlandse inlichtingendienst of instantie uitwisselt.

---

194 Deze aanbeveling stamt uit de onderzoeken naar 'De rol van de Algemene Dienst inlichting en veiligheid bij de opvolging van het conflict in Afghanistan' (zie II.1) en 'De opvolging van politieke mandatarissen door de inlichtingendiensten' (II.4).

IX.1.2. EEN RICHTLIJN OVER INLICHTINGENWERK T.A.V. PERSONEN MET BIJZONDERE VERANTWOORDELIJKHEDEN EN POLITIEKE PARTIJEN[195]

Het Vast Comité I wenst dat de Veiligheid van de Staat én de Algemene Dienst inlichting en veiligheid een gezamenlijk initiatief nemen naar het Ministerieel Comité voor inlichting en veiligheid met het oog op de aanname van een uniforme richtlijn met klare en eenduidige regels met betrekking tot de inwinning, de verwerking, de raadpleging (met inbegrip van de eventuele interne afscherming), de opslag en de archivering van gegevens van bepaalde categorieën van personen die bijzondere verantwoordelijkheden dragen of droegen evenals van politieke partijen. Bij het uitwerken van deze richtlijn moet rekening worden gehouden met de vrijheid van vereniging, de vrijheid van meningsuiting en de krijtlijnen uitgetekend in het arrest van het Europees Hof voor de Rechten van de Mens in de zaak 'Segerstedt-Wiberg and others' en moet gestalte gegeven worden aan het in artikel 2 van de Wet van 30 november 1998 gestelde principe: '*Bij het vervullen van hun opdrachten zorgen die diensten voor de naleving van, en dragen bij tot de bescherming van de individuele rechten en vrijheden alsook tot de democratische ontwikkeling van de maatschappij*'.

Het Comité wijst er ten slotte op dat het aan de wetgever toekomt om desgewenst bijzondere waarborgen in te bouwen voor politieke mandatarissen door een eventuele aanpassing van de wetgeving (bijvoorbeeld in de BIM-wet) en/of door een bijzonder toezicht op te dragen aan het Vast Comité I. Daarbij dient evenwel rekening te worden gehouden met het belang van een normale werking en ontwikkeling van de democratische instellingen alsook met de wettelijke opdrachten van de inlichtingendiensten.

IX.1.3. EENDUIDIGE RICHTLIJNEN OMTRENT HET MELDEN VAN DE OPVOLGING VAN POLITICI

Aansluitend bij de vorige aanbeveling, is het Comité van oordeel dat het aan de bevoegde ministers – als hiërarchisch en politiek verantwoordelijke overheid – toekomt om te bepalen in welke gevallen en wanneer zij in kennis wensen te worden gesteld. Daarbij is van belang dat de ministers duidelijk de finaliteit en de modaliteiten[196] van dergelijke kennisgeving omschrijven.

---

195 Deze aanbeveling werd geformuleerd naar aanleiding van de toezichtonderzoeken 'Geheime nota's over de Scientologykerk in de pers (II.2.), 'Een informant binnen het Vlaamse Belang?' (II.3) en 'De opvolging van politieke mandatarissen door de inlichtingendiensten (II.4). Het Comité herneemt daarmee de aanbeveling uit zijn onderzoek 'gereserveerde dossiers', zie VAST COMITÉ I, *Activiteitenverslag 2008*, 110-111.

196 Onmiddellijk of periodieke melding; alleen melding van collectedocumenten, analyseverslagen en/of verslagen die bestemd zijn voor externe diensten; melding ook voor regionale minis-

IX.1.4. PERMANENTE VORMING EN REËLE KWALITEITSBEWAKING INZAKE COLLECTEVERSLAGEN[197]

Het Comité is zich bewust van het feit dat het in het inlichtingenwerk niet steeds evident is op het moment van de collecte zelf uit te maken welke informatie ooit relevant zal blijken of niet. Dit neemt niet weg dat de eisen ter zake zoals die omschreven zijn in de W.I&V alsook in de Privacywet (doelbindingsprincipe, adequaatheid, correctheid…) moeten nageleefd worden. Dit betekent bijvoorbeeld dat of en op welke wijze een bepaald feit in een collecteverslag wordt opgenomen een cruciaal gegeven vormt. De wijze waarop die *input* dient te gebeuren zou het voorwerp moeten zijn van permanente vorming en onderworpen worden aan een ernstige kwaliteitsbewaking.

IX.2. AANBEVELINGEN IN VERBAND MET DE COÖRDINATIE EN DE EFFICIËNTIE VAN DE INLICHTINGENDIENSTEN, HET OCAD EN DE ONDERSTEUNENDE DIENSTEN

IX.2.1. AANBEVELINGEN IN HET KADER VAN BUITENLANDSE MISSIES VAN DE ADIV

In het kader van zijn toezichtonderzoek naar 'De rol van de Algemene Dienst inlichting en veiligheid bij de opvolging van het conflict in Afghanistan (II.1), werden diverse punctuele aanbevelingen geformuleerd.[198] Het Vast Comité I:

– beveelt aan dat de ADIV de verbanden definieert die tussen operationele, tactische en strategische inlichtingen en de wettelijke opdrachten beschreven in de W.I&V, moeten gelegd worden;
– raadt de ADIV aan om een bundel op te maken van de teksten die toepasselijk zijn tijdens een ontplooiing van de ADIV, met daarin zowel de internationale als de nationale regels. Wat deze laatste betreft, dringt een betere integratie en grotere coherentie van de inhoud zich op;

---

ters en parlementsleden en/of hoogwaardigheidsbekleders van de rechterlijke macht; eventuele controle hierop door het Vast Comité I via een autonome toegang tot de database …

197 Deze aanbeveling komt voort uit het toezichtonderzoek naar 'vermeende strafbare feiten van een buitenlandse inlichtingendienst en de informatiepositie van de VSSE' (II.6).

198 In reactie op het verslag stelde dat ADIV dat de aanbevelingen '*een wezenlijke bijdrage kunnen leveren voor de optimalisatie van organisatie en werking van ADIV. Hoewel het onderzoek zich focust op één operatie, die in meer dan 10 jaren grondige wijzigingen heeft ondergaan, blijft het zeker representatief voor het actuele inlichtingenwerk van ADIV.*' Ook blijkt dat de dienst reeds een aanvang heeft genomen met de implementatie van verschillende aanbevelingen. Het Comité kan zich hierover alleen maar verheugen.

- meent dat het noodzakelijk is om de opleiding van het personeel voorafgaand aan het vertrek voor een opdracht te versterken, en spoort de ADIV aan de al ondernomen verbeteringen voort te zetten;
- meent dat het noodzakelijk is dat de ADIV de C*omprehensive Preparation of the Operational Environnement*-methode toepast (of elke andere methodologie die hetzelfde doel beoogt) en vooral rekening houdt met de behoeften die de militaire partners in het kader van de voorbereiding van opdrachten uitdrukken;
- beveelt aan dat de ADIV ten aanzien van zijn klanten een proactieve houding zou aannemen, om zo meer precies te kunnen bepalen welke hun verwachtingen zijn maar ook om de klanten een duidelijk beeld te verschaffen over wat de ADIV kan aanleveren;
- raadt de ADIV aan een algemene inschatting te maken van de risico's voor het in de conflictzone ontplooide militair en burgerlijk personeel, en voorstellen te formuleren om met die risico's om te gaan;
- spoort de ADIV aan om nader de rol te bepalen van analisten die ingezet worden in een omgeving waar aan collecte wordt gedaan, in het bijzonder met het oog op het garanderen van de objectiviteit van de analysefunctie;
- raadt de ADIV een meer systematische benadering aan bij het inzetten van het personeel in de conflictzone. Een dergelijke benadering, waarbij vertrokken wordt van de bedreigingen die de ADIV in het kader van de W.I&V moet opvolgen, is fundamenteel ten einde te bepalen welke de in te zetten menselijke en materiële middelen zijn;
- meent dat het ontplooide ADIV-personeel in de conflictzone over geschikt materieel moet beschikken, in het bijzonder wat betreft de communicatiemiddelen en de voertuigen die ter beschikking van de BENIC worden gesteld.

IX.2.2. EEN DEBAT OVER DE INZET VAN BIM-METHODEN IN HET BUITENLAND

Om in het buitenland uitgezonden communicaties te onderscheppen, bijvoorbeeld om redenen van veiligheid en bescherming van onze troepen en van deze van onze geallieerde partners tijdens de opdrachten in het buitenland, beschikt de ADIV over een specifiek wettelijk mandaat (art. 259*bis* § 5 Sw. *juncto* art. 11 § 2, 3° W.I&V). Dat ontbreekt voor de inzet van bijzondere inlichtingenmethoden. Het Comité beveelt aan dat de wetgever een debat zou voeren over de noodzaak om bepaalde BIM-methoden mogelijk te maken in het buitenland. De minister van Defensie onderschreef de idee – onder meer met het oog op de naleving van de mensenrechten en de operationele behoeften op het terrein – om aan deze problematiek specifiek aandacht te besteden en koppelde dit aan een evaluatie van de BIM-Wet.

IX.2.3. EENDUIDIGE CONCEPTEN VOOR DE ORGANISATIE VAN DE DATABANK

In zijn toezichtonderzoek naar de opvolging van politieke mandatarissen (II.4), heeft het Vast Comité I moeten vaststellen dat de concepten die aan de basis van de organisatie van de databank van de VSSE liggen, fundamentele problemen met zich meebrengen omdat ze niet eenduidig worden geïnterpreteerd of als dusdanig worden toegepast. Hierdoor dreigt het inlichtingenwerk aan doelmatigheid en doeltreffendheid te verliezen omdat het risico bestaat dat niet (al) de juiste verslagen 'aan de oppervlakte komen' wanneer dit nodig is met het oog op het analysewerk. Ook bestaat het risico dat verkeerde conclusies worden getrokken. Het Vast Comité I is dan ook van mening dat de VSSE deze concepten dringend zou moeten herbekijken, zeker wanneer ze voorkomen in documenten die buiten de VSSE verspreid worden.

Het Vast Comité I is daarenboven van mening dat er actueel een concept ontbreekt: de aanduiding van de (vermoedelijke) rol van een in een verslag vernoemd persoon ten aanzien van de dreiging: is hij een 'voorbijganger', een 'mogelijk slachtoffer', een 'sleutelfiguur', een 'actor'…?

IX.2.4. CONCLUSIES VAN HET ANALYSEWERK SCHRIFTELIJK VASTLEGGEN[199]

Het Comité beveelt aan dat de VSSE elke analyse systematisch afsluit met een (weze het beknopte of voorlopige) conclusie, teneinde vast te leggen óf en op welke wijze en met welke intensiteit het voorwerp van de analyse (een persoon, groepering, gebeurtenis of fenomeen) verder moet worden opgevolgd.

IX.2.5. DE CONTROLE OP BUITENLANDSE INLICHTINGENDIENSTEN

Opnieuw is de noodzaak gebleken voor een uitbreiding van de bevoegdheden van de inlichtingendiensten inzake de controle op buitenlandse inlichtingendiensten.[200] Het Comité herinnert dan ook aan zijn aanbeveling en die van de Senaat om in de Wet houdende regeling van de inlichtingen- en veiligheidsdiensten een specifieke bevoegdheid op te nemen betreffende de controle van de wettelijkheid van de activiteiten van de buitenlandse inlichtingendiensten op Belgisch grondgebied.[201]

---

199 Deze aanbeveling komt voort uit het toezichtonderzoek naar 'vermeende strafbare feiten van een buitenlandse inlichtingendienst en de informatiepositie van de VSSE' (II.6).

200 *Ibid.*

201 VAST COMITÉ I, *Activiteitenverslag 2006*, 132.

IX.2.6. HOOGDRINGENDHEIDPROCEDURE IN GEVAL VAN ARTIKEL 13/1, § 2 W.I&V

Artikel 13/1 § 2, derde lid W.I&V verleent de (voltallige) BIM-Commissie de mogelijkheid om aan inlichtingenagenten de uitdrukkelijke toelating te verlenen om strafbare feiten te begaan die strikt noodzakelijk zijn voor de efficiëntie van de uitvoering van een BIM-methode of ter verzekering van hun eigen veiligheid of die van andere personen. De wet heeft hierbij echter niet voorzien in een procedure van hoogdringendheid. Het Comité is van oordeel dat wanneer de bijzondere methode zelf bij hoogdringendheid kan worden ingezet, ook in de mogelijkheid moet worden voorzien dat de accessoire bevoegdheid uit artikel 13/1 § 2, derde lid, W.I&V bij hoogdringendheid kan worden uitgeoefend.

IX.3. AANBEVELING IN VERBAND MET DE DOELTREFFENDHEID VAN HET TOEZICHT: STRIKTE TOEPASSING VAN ARTIKEL 33 § 2 W.TOEZICHT

'*De inlichtingendiensten, het Coördinatieorgaan voor de dreigingsanalyse en de andere ondersteunende diensten, zenden uit eigen beweging aan het Vast Comité I de interne reglementen en richtlijnen over, alsook alle documenten die de handelswijze van de diensten regelen*', aldus artikel 33 § 2 W.Toezicht. Het is niet de eerste maal[202] dat het Vast Comité I heeft moeten vaststellen dat deze verplichting niet strikt wordt nageleefd, in het bijzonder wat betreft de ADIV, het OCAD en de ondersteunende diensten. De nauwgezette toepassing door de gecontroleerde diensten van dit artikel vormt een *conditio sine qua non* met het oog op een doeltreffende uitvoering van de opdracht van het Comité. Om deze reden onderlijnt het Comité andermaal het belang van de tijdige, volledige en ambtshalve toezending van deze gegevens.

[202] Hierover werd eerder reeds onderzoek uitgevoerd: VAST COMITÉ I, *Activiteitenverslag 1996*, 28-32 (Verslag over de toepassing door de inlichtingendiensten van artikel 33 alinea 2 W.Toezicht); *Activiteitenverslag 2001,* 218-220 (De noodzakelijke inlichtingen waarover het Vast Comité I meent te moeten beschikken met het oog op de doeltreffende uitvoering van zijn opdracht); *Activiteitenverslag 2002,* 27 (Het ambtshalve toezenden van bepaalde documenten van de inlichtingendiensten aan het Vast Comité I); *Activiteitenverslag 2006,* 12.

BIJLAGEN

BIJLAGE A.
OVERZICHT VAN DE BELANGRIJKSTE REGELGEVING MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2013 TOT 31 DECEMBER 2013)

Wet 30 juli 2013 houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van strafvordering, *BS* 23 augustus 2013

Wet 31 juli 2013 tot wijziging van de wet van 28 februari 2007 tot vaststelling van het statuut van de militairen van het actief kader van de Krijgsmacht en tot wijziging van sommige bepalingen betreffende het statuut van het militair personeel, *BS* 20 september 2013

K.B. 14 januari 2013 besluit tot uitvoering van de wet van 4 december 2012 tot wijziging van het Wetboek van de Belgische nationaliteit teneinde het verkrijgen van de Belgische nationaliteit migratieneutraal te maken, *BS* 21 januari 2013

K.B. 23 juli 2013 tot wijziging van het koninklijk besluit van 21 juni 1996 houdende oprichting van een Ministerieel Comité voor inlichting en veiligheid, *BS* 30 juli 2013

K.B. 4 september 2013 tot vaststelling van de bedragen van de retributies verschuldigd zijn voor het afgeven van veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen, *BS* 7 oktober 2013

K.B. 4 september 2013 tot vaststelling van de samenstelling, de werkwijze en de bevoegdheden van het Beheerscomité van de Nationale Veiligheidsoverheid, een Staatsdienst met afzonderlijk beheer, *BS* 7 oktober 2013

K.B. 7 oktober 2013 tot bepaling van de inwerkingtredigen van sommige bepalingen van de wet van 15 augutus 2012 houdende oprichting en organisatie van een federale dienstenintegrator, *BS* 23 oktober 2013

M.B. 7 januari 2013 betreffende de samenstelling van de examencommissies voor de taalexamens voor de zittijd van december 2012-januari 2013, *BS* 13 februari 2013

M.B. 29 maart 2013 houdende aanwijzing van een selectiecomité belast met de evaluatie van de kandidaturen voor de post van adjunct-directeur van het Coördinatieorgaan voor de dreigingsanalyse, *BS* 8 april 2013

Vast Comité van toezicht op de inlichtingen- en veiligheidsdiensten – Directeur van de Dienst Enquêtes – Benoeming, *BS* 30 januari 2013

Omzendbrief 8 maart 2013 betreffende bepaalde aspecten van de wet van 4 december 2012 tot wijziging van het Wetboek van de Belgische nationaliteit teneinde het verkrijgen van de Belgische nationaliteit migratieneutraal te maken, *BS* 14 maart 2013

Benoeming van de twee werkende leden, twee plaatsvervangende voorzitters en vier plaatsvervangende leden van het Vast Comité van toezicht op de inlichtingendiensten (Comité I), *BS* 25 mei 2013

BIJLAGE B.
OVERZICHT VAN DE BELANGRIJKSTE WETSVOORSTELLEN, WETSONTWERPEN, RESOLUTIES EN PARLEMENTAIRE BESPREKINGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2013 TOT 31 DECEMBER 2013)

Senaat

Wetsvoorstel tot wijziging van artikelen 137 en 138 van het Strafwetboek, teneinde de strijd tegen het terrorisme op te voeren, *Parl. St.* Senaat 2012-13, nr. 5-1655/2 en *Hand.* Senaat 2012-13, 7 februari 2013, nr. 5-91, 17

Wetsontwerp tot wijziging van boek II, titel I*ter* van het Strafwetboek, *Parl. St.* Senaat 2012-13, nrs. 5-1905/2 et 5-1905/3

Wetsvoorstel tot aanvulling van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, met het oog op de uitbreiding van de controlebevoegdheid van de Cel Financiële Informatieverwerking wat betreft het extremisme, *Parl. St.* Senaat 2012-13, nrs. 5-1873/2 en 5-1873/3 en *Hand.* Senaat 2012-13, 16 mei 2013, nr. 5-102, 34

Benoeming van de leden van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *Parl. St.* Senaat 2012-13, nr. 5-1956/1

Wetsvoorstel tot wijziging van diverse wetten tengevolge van de hervorming van de Senaat, *Parl. St.* Senaat 2012-13, nrs. 5-1991/1, 5-1991/3 en 5-1991/6 en *Hand.* Senaat 2013-14, 26 november 2013, nr. 5-125, 8

Voorstel van begroting voor het jaar 2013 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM), *Parl. St.* Senaat 2012-13, nrs. 5-2014/1, 5-2014/2 en 5-2014/3 en *Hand.* Senaat 2012-13, 16 mei 2013, nr. 5-102, 39

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de gevallen waarin de dienst Veiligheid van de Staat verkozen politici schaduwt, *Parl. St.* Senaat 2012-13, nr. 5-2034/1

Voorstel tot wijziging van artikel 86*bis* van het reglement van de Senaat, met betrekking tot de vaste commissie belast met de begeleiding van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Senaat 2012-13, nr. 5-2040/1

Benoeming van de twee werkende leden, twee plaatsvervangende voorzitters en vier plaatsvervangende leden van het Vast Comité van Toezicht op de inlichtingendiensten (Comité I), *Hand*. Senaat 2012-13, 2 mei 2013, nr. 5-101, 42

Wetsvoorstel tot wijziging van de wet van 18 juli 1991 tot regeling van het toezicht op politie- en inlichtingendiensten en op het Coördinatieorgaan voor de dreigingsanalyse, met betrekking tot de samenstelling van de vaste commissie belast met de begeleiding van het Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten, *Parl. St.* Senaat 2012-13, nr. 5-2157/1

Wetsontwerp houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van Strafvordering, *Hand*. Senaat 2012-13, 18 juli 2013, nr. 5-114, 39

Vast Comité van Toezicht op de inlichtingendiensten, jaarverslag voor 2012, *Hand*. Senaat 2013-14, 10 oktober 2013, nr. 5-118, 63

Voorstel van begroting voor het jaar 2014 van de Bestuurlijke commissie belast met de controle op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten (Commissie BIM – C-BIM), *Parl. St.* Senaat 2013-14, nrs. 5-2312/2 en 5-2312/3

Kamer van Volksvertegenwoordigers

Onderzoek naar het taalevenwicht bij het leger, *Parl. St.* Kamer 2012-13, nr. 53K2631/001

Voorstel van resolutie over een verscherpte screening van de civiele en militaire (kandidaat-)leden van Defensie en over een uitbreiding van de middelen van de Algemene Dienst Inlichting en Veiligheid (ADIV), *Parl. St.* Kamer 2012-13, nr. 53K2641/001

Voorstel tot oprichting van een parlementaire onderzoekscommissie belast met het onderzoek naar de gevallen waarin de dienst Veiligheid van de Staat verkozen politici schaduwt, *Parl. St.* Kamer 2012-13, nr. 53K2652/001

Wetsvoorstel tot wijziging van de wet van 27 maart 2003 betreffende de werving van de militairen en het statuut van de militaire muzikanten en tot wijziging van verschillende wetten van toepassing op het personeel van Landsverdediging, *Parl. St.* Kamer 2012-13, nr. 53K2569/002

Hoorzittingen over de evaluatie van de wet van 19 juli 1991 tot regeling van het beroep van privédetective, *Parl. St.* Kamer 2012-13, nr. 53K2711/001

Wetsontwerp tot aanvulling van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme, met het oog op de uitbreiding van de controlebevoegdheid van de Cel Financiële Informatieverwerking wat betreft het extremisme, *Parl. St.* Kamer 2012-13, nr. 53K2817/001

Wetsontwerp houdende dringende bepalingen inzake fraudebestrijding (2763/1-11), *Hand*. Kamer 2012-13, 29 mei 2013, CRIV53PLEN144, 19

Wetsvoorstel houdende strengere bestraffing van personen die oproepen tot haat of geweld met de bedoeling afbreuk te doen aan de door de Staat gewaarborgde rechten en vrijheden, *Parl. St.* Kamer 2012-13, nr. 53K2832/001

Wetsontwerp tot wijziging van de wet van 5 februari 2007 betreffende de maritieme beveiliging, *Parl. St.* Kamer 2012-13, nrs. 53K2897/001 en 53K2897/003

Voorstel van resolutie waarbij de oprichting wordt gevraagd van een Centrum voor cyberbeveiliging in België, *Parl. St.* Kamer 2012-13, nr. 53K2918/001

Wetsontwerp houdende wijziging van de artikelen 2, 126 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie en van artikel 90*decies* van het Wetboek van Strafvordering, *Parl. St.* Kamer 2012-13, nrs. 53K2921/001, 53K2921/003, 53K2921/004, 53K2921/005 en 53K2921/006

Wetsontwerp houdende de Middelenbegroting voor het begrotingsjaar 2014, wetsontwerp houdende de algemene uitgavenbegroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nr. 53K3070/007

Ontwerp van algemene uitgavenbegroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nrs. 53K3071/001, 53-3071/008, 53K3071/021, 53K3071/024, 53K3071/027 en 53K3071/036

Verantwoording van de Algemene uitgavenbetroting voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nrs. 53K3072/002, 53K3072/003 en 53K3072/008

Algemene beleidsnota, Binnenlandse Zaken, *Parl. St.* Kamer 2013-14, nr. 53K3096/010

Wetsontwerp tot wijziging van de wet op het politieambt, de wet van 8 december 1992 tot bescherming van de persoonlijke levensfeer ten opzichte van de verwerking van persoonsgegevens en het wetboek van strafvordering, *Parl. St.* Kamer 2013-14, nrs. 53K3105/001 tot 53K3105/008 en *Hand.* Kamer 2013-14, 28 november 2013, CRIV53PLEN171, 43

Wetsontwerp tot wijziging van diverse wetten tengevolge van de hervorming van de Senaat, *Parl. St.* Kamer 2013-14, nrs. 53K3192/001 en 53K3192/004

Wetsontwerp tot wijziging van de wet van 10 april 1990 tot regeling van de private en bijzondere veiligheid, *Parl. St.* Kamer 2013-14, nr. 53K3224/001

Rekenhof, Grondwettelijk Hof, Hoge Raad voor de Justitie, Vaste Comités van toezicht op de politie- en inlichtingendiensten, Federale Ombudsmannen, Commissie voor de bescherming van de persoonlijke levenssfeer en Benoemingscommissies voor het notariaat – rekeningen van het begrotingsjaar 2012 – begrotingsaanpassingen 2013 – begrotingsvoorstellen voor het begrotingsjaar 2014, *Parl. St.* Kamer 2013-14, nrs. 53K3237/001 en 53K3237/002 en *Hand.* Kamer 2013-14, 17 december 2013, CRIV53PLEN175, 60 en *Hand.* Kamer 2013-14, 18 december 2013, CRIV53PLEN176, 11

Hoorzitting met de heer Jean-Claude Delepière, voorzitter van de Cel voor Financiële Informatieverwerking, *Parl. St.* Kamer 2013-14, nr. 53K3269/001

BIJLAGE C.
OVERZICHT VAN INTERPELLATIES, VRAGEN OM UITLEG EN MONDELINGE EN SCHRIFTELIJKE VRAGEN MET BETREKKING TOT DE WERKING, DE BEVOEGDHEDEN EN HET TOEZICHT OP DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN EN HET OCAD (1 JANUARI 2013 TOT 31 DECEMBER 2013)

Senaat

Mondelinge vraag van A. Van dermeersch aan de minister van Binnenlandse Zaken over 'de mogelijke terreuraanslagen van de islamitische groep AQIM' (*Hand.* Senaat 2012-13, 17 januari 2013, nr. 5-88, 8, Vr. nr. 5-793)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Binnenlandse Zaken over 'het OCAD – ondersteunende diensten – communicatie – veiligheidsincidenten' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7802)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'het Coördinatieorgaan voor de dreigingsanalyse (OCAD) – ondersteunende diensten – communicatie – veiligheidsincidenten' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7803)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'het Coördinatieorgaan voor de dreigingsanalyse (OCAD) – risicoanalyse – gebouw Europese Raad' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7805)

Schriftelijke vraag van Y. Vastersavendts aan de staatssecretaris voor Staatshervorming over 'het Coördinatieorgaan voor de dreigingsanalyse (OCAD) – risicoanalyse – gebouw Europese Raad' (Senaat 2012-13, 18 januari 2013, Vr. nr. 5-7806)

Schriftelijke vraag van Y. Vastersavendts aan de minister van Justitie over 'de bestrijding van internetextremisme – "Clean IT Project" – meldingsplicht – klantgegevens – toezicht op sociale media – democratische inspraak in het project – privacybescherming – standpunt regering' (Senaat 2012-13, 21 januari 2013, Vr. nr. 5-7821)

Schriftelijke vraag van J. Ceder aan de minister van Justitie over de 'Baron Benoît de Bonvoisin – schadevergoeding – nota Staatsveiligheid – beroep' (Senaat 2012-13, 23 januari 2013, Vr. nr. 5-7917)

Mondelinge vraag van J. Ceder aan de minister van Justitie over 'de rapporten van de Staatsveiligheid over parlementsleden' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 30, Vr. nr. 5-834)

Mondelinge vraag van F. Dewinter aan de minister van Justitie over 'het volgen van de activiteiten van politici door de Staatsveiligheid' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 30, Vr. nr. 5-835)

Mondelinge vraag van R. Torfs aan de minister van Justitie over 'het onderzoek van de Staatsveiligheid naar schadelijke sektarische organisaties' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 30, Vr. nr. 5-847)

Mondelinge vraag van B. Anciaux aan de minister van Justitie over 'de hulp van België aan de CIA bij de uitvoering van het detentieprogramma en harde ondervragingen' (*Hand*. Senaat 2012-13, 7 februari 2013, nr. 5-91, 47, Vr. nr. 5-839)

Schriftelijke vraag van K. Vanlouwe aan de staatssecretaris voor Ambtenarenzaken over het 'cyberdefensieproject – federale cyberstrategie – samenwerkingsverbanden – beveiligingsnormen – Disaster Recovery Plan – personeel – proactiviteit – Fedict – cyberaanvallen' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5-8183)

Schriftelijke vraag van K. Vanlouwe aan de minister van Economie over het 'cyberdefensieproject – CERT (federale cyber emergency team) – beveiligingsnormen – Disaster Recovery Plan – samenwerkingsverbanden – personeel – proactiviteit –cyberaanvallen – industriële cyberspionage' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5-8186)

Schriftelijke vraag van K. Vanlouwe aan de eerste minister over het 'cyberdefensieproject – federale coördinatie door de eerste minister – personeel – proactiviteit – cyberaanvallen – cyberspionage – actieplan voor cyberaanvallen van de Europese Unie – Disaster Recovery Plan' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5- 8212)

Schriftelijke vraag van K. Vanlouwe aan de minister van Landsverdediging over het 'cyberdefensieproject – samenwerkingsverbanden – Disaster Recovery Plan – perso-

neel – proactiviteit – cyberaanvallen –CERT – NCIRC – Benelux' (Senaat 2012-13, 19 februari 2013, Vr. nr. 5- 8213)

Vraag om uitleg van B. Anciaux aan de minister van Binnenlandse Zaken over 'de brandstichting in een Koerdisch cultureel centrum in Genk' (*Hand*. Senaat 2012-13, 19 februari 2013, nr. 5-206, 13, Vr. nr. 5-2944)

Vraag om uitleg van G. Deprez aan de minister van Binnenlandse Zaken over 'de politie en sociale media' (*Hand*. Senaat 2012-13, 19 februari 2013, nr. 5-206, 14, Vr. nr. 5-2931)

Mondelinge vraag van F. Dewinter aan de minister van Justitie over 'het volgen van politici door de Staatsveiligheid en de controle op deze dienst' (*Hand*. Senaat 2012-13, 21 februari 2013, nr. 5-92, 16, Vr. nr. 5-850)

Mondelinge vraag van K. Vanlouwe aan de staatssecretaris voor Sociale Zaken over 'de MiniDuke-cyberaanval op overheidscomputers' (*Hand*. Senaat 2012-13, 28 februari 2013, nr. 5-93, 19, Vr. nr. 5-871)

Mondelinge vraag van A. De Decker aan de minister van Justitie over 'het personeelsbestand en de middelen van de Staatsveiligheid' (*Hand*. Senaat 2012-13, 7 maart 2013, nr. 5-94, 27, Vr. nr. 5-888)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'de Staatsveiligheid – informatiebewaring – databank – onjuiste informatie – gebruik – wettelijkheid' (Senaat 2012-13, 8 maart 2013, Vr. nr. 5-8421)

Schriftelijke vraag van M. Taelman aan de minister van Justitie over 'de haatpredikers – aantallen – lijst – vervolgingen en veroordelingen – jihad – Syrië' (Senaat 2012-13, 8 maart 2013, Vr. nr. 5-8436)

Schriftelijke vraag van K. Vanlouwe aan de minister van Justitie over 'de werking van het Computer Emergency Response Team' (Senaat 2012-13, 14 maart 2013, Vr. nr. 5-8500)

Mondelinge vraag van D. Pieters aan de minister van Justitie over 'de Staatsveiligheid en politici' (*Hand*. Senaat 2012-13, 14 maart 2013, nr. 5-95, 17, Vr. nr. 5-902)

Mondelinge vraag van J.-J. De Gucht aan de minister van Binnenlandse Zaken over 'het verhoogd terreuralarm' (*Hand*. Senaat 2012-13, 21 maart 2013, nr. 5-96, 27, Vr. nr. 5-919)

Mondelinge vraag van F. Dewinter aan de minister van Buitenlandse Zaken over 'de "Belgische" jihadi's die in Syrië strijden' (*Hand*. Senaat 2012-13, 21 maart 2013, nr. 5-96, 27, Vr. nr. 5-920)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'het talmen van Justitie in het dossier van een Brusselse terrorist' (*Hand*. Senaat 2012-13, 28 maart 2013, nr. 5-97, 31, Vr. nr. 5-932)

Vraag om uitleg van R. Miller aan de minister van Binnenlandse Zaken over 'de Belgische onderdanen die in Syrië vechten en het Plan Radicalisme' (*Hand*. Senaat 2012-13, 16 april 2013, nr. 5-216, 22, Vr. nr.5-3344)

Vraag om uitleg van B. Anciaux aan de minister van Binnenlandse Zaken over 'de Belgische jongeren die in Syrië vechten en terugkeren' (*Hand*. Senaat 2012-13, 16 april 2013, nr. 5-216, 22, Vr. nr.5-3295)

Schriftelijke vraag van B. Anciaux aan de minister van Binnenlandse Zaken over 'de effecten van de cyberaanval MiniDuke op Belgische overheidscomputers' (Senaat 2012-13, 19 april 2013, Vr. nr. 5-8738)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'de beveiliging van religieuze leiders en de vrijwaring van de vrije meningsuiting' (*Hand*. Senaat 2012-13, 25 april 2013, nr. 5-99, 23, Vr. nr.5-962)

Mondelinge vraag van K. Vanlouwe aan de staatssecretaris voor Ambtenarenzaken over 'de cyberstrategie en de rol van Fedict' (*Hand*. Senaat 2012-13, 25 april 2013, nr. 5-99, 37, Vr. nr.5-957)

Schriftelijke vraag van N. Lijnen aan de minister van Landsverdediging over de 'cyberoorlogen – Verenigde Naties – handboek – gebruik' (Senaat 2012-13, 7 mei 2013, Vr. nr. 5-8972)

Schriftelijke vraag van M.Taelman aan de minister van Binnenlandse Zaken over 'privacy – opvorderen gegevens van gebruikers van sociale media – Politie – Staatsveiligheid – Algemene Dienst inlichting en veiligheid – rechtsbescherming – akkoorden – stand van zaken' (Senaat 2012-13, 23 mei 2013, Vr. nr. 5-9086)

Vraag om uitleg van B. Laeremans aan de minister van Justitie over 'de moeilijke strijd tegen cybercriminaliteit' (*Hand*. Senaat 2012-13, 29 mei 2013, nr. 5-227, 9, Vr. nr. 5-3508)

Mondelinge vraag van B. Laeremans aan de minister van Justitie over 'de radicalisering in Marokkaanse kringen en de toegenomen kans op aanslagen in België' (*Hand*. Senaat 2012-13, 30 mei 2013, nr. 5-105, voorlopig niet beschikbaar, Vr. nr. 5-1022)

Mondelinge vraag van H. Bousetta aan de minister van Justitie over 'het PRISM-programma en de bescherming van de privacy' (*Hand*. Senaat 2012-13, 13 juni 2013, nr. 5-107, 25, Vr. nr. 5-1042)

Mondelinge vraag van F. Piryns aan de minister van Justitie over 'het PRISM-programma van het Amerikaanse National Security Agency en privacy van de Belgische bevolking' (*Hand*. Senaat 2012-13, 13 juni 2013, nr. 5-107, 25, Vr. nr. 5-1049)

Mondelinge vraag van B. Hellings aan de minister van Binnenlandse Zaken over 'de nieuwe arrestatie van een Belgische activist' (*Hand*. Senaat 2012-13, 20 juni 2013, nr. 5-108, 12, Vr. nr. 5-1063)

Mondelinge vraag van G. Deprez aan de minister van Binnenlandse Zaken over 'de algemene nationale gegevensbank' (*Hand*. Senaat 2012-13, 20 juni 2013, nr. 5-108, 15, Vr. nr. 5-1066)

Vraag om uitleg van G. De Padt aan de minister van Binnenlandse Zaken over 'de hervorming van de algemene nationale gegevensbank' (*Hand*. Senaat 2012-13, 3 juli 2013, nr. 5-239, 11, Vr. nr. 5-3619)

Vraag om uitleg van K. Vanlouwe aan de minister van Justitie over 'het PRISM-project van de Amerikaanse veiligheidsdiensten en de digitale spionage van internetgebruikers' (*Hand*. Senaat 2012-13, 3 juli 2013, nr. 5-239, 11, Vr. nr. 5-3708)

Vraag om uitleg van K. Vanlouwe aan de minister van Buitenlandse Zaken over 'het PRISM-project van de Amerikaanse veiligheidsdiensten en de digitale spionage van internetgebruikers' (*Hand*. Senaat 2012-13, 3 juli 2013, nr. 5-239, 11, Vr. nr. 5-3711)

Schriftelijke vraag van K. Vanlouwe aan de staatssecretaris voor Ambtenarenzaken over 'de cyberveiligheid en cyberdefensie' (Senaat, 2012-2013, 10 juli 2013, Vr. nr. 5-9407)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over de 'terreur –Belgische lijst van verdachte personen en organisaties – procedure – openbaarheid – relatie tot andere lijsten – rechtsbescherming' (Senaat 2012-13, 10 juli 2013, Vr. nr. 5-9522)

Schriftelijke vraag van B. Anciaux aan de minister van Justitie over 'de rol van de Staatsveiligheid in het afluisterschandaal' (Senaat 2012-13, 19 juli 2013, Vr. nr. 5-9634)

Schriftelijke vraag van B. De Nijn aan de minister van Buitenlandse Zaken over 'Kenia – Al–Shabaab – Somalië – Belgische Jihad-strijders – overzicht – inhouden van paspoorten – rekruteringsgroepen – terugkomst' (Senaat 2012-13, 2 oktober 2013, Vr. nr. 5-9962)

Mondelinge vraag van F. Dewinter aan de minister van Binnenlandse Zaken over 'de lijst van te volgen organisaties' (*Hand*. Senaat 2013-14, 24 oktober 2013, nr. 5-121, 24, Vr. nr. 5-1131)

Schriftelijke vraag van M. Taelman aan de minister van Buitenlandse Zaken over 'National Security Agency – bedrijfsspionage – afluisteren van bedrijfspersoneel – Staatsveiligheid – maatregelen' (Senaat 2013-14, 31 oktober 2013, Vr. nr. 5-10260)

Schriftelijke vraag van M. Taelman aan de eerste minister 'National Security Agency – Belgacom – Swift – afluisterenpraktrijken – hacking overzicht – onderzoek – maatregelen' (Senaat 2013-14, 31 oktober 2013, Vr. nr. 5-10284)

Vraag om uitleg van B. Hellings aan de minister van Binnenlandse Zaken over 'het toekomstige telecommunicatiesysteem van de veiligheidsdiensten' (*Hand*. Senaat 2013-14, 5 november 2013, nr. 5-254, 10, Vr. nr. 5-3895)

Mondelinge vraag van B. Hellings aan de minister van Landsverdediging over 'het potentiële gebruik van de bewakingsinstrumenten van de NSA door de Algemene Dienst inlichtingen en veiligheid in het kader van de opdrachten van het Belgisch leger in Afghanistan' (*Hand*. Senaat 2013-14, 14 november 2013, nr. 5-123, 11, Vr. nr. 5-1164)

Vraag om uitleg van R. Miller aan de minister van Justitie over 'de rechtspositie van gedetineerden' (*Hand*. Senaat 2013-14, 20 november 2013, nr. 5-159, 39, Vr. nr. 5-4222)

Mondelinge vraag van F. Dewinter aan de minister van Binnenlandse over 'de foto op het internet waarop de minister staat te poseren met een salafist, lid van Al Qaida' (*Hand*. Senaat 2013-14, 5 december 2013, nr. 5-129, 12, Vr. nr. 5-1209)

Kamer van Volksvertegenwoordigers

Vraag van M. Doomst aan de minister van Justitie over 'cybercriminaliteit' (*Hand*. Kamer, 2012-13, 10 januari 2013, CRIV53PLEN124, 57, Vr. nr. 1422)

Samengevoegde vragen van B. Schoofs en P. Luykx aan de minister van Binnenlandse over 'het geweld na een pro-Koerdische betoging in Genk' (*Hand*. Kamer, 2012-13, 24 januari 2013, CRIV53PLEN126, 44, Vr. nrs. 1471 en 1472)

Vraag van P. Dedecker aan de minister van Binnenlandse Zaken over 'cyberveiligheid' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 46, Vr. nr. 714)

Vraag van B. Slegers aan de minister van Justitie over de 'Staatsveiligheid – beperkte budgettaire middelen' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 60, Vr. nr. 770)

Vraag van P. Logghe aan de minister van Financiën over het 'witwassen van geld' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 104, Vr. nr. 668)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'de militaire achtergrond van de Special Forces' (*Vr. en Ant*. Kamer 2012-13, 28 januari 2013, QRVA 098, 268, Vr. nr. 363)

Vraag van N. Lanjri aan de minister van Justitie over 'de bevoegdheden en de toekomst van het Executief van de Moslims van België' (*Hand*. Kamer, 2012-13, 30 januari 2013, CRIV53COM 658, 6, Vr. nr. 15265)

Samengevoegde vragen van J. Galant en D. Ducarme aan de minister van Justitie over 'de controle van de islamitische scholen in België' (*Hand*. Kamer, 2012-13, 30 januari 2013, CRIV53COM 658, 35, Vr. nrs. 15448 en 15518)

Samengevoegde vragen van D. Ducarme, A. Ponthier en G. Dallemagne aan de minister van Landsverdediging over 'de aanwezigheid van extremisten in het leger' (*Hand*. Kamer, 2012-13, 17 februari 2013, CRIV53PLEN125, 26, Vr. nrs. 1442, 1443 en 1444)

Samengevoegde vragen van M. Doomst, P. Logghe, C. Van Cauter, G. Dallemagne, S. Van Hecke, B. Schoofs, K. Degroote en M. Jabour aan de minister van Justitie over 'de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 7 februari 2013, CRIV53COM666, 1, Vr. nrs. 15667, 15671, 15693, 15705, 15706, 15730, 15739 en 15767)

Vraag van Z. Génot aan de minister van Justitie over 'de opvolging van de aanbevelingen van de Lumumbacommissie' (*Hand*. Kamer, 2012-13, 20 februari 2013, CRIV-53COM678, 35, Vr. nr. 15688)

Vraag van G. Dallemagne aan de eerste minister over 'het stelen van gegevens en saboteren van een Belgisch bedrijf door China' (*Hand*. Kamer, 2012-13, 21 februari 2013, CRIV53PLEN132, 19, Vr. nr. 1534)

Samengevoegde vragen van B. Schoofs, K. Degroote en M. Doomst aan de minister van Binnenlandse Zaken over 'de werking van de Veiligheid van de Staat' (*Hand*. Kamer, 2012-13, 21 februari 2013, CRIV53PLEN132, 27, Vr. nrs. 1535, 1536 en 1537)

Samengevoegde vragen van K. Degroote, M. Doomst, C. Van Cauter, S. Van Hecke, B. Weyts en B. Schoofs aan de minister van Justitie over 'de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 26 februari 2013, CRIV53COM682, 1, Vr. nrs. 15873, 15876, 15882, 15896, 15934 en 15983)

Samengevoegde vragen van K. Lalieux, L. Van Biesen en T. Veys aan de staatssecretaris voor Leefmilieu over 'de veiligheid op Brussels Airport programma' (*Hand*. Kamer, 2012-13, 5 maart 2013, CRIV53COM689, 19, Vr. nrs. 16011, 16038 en 16355)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'de deelname aan het MUSIS-programma' (*Hand*. Kamer, 2012-13, 6 maart 2013, CRIV53COM691, 4, Vr. nr. 16186)

Samengevoegde vragen van B. Valkeniers en D. Ducarme aan de minister van Justitie over ''Belgische' jongeren als huurlingen voor de radicale moslims in Syrië' (*Hand*. Kamer, 2012-13, 13 maart 2013, CRIV53COM698, 4, Vr. nrs. 16484, 16485 en 16587)

Samengevoegde vragen van B. Slegers, P. Logghe en S. Van Hecke aan de minister van Justitie over 'de databank van de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 13 maart 2013, CRIV53COM698, 9, Vr. nrs. 16457, 16487 en 16524)

Vraag van P. Logghe aan de minister van Justitie over 'moslimterroristen en de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 20 maart 2013, CRIV53COM703, 6, Vr. nr. 16711)

Vraag van J. Van Esbroeck aan de minister van Binnenlandse Zaken over de 'aanpassing van het dreigingsniveau' (*Vr. en Ant*. Kamer 2012-13, 25 maart 2013, QRVA 106, 146, Vr. nr. 711)

Samengevoegde vragen van O. Maingain en E. Thiébaut aan de minister van Binnenlandse Zaken en Gelijke Kansen over 'de zaak-Benladghem' (*Hand*. Kamer, 2012-13, 28 maart 2013, CRIV53PLEN137, 32, Vr. nrs. 1660 en 1661)

Vraag van T. Francken aan de minister van Landsverdediging over de 'topofficieren die geen functie vervullen' (*Vr. en Ant*. Kamer 2012-13, 2 april 2013, QRVA 107, 98, Vr. nr. 414)

Vraag van D. Thiéry aan de staatssecretaris voor Ambtenarenzaken over de 'maatregelen tegen cyberaanvallen' (*Vr. en Ant*. Kamer 2012-13, 2 april 2013, QRVA 107, 284, Vr. nr. 61)

Vraag van B. Valkeniers aan de minister van Buitenlandse Zaken over 'de monitoring van eurokritische meningen' (*Vr. en Ant*. Kamer 2012-13, 12 april 2013, QRVA 108, 422, Vr. nr. 424)

Vraag van P. Dedecker aan de minister van Binnenlandse Zaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2012-13, 12 april 2013, QRVA 108, 503, Vr. nr. 714)

Samengevoegde vragen van P. Logghe en W.-F. Schiltz aan de minister van Binnenlandse Zaken over 'de diamantroof op de luchthaven van Zaventem' (*Hand*. Kamer, 2012-13, 16 april 2013, CRIV53COM713, 24, Vr. nrs. 160534 en 16535)

Samengevoegde vraag van Ch. Lacroix en K. Grosemans aan de minister van Landsverdediging over 'de ambities van het Belgische leger op het stuk van satellietbeeldverwerking' (*Hand*. Kamer, 2012-13, 16 april 2013, CRIV53COM714, 6, Vr. nrs. 16482 en 85)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'het lek tijdens een hoorzitting achter gesloten deuren' (*Hand*. Kamer, 2012-13, 16 april 2013, CRIV-53COM714, 21, Vr. nr. 16826)

Samengevoegde vragen van D. Ducarme, B. Somers en B. Schoofs aan de minister van Justitie over 'het uitblijven van wettelijke sancties tegen Belgen die geronseld worden voor de strijd of individueel gaan vechten in Syrië' (*Hand*. Kamer, 2012-13, 17 april 2013, CRIV53COM718, 6, Vr. nrs. 16917, 17256 en 17279)

Samengevoegde vragen B. Clerfayt, F. De Man, H. Bonte, L. Devin, B. Slegers, B. Weyts et J. M. Dedecker aan de eerste minister over 'de jonge Belgen die in Syrië gaan vechten' (*Hand*. Kamer, 2012-13, 18 april 2013, CRIV53PLEN138, 22, Vr. nrs. 1679 tot 1685)

Vraag van B. Slegers aan de minister van Justitie over de 'Staatsveiligheid – beperkte budgettaire middelen' (*Vr. en Ant*. Kamer 2012-13, 19 april 2013, QRVA 109, 203, Vr. nr. 770)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'het standpunt van Defensie inzake het MUSIS-programma' (*Hand*. Kamer, 2012-13, 24 april 2013, CRIV-53COM723, 15, Vr. nr. 17386)

Vraag van S. Van Hecke aan de minister van Justitie over 'de werkomstandigheden bij de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 24 april 2013, CRIV53COM725, 2, Vr. nr. 17123)

Vraag van S. De Wit aan de minister van Binnenlandse Zaken over 'de talenkennis bij de ondersteunende diensten van de politie' (*Vr. en Ant*. Kamer 2012-13, 26 april 2013, QRVA 110, 131, Vr. nr. 21)

Samengevoegde vragen van T. Francken aan de minister van Justitie over 'het inzagerecht van de koning in geheime documenten van de Staatsveiligheid' (*Hand*. Kamer, 2012-13, 30 april 2013, CRIV53COM732, 17, Vr. nrs. 17559 en 17577)

Samengevoegde vragen van D. Ducarme aan de minister van Justitie over 'Sharia4Belgium, de terugkeer van Belgische Syriëstrijders en de communicatie van gegevens van justitie aan het departement Buitenlandse Zaken' (*Hand*. Kamer, 2012-13, 30 april 2013, CRIV53COM732, 19, Vr. nrs. 17586 en 17587)

Vraag van K. Grosemans aan de minister van Landsverdediging over de 'Malware detecties in de computersystemen van Defensie' (*Vr. en Ant*. Kamer 2012-13, 6 mei 2013, QRVA 111, 64, Vr. nr. 441)

Samengevoegde vragen van T. Francken, W. De Vriendt, D. Van der Maelen en Ph. Blanchart aan de minister van Landsverdediging over 'de wapenleveringsdeal van Defensie' (*Hand*. Kamer, 2012-13, 8 mei 2013, CRIV53PLEN141, 2, Vr. nr. 1738, 1739, 1740 en 1741)

Vraag van D. Ducarme aan de minister van Justitie over 'het gebrek aan middelen van de Veiligheid van de Staat' (*Hand*. Kamer, 2012-13, 8 mei 2013, CRIV53PLEN141, 15, Vr. nr. 1747)

Vraag van B. Pas aan de minister van Buitenlandse Zaken over 'de dreigementen van Sharia4UK' (*Hand*. Kamer, 2012-13, 16 mei 2013, CRIV53PLEN142, 20, Vr. nr. 1768)

Samengevoegde vragen van D. Ducarme, W. De Vriendt, D. Geerts en A. Ponthier aan de minister van Landsverdediging over 'het noodzakelijke toezicht door Defensie en onze regering op de doorverkoop van militair materieel' (*Hand*. Kamer, 2012-13, 21 mei 2013, CRIV53COM750, 17, Vr. nrs. 17801, 17873, 17898 en 18001)

Vraag van G. Dallemagne aan de minister van Landsverdediging over 'cyberaanvallen' (*Hand*. Kamer, 2012-13, 21 mei 2013, CRIV53COM750, 24, Vr. nr. 17925)

Samengevoegde vragen van D. Ducarme en P. Logghe aan de minister van Binnenlandse Zaken over 'de terugkeer van Belgische gewezen jihadisten uit Syrië' (*Hand*. Kamer, 2012-13, 23 mei 2013, CRIV53PLEN143, 13, Vr. nrs. 1784 en 1785)

Vraag van B. Weyts aan de minister van Binnenlandse Zaken over de 'radicale islamisten in Syrië' (*Vr. en Ant*. Kamer 2012-13, 27 mei 2013, QRVA 114, 48, Vr. nr. 860)

Vraag van P. Dedecker aan de staatssecretaris voor Ambtenarenzaken over de 'cyberveiligheid' (*Vr. en Ant*. Kamer 2012-13, 27 mei 2013, QRVA 114, 325, Vr. nr. 125)

Samengevoegde vragen van K. Grosemans en A. Ponthier aan de minister van Landsverdediging over 'de kritiek van het Comité I op het gebrek aan controle op ISTAR' (*Hand*. Kamer, 2012-13, 29 mei 2013, CRIV53COM760, 8, Vr. nrs. 18156 en18164)

Samengevoegde vragen van L. Van Biesen, B. Slegers en P. Logghe aan de minister van Binnenlandse Zaken over 'het dreigement van Sharia4UK' (*Hand*. Kamer, 2012-13, 29 mei 2013, CRIV53COM761, 35, Vr. nrs. 17926, 17933, 18007, en 18050)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'radicalisering van jongeren – invloed/tips uit Saoedi-Arabië, Tsjetsjenië en Quatar' (*Vr. en Ant*. Kamer 2012-13, 3 juni 2013, QRVA 115, 60, Vr. nr. 891)

Vraag van D. Ducarme aan de minister van Justitie over 'de gerechtelijke opvolging van Syriëstrijders na hun terugkeer naar België' (*Hand*. Kamer, 2012-13, 11 juni 2013, CRIV53COM773, 14, Vr. nr. 18227)

Vraag van D. Ducarme aan de minister van Justitie over 'de dreiging met terreur van Sharia4UK aan het adres van België' (*Hand*. Kamer, 2012-13, 11 juni 2013, CRIV53COM773, 15, Vr. nr. 18382)

Samengevoegde vragen van J. Van Esbroeck en P. Logghe aan de minister van Binnenlandse Zaken over 'terugkerende Syriëstrijders' (*Hand*. Kamer, 2012-13, 13 juni 2013, CRIV53PLEN148, 21, Vr. nrs. 1857 en 1858)

Vraag van I. Emmery aan de minister van Buitenlandse Zaken, Buitenlandse Handel over 'het PRISM-programma van de Amerikaanse geheime dienst' (*Hand*. Kamer, 2012-13, 13 juni 2013, CRIV53PLEN148, 54, Vr. nr. 1861)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'Moslimstrijders in Syrië en berichtgeving' (*Vr. en Ant*. Kamer 2012-13, 17 juni 2013, QRVA 117, 70, Vr. nr. 929)

Vraag van K. Grosemans aan de minister van Landsverdediging over de 'aanbevelingen van het Comité I inzake de werking van de ADIV' (*Vr. en Ant*. Kamer 2012-13, 17 juni 2013, QRVA 117, 161, Vr. nr. 474)

Vraag van F. De Man aan de minister van Binnenlandse Zaken over 'de discretie met betrekking tot de dossiers van jihadi's die naar Syrië zijn vertrokken' (*Hand*. Kamer, 2012-13, 20 juni 2013, CRIV53PLEN150, 10, Vr. nr. 1880)

Vraag van G. Dallemagne aan de minister van Justitie over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 20 juni 2013, CRIV53PLEN150, 27, Vr. nr. 1887)

Vraag van B.Weyts aan de minister van Binnenlandse Zaken over 'het crisiscentrum – behandeling van dossiers van bedreigde personen' (*Vr. en Ant*. Kamer 2012-13, 24 juni 2013, QRVA 118, 172, Vr. nr. 824)

Vraag van A. Frédéric aan de minister van Sociale Zaken over de 'Frans rapport over therapeutische sekten' (*Vr. en Ant*. Kamer 2012-13, 1 juli 2013, QRVA 119, 161, Vr. nr. 1005)

Samengevoegde vragen van H. De Croo, T. Francken, J. Fernandez Fernandez en S. Van Hecke aan de minister van Buitenlandse Zaken over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 2, Vr. nrs. 18510, 18525, 18693, 19037, 19071 en 19075)

Samengevoegde vragen van T. Francken aan de minister van Justitie over 'het gerechtelijk onderzoek naar mogelijke terroristische feiten door mensen uit het Brusselse anarchistische milieu' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 38, Vr. nrs. 18734 en 18735)

Samengevoegde vragen van P. Logghe aan de minister van Binnenlandse Zaken over 'de internationale financiële stromen van het terrorisme' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 42, Vr. nrs. 18756 en 18918)

Samengevoegde vragen van B. Schoofs aan de minister van Justitie over 'de adviezen van de Raad van Theologen van de Moslimexecutieve' (*Hand*. Kamer, 2012-13, 3 juli 2013, CRIV53COM795, 45, Vr. nrs. 18760 en 18785)

Samengevoegde vragen van O. Henry, H. De Croo en D. Van der Maelen aan de minister van Buitenlandse Zaken over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 4 juli 2013, CRIV53PLEN154, 8, Vr. nrs. 1925, 1935 en 1926)

Samengevoegde vragen van P. Logghe en J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'het aantal radicale moslims in ons land' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM800, 25, Vr. nrs. 18161 en 18215)

Samengevoegde vragen van J. Van Esbroeck, B. Slegers, P. Logghe en D. Ducarme aan de minister van Binnenlandse Zaken over 'het gebrek aan eensgezindheid in de Syrië-

taskforce' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM800, 44, Vr. nrs. 18699, 18942, 19030, en 19073)

Samengevoegde vragen van K. Grosemans, Ch. Lacroix en T. Francken aan de minister van Landsverdediging over 'het PRISM-programma' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM801, 16, Vr. nrs. 18527, 18588 en 19070)

Interpellatie van de heer Filip De Man aan de minister van Landsverdediging over 'het bericht dat een fundamentalistische moslim, opgeleid door het Belgisch leger, sneuvelde in Syrië' (*Hand*. Kamer, 2012-13, 9 juli 2013, CRIV53COM801, 31, Vr. nr. 99)

Vraag van de P. Dedecker aan de staatssecretaris voor Ambtenarenzaken over 'de spionage door de Amerikaanse autoriteiten bij IT-bedrijven' (*Vr. en Ant*. Kamer 2012-13, 22 juli 2013, QRVA 122, 228, Vr. nr. 159)

Vraag van B. Schoofs aan de minister van Justitie over 'de werkzaamheden van de Staatsveiligheid' (*Vr. en Ant*. Kamer 2012-13, 29 juli 2013, QRVA 123, 182, Vr. nr. 841)

Vraag van G. Dallemagne aan de eerste minister over 'Chinese cyberaanvallen' (*Vr. en Ant*. Kamer 2012-13, 19 augustus 2013, QRVA 124, 389, Vr. nr. 95)

Vraag van S. Van Hecke aan de minister van Justitie over 'de cyberveiligheid' (*Hand*. Kamer, 2012-13, 29 september 2013, CRIV53COM816, 6, Vr. nr. 19749)

Vraag van S. Van Hecke aan de minister van Justitie over 'de opvolging van PRISM' (*Hand*. Kamer, 2012-13, 29 september 2013, CRIV53COM817, 47, Vr. nr. 19643)

Samengevoegde vragen van O. Maingain en M. Senecaut aan de minister van Justitie over 'de klacht die Belgacom heeft ingediend nadat zijn intern computersysteem werd gehackt' (*Hand*. Kamer, 2012-13, 2 oktober 2013, CRIV53COM824, 11, Vr. nrs. 19703 en 19716)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'Belgische jihadstrijders' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 309, Vr. nr. 684)

Vraag van J. Galant aan de minister van Binnenlandse Zaken over de 'dodelijke schietpartij op de A8-autosnelweg – ontdekking van een wapenarsenaal in de woning van de neergeschoten gangster – terreurdreigingsniveau' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 317, Vr. nr. 889)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over de 'radicalisering van jongeren – invloed/tips uit Saoedi-Arabië, Tsjetsjenië en Quatar' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 322, Vr. nr. 891)

Vraag van B. Slegers aan de minister van Binnenlandse Zaken over de 'terrorismeaanpak – gesprekken met de Amerikaanse autoriteiten' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 345, Vr. nr. 973)

Vraag van Ph. Blanchart aan de minister van Binnenlandse Zaken over de 'inlichtingendienst van de Europese Unie (SitCen)' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 351, Vr. nr. 1118)

Vraag van D. Bacquelaine aan de minister van Justitie over de 'sluiting van provincieposten van de Veiligheid van de Staat – gebrek aan financiële en personele middelen' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 382, Vr. nr. 1047)

Vraag van I. De Meulenmeester aan de minister van Overheidsbedrijven over 'het bezoek van minister Labille aan Rwanda in juni 2013' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 464, Vr. nr. 584)

Vraag van J. Van den Bergh aan de staatssecretaris voor Leefmilieu over 'prioritaire voertuigen' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 582, Vr. nr. 150)

Vraag van K. Calvo aan de staatssecretaris voor Leefmilieu over 'de controle eindgebruiker na intra-EU nucleaire export' (*Vr. en Ant*. Kamer 2012-13, 4 oktober 2013, QRVA 130, 588, Vr. nr. 158)

Vraag van K. Grosemans aan de minister van Landsverdediging over 'het toezicht op het ISTAR-bataljon' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM826, 7, Vr. nr. 19436)

Samengevoegde vragen van K. Grosemans en Ch. Lacroix aan de minister van Landsverdediging over 'de waarschuwingen per e-mail voor dreigende aanslagen op militairen' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM826, 9, Vr. nrs. 19449 en 19595)

Samengevoegde vragen van J. Galant, J. Van Esbroeck en B. Slegers aan de minister van Binnenlandse Zaken over 'de verscherpte veiligheidsmaatregelen en het verslag van het Comité P waarin brandhout wordt gemaakt van het gegevensbeheer op het stuk van terrorisme, radicalisme en extremisme' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM830, 7, Vr. nrs. 19452, 19473 en 19763)

Samengevoegde vragen van P. Dedecker, S. Van Hecke, R. Deseyn S. Lahaye-Battheu en T. Veys aan de minister van Overheidsbedrijven over 'de spionage bij Belgacom' (*Hand*. Kamer, 2013-14, 9 oktober 2013, CRIV53COM831, 29, Vr. nrs. 19670, 105, 108, 20082, 20083, 20084, 20142 en 20154)

Vraag van A. Frédéric aan de minister van Binnenlandse Zaken over 'het vertrouwelijke verslag van de Veiligheid van de Staat over de pogingen van de Scientologykerk om onze politici te benaderen' (*Hand*. Kamer, 2013-14, 23 oktober 2013, CRIV53COM839, 4, Vr. nr. 19591)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'de bevoegdheden voor privébewakingsfirma's' (*Hand*. Kamer, 2013-14, 23 oktober 2013, CRIV-53COM839, 10, Vr. nr. 19679)

Samengevoegde vragen van D. Ducarme, B. Somers en P. Logghe aan de minister van Binnenlandse Zaken over 'de trainingskampen voor jihadstrijders in de Ardennen' (*Hand*. Kamer, 2013-14, 24 october 2013, CRIV53PLEN165, 2, Vr. nrs. 2000, 2001 en 2002)

Samengevoegde vragen van H. De Croo, G. Dallemagne, R. Deseyn, P. Dedecker en P. Logghe aan de minister van Binnenlandse Zaken over 'afluisterpraktijken' (*Hand*. Kamer, 2013-14, 24 october 2013, CRIV53PLEN165, 17, Vr. nrs. 2010, 2011, 2012, 2013 en 2014)

Vraag van de J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'de kosten veroorzaakt door Sharia4Belgium' (*Vr. en Ant*. Kamer 2013-14, 4 november 2013, QRVA 134, 148, Vr. nr. 700)

Vraag van K. Grosemans aan de minister van Binnenlandse over de 'deelname van de ADIV aan het werkbezoek van de minister aan Turkije' (*Vr. en Ant*. Kamer 2013-14, 4 november 2013, QRVA 134, 155, Vr. nr. 974)

Vraag van R. Deseyn aan de minister van Binnenlandse Zaken over 'het PRISM-systeem' (*Vr. en Ant*. Kamer 2013-14, 4 november 2013, QRVA 134, 165, Vr. nr. 1012)

Vraag van H. Bonte aan de minister van Justitie over 'de risicovolle traagheid bij Justitie' (*Hand*. Kamer, 2013-14, 6 november 2013, CRIV53COM846, 24, Vr. nr. 20597)

Samengevoegde vragen van J. De Potter, D. Bacquelaine, P. Logghe en J. Van Esbroeck aan de minister van Binnenlandse Zaken over 'de radicalisering van jongeren en de genomen maatregelen' (*Hand*. Kamer, 2013-14, 12 november 2013, CRIV53COM850, 46, Vr. nrs. 20399, 20410, 20412 en 20433)

Samengevoegde vragen van D. Thiéry, Ch. Lacroix et D. Ducarme aan de minister van Landsverdediging over 'de samenwerking mer Amerikaanse inlichtingendiensten in het kader van onze militaire cyberdefensie' (*Hand*. Kamer, 2013-14, 13 november 2013, CRIV53COM851, 1, Vr. nrs. 19438, 19875, 20643 en 20749)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'Belgische burgers bij Al-Shabaab' (*Vr. en Ant*. Kamer 2013-14, 18 november 2013, QRVA 136, 78, Vr. nr. 1186)

Vraag van G. D'haeseleer aan de minister van Justitie over 'de extra bezoldigingen of vergoedingen van vakbondsafgevaardigden in beheerscomités en andere raden/ commissies' (*Vr. en Ant*. Kamer 2013-14, 18 november 2013, QRVA 136, 112, Vr. nr. 1020)

Vraag van Ch. Brotcorne aan de minister van Justitie over 'proselietenmakerij in de gevangenis van Bergen – radicale islam' (*Vr. en Ant*. Kamer 2013-14, 18 november 2013, QRVA 136, 127, Vr. nr. 1059)

Samengevoegde vragen van P. Logghe en J. Van Esbroeck aan de minister van Justitie over 'de verklaringen van een salafistische predikant' (*Hand*. Kamer, 2013-14, 4 december 2013, CRIV53COM879, 1, Vr. nrs. 20784 en 20807)

Samengevoegde vragen van J. Van Esbroeck en P. Logghe aan de minister van Justitie over 'de terugkeer van minderjarige strijders uit Syrië' (*Hand*. Kamer, 2013-14, 4 december 2013, CRIV53COM879, 5, Vr. nrs. 20805, 20833 en 21065)

Vraag van R. Deseyn aan de minister van Landsverdediging over 'het PRISM-systeem' (*Vr. en Ant*. Kamer 2013-14, 9 december 2013, QRVA 139, 71, Vr. nr. 614)

Vraag van E. Brems aan de minister van Buitenlandse Zaken over 'de opvang van gedetineerden in Guantanamo' (*Vr. en Ant*. Kamer 2013-14, 9 december 2013, QRVA 139, 92, Vr. nr. 574)

Vraag van E. Brems aan de minister van Buitenlandse Zaken over 'de Belgisch-Iraanse spion' (*Vr. en Ant*. Kamer 2013-14, 9 december 2013, QRVA 139, 132, Vr. nr. 650)

Vraag van P. Logghe aan de minister van Binnenlandse Zaken over 'het vertrek van minderjarigen naar Syrië' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 140, 146, Vr. nr. 930)

Vraag van P. Logghe aan de minister van Justitie over 'Radicalisering van jongeren – invloed/tips uit Saoedi-Arabië, Tsjetsjenië en Quatar' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 140, 244, Vr. nr. 1114)

Vraag van T. Francken aan de minister van Justitie over 'inzet van de Dienst voor de Veiligheid van de Staat voor de beveiliging van de Koning en zijn entourage' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 140, 271, Vr. nr. 1175)

Vraag van T. Francken aan de minister van Landsverdediging over 'inzet van de militaire veiligheidsdienst ADIV voor de beveiliging van de Koning en zijn entourage' (*Vr. en Ant*. Kamer 2013-14, 16 december 2013, QRVA 141, 194, Vr. nr. 621)

BIJLAGE D.
EERSTE TUSSENTIJDSE VERSLAG VAN HET TOEZICHTSONDERZOEK NAAR DE INFORMATIEPOSITIE VAN DE BELGISCHE INLICHTINGENDIENSTEN TEN AANZIEN VAN DE MOGELIJKHEDEN VAN BEPAALDE STATEN TOT MASSALE DATA-CAPTATIE EN -MINING EN VAN DE WIJZE WAAROP DEZE STATEN AAN POLITIEKE SPIONAGE ZOUDEN DOEN VAN ZOGENAAMDE 'BEVRIENDE LANDEN' (PRISM)

I. INLEIDING

Op 6 juni 2013 publiceerden *The Guardian*[203] en *The Washington Post*[204] voor het eerst informatie uit de tienduizenden (geclassificeerde) documenten die door Edward Snowden, die verschillende functies heeft vervuld in of voor Amerikaanse inlichtingendiensten, waren gelekt. Sindsdien volgden nieuwe onthullingen elkaar op met de regelmaat van de klok.

De berichten gaven een inkijk in uitermate geheime programma's van voornamelijk de NSA. Ze onthulden onder meer het bestaan van het zogenaamde PRISM-programma waarbij de NSA massaal (meta)data van telecommunicatie verkrijgt en brachten aan het licht dat Amerikaanse maar ook Britse diensten inlichtingenoperaties hebben opgezet ten aanzien van bepaalde internationale instellingen en samenwerkingsverbanden (VN, EU en G20) waarbij ook 'bevriende landen' werden geviseerd.

Deze onthullingen waren het startschot voor vele (parlementaire, gerechtelijke en inlichtingen-[205]) onderzoeken over heel de wereld. Zo ook in België. Op 1 juli 2013 vroeg de Begeleidingscommissie van de Senaat aan het Vast Comité I '*[…] een update van de bestaande informatie over de praktijken op het vlak van datamining. Niet alleen de Amerikaanse inlichtingendienst NSA zou dit doen, maar ook het Verenigd Koninkrijk zou massaal gegevens onderscheppen en analyseren. In de tweede plaats wil de begeleidingscommissie dat het Comité I onderzoekt welke de gevolgen zijn voor de bescherming van het economisch en wetenschappelijk potentieel van ons land, een van de wettelijke opdrachten van onze inlichtingendiensten. Ten slotte wenst de begeleidingscommissie dat het Comité I onderzoekt hoe dergelijke praktijken worden getoetst aan de nationale en internationale rechtsregels die de privacy van burgers beschermen.*'

---

203 G. GREENWALD en E. MACASKILL, *The Guardian*, 6 juni 2013 ("NSA Taps in to Internet Giant's Systems to Mine User Data, Secret files Reveals").

204 B. GELLMAN en L. POITRAS, *The Washington Post*, 6 juni 2013 ("US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program").

205 Zo bijvoorbeeld in het Europese Parlement, waar Senator en lid van de Begeleidingscommissie Armand De Decker, samen met voorzitter van het Vast Comité I Guy Rapaille, werd gehoord voor het *LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens* over 'The role of Parliamentary oversight of intelligence services at national level in an era of mass surveillance' (zie hierover: www.europarl.europa.eu/committees/en/libe/events.html) en binnen de schoot van de Verenigde Naties (J. KASTRENAKES, *The Verge*, 3 december 2013 ("United Nations Counterterrorism Official Launches Investigation into NSA Surveillance")).

Het Vast Comité I heeft daarop drie toezichtonderzoeken geopend die uiteraard nauw met elkaar verweven zijn. Dit geldt ook voor een vierde onderzoek dat werd geïnitieerd op klacht van de voorzitter van de Nederlandse Orde van advocaten bij de Balie van Brussel.

Het **eerste toezichtonderzoek,** waarvan voorliggend verslag het eerste tussentijdse resultaat is, wil een antwoord bieden op volgende vragen:

– Over welke mogelijkheden beschikken grootmachten als de Verenigde Staten en Groot-Brittannië om op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren en over welke gegevens gaat het (zowel kwantitatief als kwalitatief)?
– In welke mate waren de Belgische inlichtingendiensten op de hoogte van de mogelijkheden van deze grootmachten (of in welke mate dienden ze er – gegeven hun wettelijke opdrachten – van op de hoogte te zijn)? Werden hierover inlichtingen gecollecteerd of werd dit niet wenselijk geacht? Bieden onze diensten voldoende bescherming ter zake?
– Wat is de betekenis/waarde van de notie 'bevriende staat' in de context van inlichtingendiensten en in welke mate bepaalt die notie de houding van onze eigen inlichtingendiensten? Alhoewel dit aspect van de onthullingen (met name bepaalde operaties van inlichtingendiensten van zogenaamde 'bevriende landen' ten aanzien van internationale of supranationale instellingen waarin België vertegenwoordigd is of ten aanzien van Belgische belangen) niet expliciet in de vraagstelling van de Begeleidingscommissie was opgenomen, heeft het Vast Comité I beslist om ook hieraan aandacht te besteden, en dit gelet op het intrinsieke belang van deze vraag.

Het eerste toezichtonderzoek omvat drie luiken:

– Een door een externe expert (met name drs. Mathias Vermeulen, VUB en *European University Institute,* Firenze) aan de hand van open bronnen opgesteld overzicht van de soorten 'gegevens' die mogelijks betrekking hebben op of afkomstig zijn van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) en die door overheidsdiensten of private firma's in opdracht van de Amerikaanse en Britse overheid op grote schaal worden gecapteerd en opgeslagen en dit met het oog op een (eventuele latere) exploitatie door hun inlichtingendiensten.[206]
– Een analyse van de informatie die actueel beschikbaar is op het Comité onder meer op basis van BIM-dossiers en afgesloten toezichtonderzoeken (zoals de onderzoeken naar Echelon, SWIFT, Echelon bis, de inlichtingenactiviteiten van de ADIV in het buitenland …). Daarnaast werden derden bevraagd die mogelijks over relevante informatie beschikten.
– Een evaluatie van de inlichtingenpositie van de Veiligheid van de Staat (VSSE) en de Algemene Dienst inlichting en veiligheid (ADIV): wat wisten ze (of wat hoorden ze te weten) en hoe zijn ze met die informatie en kennis omgesprongen? Wat dit luik betreft, werden beide inlichtingendiensten reeds tweemaal grondig bevraagd. De analyse van alle antwoorden noopte het Vast Comité I tot een derde vragenronde.

---

206 Het ontwerpverslag van drs. Vermeulen werd aan een kritische lezing onderworpen door een werkgroep binnen het Vast Comité I. Op aangeven van de werkgroep werden verduidelijkingen aangebracht en elementen toegevoegd. Tevens werd aan de expert, onder de vorm van een bijkomende opdracht, gevraagd om het verslag te *updaten*, om een glossarium op te stellen en om (mogelijke) 'linken' met België op te lijsten.

Het **tweede toezichtonderzoek**[207] behandelt de in België geldende rechtsregels ter bescherming van de privacy ten aanzien van middelen die toelaten om op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren. Qua internationale regels zal er uiteraard aandacht zijn voor artikel 8 EVRM (waarbij zowel de 'horizontale werking' van deze bepalingen en de eventuele 'positieve verplichtingen' die eruit voortvloeien voor een Staat, belicht worden), artikel 17 van het Verdrag inzake burgerrechten en politieke rechter (BUPO-verdrag), Richtlijn 95/46/EC van 24 oktober 1995 (met aandacht voor de uitzondering inzake data met betrekking tot de nationale veiligheid en voor de recente onderhandelingen om de Richtlijn te verscherpen), Verdrag nr. 108 van 28 januari 1981 van de Raad van Europa en de artikelen 7 en 8 van het Handvest van de Grondrechten van de Europese Unie. Maar ook meer specifieke regels zullen aan bod komen: de regels inzake Passenger Name Record, Swift, Safe Harbour … Ten slotte zullen de interne rechtsregels die betrekking hebben op de privacybescherming en dataprotectie, belicht worden: artikel 10 van de Grondwet, de Wet Verwerking Persoonsgegevens en haar uitvoeringsbesluit en de bepalingen die specifiek zijn voor de werking van inlichtingendiensten (bijvoorbeeld de grenzen gesteld aan de internationale uitwisseling van gegevens).

Daarnaast moet dit tweede toezichtonderzoek ook een overzicht bieden van de juridische mogelijkheden waarover Staten, burgers of bedrijven beschikken om actie te ondernemen tegen (mogelijke) inbreuken op (grond)rechten. In dit luik zal onder meer aandacht besteed worden aan de 'bruikbaarheid' van informatie die in het buitenland rechtmatig is verkregen maar in België nooit (op die wijze) had kunnen verkregen worden.

Ook voor dit tweede toezichtonderzoek werd een extern expert aangezocht. Het betreft Prof Annemie Schaus. Tevens werden de VSSE en de ADIV bevraagd omtrent bovenstaande regels en juridische mogelijkheden voor Staten, burgers en bedrijven. Ten slotte wordt informatie uitgewisseld met de Belgische Privacycommissie.

Het **derde toezichtonderzoek**[208] behandelt de mogelijke implicaties van datamining op de bescherming van het wetenschappelijk en economisch potentieel van het land. Het wil nagaan of de Belgische inlichtingendiensten:

- aandacht hebben besteed aan dit fenomeen;
- een reële of mogelijke bedreiging hebben gedetecteerd voor het Belgische wetenschappelijk en economisch potentieel;
- er de bevoegde overheden van in kennis hebben gesteld en beschermingsmaatregelen hebben voorgesteld; en
- over voldoende en adequate middelen beschikken om deze problematiek op te volgen.

---

207 Toezichtonderzoek naar de in België geldende regels ter bescherming van de privacy ten aanzien van middelen die toelaten op grote schaal gegevens van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) te onderscheppen en te exploiteren.

208 Toezichtonderzoek over de aandacht die de Belgische inlichtingendiensten (al dan niet) besteden aan de mogelijke dreigingen voor het Belgisch wetenschappelijk en economisch potentieel uitgaande van op grote schaal door buitenlandse grootmachten en/of inlichtingendiensten gehanteerde elektronische bewakingsprogramma's op communicatie- en informatiesystemen.

II. WOORD VOORAF BIJ HET EXPERTVERSLAG

Sinds de eerste gelekte NSA-slides en de opening van het toezichtonderzoek zijn onophoudelijk nieuwe (uitermate gevoelige) gegevens aan het licht gekomen die wijzen op massale datacaptatie én politieke en economische spionage van en bij bevriende landen. Daarbij gaat het al lang niet meer over PRISM, TEMPURA of de spionage van de G20 alleen. Dat zal ook overduidelijk worden bij het doornemen van het expertverslag.

Uiteraard dient het verslag met de nodige reserves te worden gelezen. Het is *quasi* uitsluitend gebaseerd op open bronnen. Wel ging de expert zeer kritisch te werk en werden al te speculatieve denkpistes of theorieën niet weergegeven. Toch wil het Comité hier reeds benadrukken dat het nog geen onderbouwde indicaties vond waaruit blijkt dat de Snowden-slides niet authentiek zouden zijn. Integendeel, uit de reeds verrichte onderzoeken meent het Comité te kunnen afleiden dat de onthullingen, zeker wat betreft de 'grote lijnen', waarheidsgetrouw zijn.[209] Dat daarbij – mede gelet op het fragmentarische karakter van de onthullingen[210] – geen zekerheid bestaat omtrent de waarachtigheid van *elk* (technisch) aspect van de zaak, doet geen afbreuk aan deze vaststelling. Hierbij moet ook rekening worden gehouden met het feit dat het expertverslag werd afgesloten op 23 oktober 2013. Nieuw vrijgegeven informatie of de contestatie vanuit officiële hoek van eerder becommentarieerde gegevens (zoals met betrekking tot – zie II.4) sluit een andere lezing van bepaalde aspecten van de zaak, niet uit.

Vooraf wil het Vast Comité I kort nog een aantal elementen toelichten. Ze moeten enerzijds een vlottere lezing van het uitgebreide en technische expertverslag toelaten en anderzijds de noodzakelijke context bieden waarbinnen dit verslag moet begrepen worden.

II.1. NIET ALLEEN DE NSA EN HET GCHQ

Het verslag bespreekt alleen de massale datacaptatie door het Amerikaanse *National Security Agency* en het Britse *Government Communications Headquarters* (GCHQ). Wellicht zijn er in deze landen nog andere diensten die aan massale data-captatie doen. En uiteraard zijn Amerika en Groot-Brittannië niet de enige grootmachten die op dergelijke wijze tewerk gaan.

In de marge van de Snowden-onthullingen zijn bijvoorbeeld ook de activiteiten van de Franse[211], Duitse[212] en Zweedse[213] inlichtingendiensten aangekaart. En natuurlijk zijn er

---

209 Daarbij moet ook rekening worden gehouden met het gegeven dat de Amerikaanse, noch de Britse overheden tot op heden de authenticiteit van de gelekte documenten betwijfeld hebben. Hooguit werd de interpretatie die er soms aan werd gegeven in open bronnen, betwist.

210 *The Guardian* zou vooralsnog slechts één procent van alle documenten die ze van Snowden kreeg, hebben gepubliceerd (X, *De Standaard*, 3 december 2013 ("Amper 1 procent van informatie Snowden gepubliceerd")).

211 *Le Monde* stelde bijvoorbeeld dat de Franse DGSE op een systematische manier de metadata van telefoon, fax en internetcommunicaties tussen een Frans en een buitenlands nummer '*voor jaren*' bewaart in haar hoofdkwartier. Zes andere diensten hebben toegang tot deze database (J. FOLLOROU en F. JOHANNES, *Le Monde*, 4 juillet 2013 ("Révélations sur le Big Brother français")).

212 A. REIβMANN, *Der Spiegel*, 13 november 2013 ("Uberwachung: BND soll weitgehenden Zugriff auf Internetverkehr in Deutschland haben").

213 T.T., *The Local*, 6 september 2013 ("Sweden 'a close partner' in NSA surveillance"). Zie ook: "Snowden papers unmask close technical cooperation and loose alliance between British, Ger-

ook de mogelijkheden die ontplooid kunnen worden door pakweg Rusland[214] en China.[215] Maar minstens even belangrijk in dit kader zijn de samenwerkingsverbanden inzake *Signal Intelligence* (SIGINT) die (zouden) bestaan tussen bepaalde landen. Het meest gekend is de zogenaamde FIVE EYES die naast de Amerika en Groot-Brittannië ook Canada, Australië en Nieuw-Zeeland tellen. Deze landen werken sinds decennia zeer nauw samen en gecapteerde datacommunicatie zou *quasi* ongelimiteerd worden uitgewisseld. Daarnaast werd in de pers bijvoorbeeld ook gewag gemaakt van de NINE EYES en de FOURTEEN EYES, waartoe volgens open bronnen ook België behoort.[216]

Ten slotte is massale data-captatie en -exploitatie geen monopolie van de overheid. Grote private spelers beschikken soms over gelijkaardige mogelijkheden, al ligt de finaliteit van hun activiteiten meestal elders. Deze problematiek werd om evidente redenen niet opgenomen in de toezichtonderzoeken van het Comité: ze ligt buiten zijn bevoegdheidssfeer.

II.2. NIET ALLEEN PRISM EN TEMPURA

De eerste onthullingen hadden vooral betrekking op – wat betreft de Amerikanen – het PRISM-programma en – wat betreft de Britten – TEMPURA. Deze twee inlichtingenprogramma's blijken een zeer belangrijke bron van informatie maar ze zijn zeker niet de enigen. Enigszins schematiserend zou men vijf[217] vormen of technieken van massale datacaptatie of 'ongerichte interceptie' van (tele)communicatie kunnen onderscheiden (II.2.1). Daarnaast zijn er de diverse mogelijkheden om deze bulk aan gegevens te bewaren en te exploiteren (II.2.2).

II.2.1. Vijf vormen van massale data-captatie

Het toezichtonderzoek van het Comité beperkt zich in essentie tot inlichtingenprogramma's of -technieken waarbij in essentie 'ongericht' gecapteerd wordt (ook '*phishing expedition*' genoemd) waarbij bij wijze van spreken een gigantisch fijnmazig net wordt uitgegooid en pas nadien, manueel of aan de hand van geautomatiseerde processen, wordt bekeken wat mogelijks relevant en nuttig is.

Het betreft dus *niet* het afluisteren van het telefoonverkeer van één persoon of instantie (ook al kan het gaan om veel én gevoelige gegevens). Een zuivere vorm van 'ongericht' capteren is bijvoorbeeld het aftappen en bewaren van *alle* informatie die via een internati-

man, French, Spanish and Swedish spy agencies", in: J. BOGER, *The Guardian*, 1 november 2013 ("GCHQ and European Spy Agencies Worked together on Mass Surveillance").

214 Zie in dat kader de beweringen over 'SORM': S. WALKER, *The Guardian*, 6 oktober 2013 ("Russia to monitor 'all communications' at Winter Olympics in Sochi").

215 X., *www.sophos.com*, 7 mei 2008 ("Belgium accuses Chinese government of cyber-espionage").

216 "*Beyond that, the NSA has other coalitions, although intelligence-sharing is more restricted for the additional partners: the 9-Eyes, which adds Denmark, France, The Netherlands and Norway; the 14-Eyes, including Germany, Belgium, Italy, Spain and Sweden […].*" (E. MACASKILL en J. BALL, *The Observer*, 2 november 2013 ("Portrait of the NSA: no detail too small in quest for total surveillance").

217 Uiteraard zijn andere voorstellingen, waarbij eventueel meer of minder vormen van massale datacaptatie worden onderscheiden, even waardevol.

onale internetkabel passeert om vervolgens op digitale wijze zoekingen te verrichten (datamining). Een ander voorbeeld is het capteren van alle gsm-signalen in een bepaalde regio.

Uit het expertverslag blijkt dat bij het capteren van bijvoorbeeld glasvezelkabels, meestal gewerkt wordt met zogenaamde '*selectors*': een gsm-nummer, een IP-adres of een bepaald woord (bijv. 'aanslag'). Dit betekent dat alle data die door de kabel passeren weliswaar gescreend worden op basis van die vooraf ingegeven parameters, maar dat alleen informatie die beantwoordt aan een of meerdere selectiecriteria effectief wordt weggeplukt en bewaard. In dit geval hangt de appreciatie van het feit of de captatie 'gericht' of 'ongericht' gebeurt grotendeels af van de hoeveelheid en van de omschrijving van de selectoren. Wanneer de 'selectoren' voornamelijk beperkt blijven tot welbepaalde gsm-nummers of IP-adressen dan lijkt de inlichtingengaring eerder 'gericht' (in de veronderstelling uiteraard dat er niet massaal veel nummers en adressen worden ingegeven). Worden daarentegen zeer ruime selectiecriteria gehanteerd (zoals het gebruik van bepaalde woorden, een domeinnaam (bijv. '@comiteri.be'), het gebruik van bepaalde zoektermen op internetzoekmachines of het gebruik van bepaalde toepassingen (bijvoorbeeld VPN-technieken of TOR) dan kunnen we er niet omheen dat er op ongerichte wijze wordt gecollecteerd. Alhoewel hierover (vooralsnog) geen volledige duidelijkheid bestaat, zijn de aanwijzingen dat er zeker ook ongericht, massaal gecapteerd wordt, overtuigend.

Vooraf willen we nog opmerken dat onderstaande 'technieken' zowel elkaar zowel kunnen aanvullen (bijvoorbeeld: omdat een e-mailbericht via een getapte kabel mogelijks niet volledig kan gelezen worden, kan het nuttig zijn het volledige bericht op te halen bij de *provider*) als overlappen (een gsm-gesprek kan rechtstreeks uit de ether zijn gehaald en ook van een kabel zijn geplukt).

II.2.1.1. Upstream-collectie

Upstream-collectie[218] is de naam die gegeven wordt aan het 'aftappen' van internet of telefoonverkeer dat via (internationale) (glasvezel)kabels verloopt, bijvoorbeeld door apparatuur te plaatsen op cruciale punten die uitgebaat worden door grote telecom-operatoren of door de kabel zelf rechtstreeks te tappen. Dit kan – zoals bij de meeste technieken – met of zonder medeweten van de operator/uitbater van de kabel.

TEMPURA is volgens de slides van Snowden de codenaam voor het Britse programma van deze vorm van captatie.

Omdat er door dergelijke kabels massaal veel gegevens passeren, worden naar alle waarschijnlijkheid 'filters' of 'selectoren' geplaatst (zie II.2.1) zodat alleen mogelijks relevante informatie moet worden opgeslagen en verwerkt.

---

218 *Upstream* of stroomopwaarts ten aanzien van de bestemmeling van de communicatie. Een voorbeeld: wanneer een persoon webmail gebruikt (dit wil zeggen vanaf zijn PC inlogt bij een dienstenverstrekker van webmail, zoals bijvoorbeeld de *outlook* van Microsoft) dan is hij in feite aan het werk op de server van deze dienstenverstrekker. Zijn mailbox staat niet op zijn eigen PC maar wel op een server op een andere locatie (zeer dikwijls in de USA). Het bericht dat wordt verzonden, kan dus worden onderschept tussen de betrokken persoon en de server.

II.2.1.2. Downstream-collectie

Een andere mogelijkheid om op massale wijze data te capteren is deze ophalen of – al dan niet onder dwang – opvragen bij telecomoperatoren zelf. Deze vorm van dataverwerving is gekend onder de naam downstream-collectie.[219] Het meest gekende voorbeeld vormt het PRISM-programma waarbij negen grote Amerikaanse technologiebedrijven bereid werden gevonden en/of verplicht waren/zijn om op gestructureerde wijze gebruikersdata aan te leveren. Het betreft Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple. Alhoewel PRISM ook werkt op basis van 'selectors' (zie II.2.1), blijkt uit het expertverslag dat op basis van dit programma massaal veel gegevens naar de NSA doorstroomden.

II.2.1.3. Draadloze communicatie onderscheppen

Heel wat (internationale) communicatie verloopt (ten dele) via elektromagnetische stralen: van klassieke radiosignalen tot meer moderne gsm-technologie dat via zendmasten en satellieten (kan) verlopen.

Het ongemerkt en massaal onderscheppen van deze signalen is technisch perfect mogelijk en laat toe in *real time* gesprekken te beluisteren. FORNSAT zou de codenaam zijn voor een van de programma's die zich richten op dergelijke captatie van communicatie die via satellieten verloopt. Maar ook de interceptie van communicatie vanuit tientallen Amerikaanse diplomatieke en consulaire posten verspreid over de hele wereld (F6 SITES), zou onder deze noemer kunnen geplaatst worden.

II.2.1.4. Hacken van IT-systemen

Een andere mogelijkheid om *en masse* interessant geachte gegevens te verzamelen, is het binnendringen in het IT-systeem van bijvoorbeeld een operator om ongezien alle nuttige informatie weg te sluizen. Dit was het geval met BICS, een dochteronderneming van Belgacom, die instaat voor *roaming* van telecommunicatie in grote delen van de wereld. Via de OPERATIE SOCIALIST[220] (*sic*) zouden de Britten er in geslaagd zijn om, met medewerking van de NSA, technisch zeer hoogstaande *malware* te installeren en zo naar alle waarschijnlijkheid een massa aan gegevens weg te sluizen. Maar BICS is hoogst waarschijnlijk niet de enige die zich in dit geval bevindt. Recente onthullingen spreken over tienduizenden computersystemen wereldwijd die zouden besmet zijn met *malware* van de NSA.[221]

---

219 *Downstream* of stroomafwaarts ten aanzien van de bestemmeling van de communicatie. Hier wordt de informatie betrokken uit de server van de dienstverstrekker zelf door bijvoorbeeld toegang te nemen tot de mailbox op die server of door de informatie te vragen.

220 X., *Der Spiegel*, 20 september 2013 ("Belgacom Attack: Britain's GCQH tracked Belgian Telecoms Firm").

221 S. DERIX en H. MODDERKOLK, *NRC Handelsblad*, 23 november 2013 ("De hackers van de NSA dringen overal binnen").

II.2.1.5. Samenwerking en uitwisseling van gegevens

Een laatste 'methode' is het in bulk uitwisselen van informatie tussen partnerdiensten. Soms gebeurt die 'spontaan', soms binnen het kader van een samenwerkingsverband waarbij dan iedere betrokken dienst de *monitoring* van een bepaald aspect van de (tele) communicatie voor zijn rekening neemt en de verzamelde gegevens vervolgens doorgeeft. Het hoeft geen betoog dat – zoals overigens blijkt uit de open bronnen – hierbij het gevaar bestaat dat dienst A doet wat dienst B niet mag volgens zijn nationale wetgeving en omgekeerd en waarbij men de gegevens met elkaar deelt zodat de wettelijke beperkingen *de facto* worden omzeild.[222]

Het meest gekende samenwerkingsverband is de FIVE EYES. De landen die er deel van uitmaken, delen bijvoorbeeld de informatie die zij elk afzonderlijk uit de glasvezelkabel halen die op hun grondgebied passeren. Maar ook andere landen geven massaal vergaarde data in bulk door. Zo zouden bijvoorbeeld de Noren, de Fransen en de Nederlanders op een periode van een maand tijd verschillende miljoenen gegevens hebben doorgespeeld.[223]

II.2.2. Bewaren en exploiteren van bulkinformatie

Het is natuurlijk zinloos om massaal veel data te capteren – volgens *The Washington Post* onderschept de NSA elke dag 1,7 miljard e-mailberichten en andere vormen van communicatie –wanneer die niet kunnen bewaard en geëxploiteerd worden. Gelet op de enorme hoeveelheden data die de diverse programma's samen genereren, is niet alleen gigantische *hardware* nodig om gegevens te stockeren maar ook performante *software* die toelaat de spreekwoordelijke speld in de hooiberg te vinden.

XKEYSCORE stelt de NSA-analisten onder meer in staat om *upstream*-informatie te verwerken. Ongetwijfeld verloopt een deel van de analyse ook geautomatiseerd waarbij algoritmen speuren naar vooraf bepaalde 'patronen' en 'anomalieën' in de gegevens. Maar het is ook mogelijk bulkgegevens aan partnerlanden of –diensten te geven voor verdere analyse.

II.3. WELK SOORT GEGEVENS WORDEN GECAPTEERD VIA DE AMERIKAANSE EN BRITSE SIGINT?

Alhoewel hierover in het begin geen zekerheid bestond, is snel duidelijk geworden dat de diverse programma's niet alleen metadata capteren (zoals bijvoorbeeld het adres van afzender en bestemmeling, de connectie-identificatie, het tijdstip en duur, het gebruikte

---

222 "*De Amerikaanse inlichtingendienst bespioneerde volgens The Gardian sinds 2007 in ruime mate de gegevens van Britse burgers – en dat met gedoging van Londen.*" (X, De Morgen, 22 november 2013 ("Britse burgers massaal bespioneerd").

223 Dit werd publiekelijk toegegeven onder meer door de Noorse inlichtingendienst en door NSA-officials die zich verplicht voelden om een vermeende verkeerde lezing van bepaalde Snowden-slides door journalisten recht te zetten. De journalisten waren immers van mening dat het in elk van die landen om door de NSA afgetapte communicaties ging (VHN, *De Standaard*, 27 november 2013 ("Noorse inlichtingendienst betwist claims over NSA-spionage")).

technische middel, de grootte van een bestand …) maar ook de pure inhoud van berichten, of deze nu verzonden zijn via gsm, telefoon, interne voip-mail, chats, online forumberichten, clouding, e-mailattachments, Skype …

Er is door de Amerikaanse overheid lang beweerd dat alleen berichten die gerelateerd zijn aan terrorisme, werden onderschept. Maar ook hier hebben de open bronnen op overtuigende wijze aangetoond dat de interesse en de bevoegdheidssfeer van bijvoorbeeld de NSA vele malen ruimer is: ook economische en politieke informatie blijkt een target.

II.4. WAT MET PERSOONS-, ECONOMISCHE – OF POLITIEKE GEGEVENS VAN EN OVER BELGEN EN BELGIË?

De onophoudelijke onthullingen doen verwerkingscapaciteiten vermoeden van meerdere peta-bytes per dag of van miljarden metadata over langere periodes. Dat het virtuele net dat grote inlichtingendiensten over de digitale wereld hebben gespannen, een nooit geziene captatie toelaat, lijkt dan ook aangetoond.

Maar het Vast Comité I is vanzelfsprekend voornamelijk geïnteresseerd in de eventuele onderschepping van gegevens die betrekking hebben op of afkomstig zijn van in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België). Vooralsnog is hierover weinig specifieks bekend.

Het zou echter naïef zijn te besluiten dat wij als een van de enige Europese landen buiten schot zijn gebleven, zeker gelet op de aanwezigheid van belangrijke internationale organisaties op ons grondgebied. Mogelijks brengen nieuwe onthullingen hierover meer klaarheid.

Los daarvan zijn er in het expertverslag heel wat elementen aanwezig die doen besluiten dat 'Belgische data' noodzakelijkerwijs op grote schaal werden onderschept.

Alleen al de wijze waarop de NSA bepaalde gebruikersdata verkrijgt bijvoorbeeld, impliceert per definitie dat ook gegevens van Belgen kunnen gecapteerd worden. Immers talrijke landgenoten maken dagelijks gebruik van de diensten van een van de negen Amerikaanse bedrijven die opgenomen zijn in het PRISM-programma (Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple).

Maar ook voor *upstream*-collecte zijn Belgische data niet immuun. E-mails of chats kunnen bepaalde 'selectors' triggeren wanneer zij bijvoorbeeld – wat veelal het geval is – passeren via een kabel die over het Amerikaanse grondgebied loopt.

Daarbij is het van belang te weten dat een (deel van een) elektronische boodschap die vanuit België naar een ander land verstrekt veelal via Amerika reist. De route die een bericht (of een deel van een bericht) neemt, hangt af van de verkeersdensiteit of de kost op een bepaald moment op een bepaald traject, en dus niet van wat de geografisch kortste weg is. Heel veel informatie op het internet reist via de USA omdat zich daar de grootste vervoerscapaciteit van en naar de andere landen van de wereld bevindt, zelfs al moeten de berichten daarvoor een 'omweg' van duizenden kilometers maken. En wat de Amerikaanse diensten is ontgaan, hebben de Britse mogelijks onderschept via hun mogelijkheden om glasvezelkabels te tappen. In dezelfde context kan melding worden gemaakt van het feit dat de GCHQ data zou aftappen van de interne glasvezelverbindingen tussen Google's data centers. Daarbij moet opgemerkt dat een van de belangrijkste datacenters van Google in België ligt.

Verder worden metadata van 'Belgische gesprekken' verzameld indien Belgen rechtstreeks communiceren met een Amerikaan die door de NSA als *target* wordt beschouwd, maar ook indien ze communiceren met een 'contact van een contact' van die persoon.

Een totaal ander voorbeeld vormt de onthulling dat de NSA-divisie die instaat voor 'internationale veiligheid', onder meer focust op 'de buitenlandse politiek en handelsrelaties van België'.[224]

Ten slotte is er uiteraard de *hacking* van BICS/Belgacom. Alhoewel hier naar alle waarschijnlijkheid weinig 'puur' Belgische data zijn verzameld, kunnen we er natuurlijk niet om heen dat dit overheidsbedrijf deel uitmaakt van de Belgische kritieke infrastructuur.

III. TER AFRONDING

Dat bepaalde grootmachten – zoals de Verenigde Staten – al geruime tijd over verregaande middelen en programma's beschikten om aan massale data-captatie te doen, is algemeen geweten. Bij wijze van voorbeeld kunnen we hier verwijzen naar de onthullingen inzake het Echelon-netwerk en de Swift-zaak.[225]

Maar vandaag worden we geconfronteerd met twee nieuwe elementen.

Vooreerst is er het gegeven dat de elektronische spionage alomvattend en massaal plaatsgrijpt vanuit honderden SIGADS (dataverzamelingspunten) verspreid over de hele wereld en dit met de meest geavanceerde soft- en hardware en een ongekende inzet aan menselijke en financiële middelen. Weinige communicatiemiddelen of –berichten schijnen te kunnen ontsnappen aan een mogelijke onderschepping. Dat dit gebeurd is vanuit een inlichtingencontext is niet eens zo verwonderlijk. Bijvoorbeeld biedt de internettechnologie, inclusief alle communicatievormen die zich via het internet voordoen, een gedroomde bron van gedetailleerde gegevens die voordien onbereikbaar waren. Met de digitalisering opende zich een nieuwe dimensie voor de inlichtingenwereld, waarvan iedereen zich bewust moet zijn.

Tweede nieuwe element is dat er vandaag met quasi zekerheid – in de vorm van interne, officiële overheidsdocumenten (o.a. gelekte slides) – elementen voorhanden zijn die deze captaties en hun omvang aantonen.

---

224 X., *De Tijd*, 4 september 2013 ("Staatsveiligheid onderzoekt spionage door NSA").

225 Minder gekend is het feit dat er vóór Snowden reeds andere klokkenluiders bepaalde praktijken van de NSA hebben aangeklaagd. Zo bijvoorbeeld brachten voormalig NSA-medewerkers William Binney, Thomas Andrew Drake en Thomas Tamm in het begin van de jaren 2000 bepaalde collecte-programma's in de openbaarheid.

DE SNOWDEN-REVELATIES, MASSALE DATA-CAPTATIE EN POLITIEKE SPIONAGE

Open bronnenonderzoek[226]

INLEIDING

1. Dit verslag biedt een overzicht – aan de hand van open bronnen[227] – van de soorten gegevens die mogelijks betrekking hebben op (of afkomstig zijn van) in België verblijvende personen, organisaties, ondernemingen of instanties (of die enige link hebben met België) en die door het Amerikaanse National Security Agency (NSA) het Britse Government Communications Headquarters (GCHQ), of private firma's in opdracht van deze diensten, op grote schaal worden gecapteerd en opgeslagen en dit met het oog op een (eventuele latere) exploitatie door hun inlichtingendiensten. Tevens werd een overzicht geboden van gevallen waaruit blijkt dat onder meer deze diensten de afgelopen decennia operaties hebben opgezet die gericht waren op politiek spionage ten aanzien van zogenaamde 'bevriende landen'. De open bronnen die voor dit verslag geconsulteerd werden zijn van wisselende kwaliteit. Waar mogelijk werd zoveel mogelijk gebruikt gemaakt van primaire bronnen (*slideshows*, officiële documenten) die in de laatste maanden gepubliceerd werden door onderzoeksjournalisten. De kritische interpretatie van deze (onvolledige) stukken informatie werd geholpen door de consultatie van andere experten. Te speculatieve persanalyses waarbij geen extra informatie gevonden werd ter ondersteuning van een denkpiste werden niet weerhouden. Als bijlage bij dit verslag werd een verklarende afkortingenlijst opgenomen.

2. Om de specifieke collectiemechanismen die onthuld werden sinds juni 2013 beter te begrijpen, is het vooreerst evenwel nodig om summier de wettelijke context te beschrijven waarin respectievelijk de NSA en GCHQ actief zijn, om vervolgens inzicht te krijgen in het mandaat en de voorzorgsmaatregelen die al dan niet van toepassing zijn in de uitvoering van dat mandaat. Ook werd getracht om telkens een inzicht te krijgen in de grootteorde van de gegevensverzameling en de tijdsspanne waarin deze collectiemechanismen actief zijn.

---

226 Dit open bronnenonderzoek werd in opdracht van het Vast Comité I uitgevoerd door drs. Mathias Vermeulen, Research Fellow aan het European University Institute in Firenze en het Centre for Law, Science and Technology Studies aan de VU Brussel. Werkte van 2008 tot 2011 als onderzoeker voor de toenmalige United Nations Special Rapporteur on the promotion and protection of human rights while countering terrorism, en deed onderzoek voor het Europese Parlement over 'Parliamentary oversight of security and intelligence agencies in the European Union'. Zie:www.europarl.europa.eu/document/activities/cont/201109/20110927ATT27674/20110927ATT27674EN.pdf).

227 De expert ging zeer kritisch te werk en werden al te speculatieve denkpistes of theorieën niet weergegeven. Nieuw vrijgegeven informatie of de contestatie vanuit officiële hoek van eerder becommentarieerde gegevens sluit een andere lezing van bepaalde aspecten van de zaak, niet uit.

3. De ervaring met de Snowden-documenten tot nu toe leert dat vooralsnog ongepubliceerde, vertrouwelijke documenten die mogelijks in de toekomst gepubliceerd zullen worden, een impact zullen hebben op de interpretatie van eerdere gepubliceerde documenten en berichtgeving over de revelaties. Deze nota is dus onvermijdelijk een tijdsopname, die een stand van zaken weergeeft tot en met 23 oktober 2013.

I. HET AMERIKAANSE NATIONAL SECURITY AGENCY (NSA)

4. De NSA is een militaire inlichtingendienst die geleid wordt door Generaal Keith B. Alexander. Alexander rapporteert aan de Under Secretary of Defense for Intelligence, Michael G. Vickers, de voornaamste intelligence-adviseur van de Amerikaanse Minister van Defensie, Chuck Hagel. De NSA is ook een onderdeel van de US 'Intelligence Community', die geleid wordt door James Clapper. Volgens EO 12333 heeft de directeur van de NSA (DIRNSA) onder meer de taak om *signals intelligence* (SIGINT[228]) te verzamelen (inclusief via clandestiene middelen), verwerken, analyseren, produceren en te verspreiden voor *foreign intelligence* en *counterintelligence* doelen[229] en om militaire operaties te ondersteunen.[230] De NSA's SIGINT-verzameling is geregeld door twee belangrijke documenten: Executive Order 12333 (EO 12333)[231] en de Foreign Intelligence Surveillance Act (FISA).

I.1. HET WETTELIJKE KADER VOOR HET INZAMELEN VAN INFORMATIE OVER BUITENLANDSE DOELWITTEN

I.1.1. Executive Order 12333

5. *Foreign intelligence*' wordt in EO 12333 gedefinieerd als alle informatie die gerelateerd is aan de capaciteiten, intenties of activiteiten van buitenlandse machten, organisaties of personen.[232] Het verzamelen van SIGINT kan gebaseerd worden louter en alleen op basis

---

228 SIGINT is *intelligence* die gecreëerd wordt door elektronische signalen en systemen, zoals communicatiesystemen, radars, satellieten of wapensystemen. Zie hierover bijvoorbeeld www.nsa.gov/sigint/.

229 Executive Order 12333 – United States intelligence activities, 4 December 1981, sectie 1.7(c)(1). EO 12333 werd geamendeerd door de Executive Orders 13284 (2003), 13355 (2004) en 13470 (2008). De geconsolideerde versie van EO 12333 is consulteerbaar op https://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf. Er moet opgemerkt worden dat EO 12333 de activiteiten van alle leden van de US Intelligence Community regelt, en dus niet alleen van de NSA.

230 *Idem*, sectie 1.7(c)(3) en (5).

231 Voor EO 12333 was er al EO 12139 (Exercise of Certain Authority Respecting Electronic Surveillance), die werd geamendeerd door EO 12333, EO 13383 en EO 13475.

232 *Idem*, sectie 3.5(e). EO 12333 maakt ook duidelijk dat *foreign intelligence* niet alleen via SIGINT kan verzameld worden, maar ook door andere elementen van de *intelligence community* kan gebeuren via fysieke surveillance (zie bijv. sectie 2.4(d) "*Physical surveillance of a United States person abroad to collect foreign intelligence, except to obtain significant information that cannot reasonably be acquired by other means*".

van deze *executive order*, zonder dat daarbij de uitgebreidere FISA-procedures moeten gevolgd worden.[233] EO 12333 vormt bijvoorbeeld de wettelijke basis voor het verwerven van enorme hoeveelheden metadata buiten Amerikaans grondgebied[234], alsook voor het verzamelen van contactlijsten of adresboeken van e-mail- en chatprogramma's.[235] Dat soort informatie valt immers niet onder de definitie van *electronic surveillance* zoals FISA die gebruikt.[236] EO 12333 lijkt ook de wettelijke basis te vormen voor de meest controversiële activiteiten van de NSA, en dan vooral van subdivisies zoals het Office of Tailored Access Operations (TAO) en de Special Collection Service (SCS), zoals het omzeilen van commerciële encryptiebeveiligingen[237], het hacken van buitenlandse computers[238] of het bespioneren van buitenlandse leiders vanuit Amerikaanse ambassades.[239] Er is weinig tot geen toezicht over deze activiteiten door het US Senate Intelligence Committee.[240]

I.1.2. Foreign Intelligence Surveillance Act

6. Een groot deel van de 'elektronische surveillance' wordt geregeld door de Foreign Intelligence Surveillance Act (FISA) uit 1978. FISA werd gecodificeerd in 50 U.S.C. § 1801 *et seq*., en werd daarna onder meer significant aangevuld met nieuwe provisies uit de Patriot Act[241], die onder meer de installatie en het gebruik van 'pen registers'[242] en '*trap*

---

233 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships. 9 Augustus 2013 (www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 2).

234 Foreign Intelligence Surveillance Court, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13 – 109, 29 August 2013 op pag. 10, n.10. ("*The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders*".) Zie ook paragraaf 15.

235 Zie paragrafen 25-27.

236 US Code Title 50 – War and National Defence, 50 USC 1801(f).

237 Zie paragrafen 45-48.

238 Zie bijvoorbeeld paragrafen 29, 47 en 48.

239 Zie bijvoorbeeld paragraaf 19.

240 Een staflid van het Committee hierover: "*In general, the committee is far less aware of operations conducted under 12333 (…). I believe the NSA would answer questions if we asked them, and if we knew to ask them, but it would not routinely report these things, and, in general, they would not fall within the focus of the committee*." www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html.

241 Zie 50 U.S.C. § 1841 *et seq*.

242 Een '*pen register*' wordt gedefinieerd in 18 U.S.C. § 3127(3) als "*a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business*".

and trace devices'[243] en het produceren van 'tastbare dingen' regelen.[244] FISA werd het meest recent geamendeerd in 2008 door de FISA Amendments Act (FAA).[245] In december 2012 verlengde de Amerikaanse Senaat de werking van de FISA Amendments Act tot en met 31 december 2017. Volgens de NSA is de belangrijkste toepassing van FAA het verzamelen van de communicaties van buitenlandse personen die Amerikaanse aanbieders van communicatiediensten gebruiken.[246] Momenteel liggen er verschillende wetgevende voorstellen op tafel die de binnenlandse collectie van informatie door de VS zou moeten beperken[247], maar tot nu toe zijn er geen gelijkaardige initiatieven om de collectie van informatie van 'buitenlanders' in te perken.[248] In dit verslag zal alleen verder ingegaan worden op de recentste FISA-Amendments Act, die op zich een aanvulling vormen op 50 USC § 1802. Onder 50 U.S.C. § 1802 kan de Amerikaanse Procureur-Generaal (*Attorney-General*) elektronische surveillance machtigen voor een periode van één jaar als die surveillance exclusief gericht is op (1) het verwerven van de inhoud van de communicaties die uitgezonden worden communicatiemiddelen die alleen door of tussen 'buitenlandse machten'[249] gebruikt worden of (2) het verwerven van *technical intelligence* van plaatsen die onder de openlijke en exclusieve controle van een 'buitenlandse macht' staan.

7. De FISA Amendments Act geeft de AG en de DNI de bevoegdheid om voor een periode van één jaar elektronische surveillance te machtigen van personen waarvan redelijkerwijs kan aangenomen kan worden dat die zich buiten de Verenigde Staten bevinden, met als specifiek doel om 'buitenlandse inlichtingen' te verzamelen.[250] 'Buitenlandse inlichtingen' worden zeer breed gedefinieerd als:

---

243 Een '*trap and trace device*' wordt gedefinieerd in 18 U.S.C. § 3127(4) als "*a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication*".

244 Zie 50 U.S.C. § 1861. Dit is bijvoorbeeld de wettelijke basis voor de MAINWAY database, zie para. 37.

245 Zie H.R. 6404, FISA Amendments Act of 2008' (zie www.gpo.gov/fdsys/pkg/BILLS-110hr6304enr/pdf/BILLS-110hr6304enr.pdf. De vaak aangehaalde 'Section 702. Procedures for targeting certain persons outside the United States other than United States persons' werd geconsolideerd in de U.S Code als 50 USC § 1881a, (www.law.cornell.edu/uscode/text/50/chapter-36). Eerder werd FISA ingrijpend geamendeerd door de Patriot Act in 2001.

246 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013. zie www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf, 4.

247 Voor een overzicht van de twee belangrijkste initiatieven, zie J. GRANICK, "A tale of two surveillance reform bills. Centre for Internet and Society", 29 October 2013, zie https://cyberlaw.stanford.edu/blog/2013/10/tale-two-surveillance-reform-bills.

248 Zie bijvoorbeeld D. POKEMPNER, "Dispatchers: Taming the NSA – Reform bills fall short. Human Rights Watch", 30 October 2013, zie www.hrw.org/news/2013/10/30/dispatches-taming-nsa-reform-bills-fall-short.

249 Zie definitie in para. 8.

250 Het moet opgemerkt worden dat *acquire* niet hetzelfde betekent als *collect*. Zie bijvoorbeeld Department of Defense, DoD 5240 1-R, Procedures governing the activities of DoD intelligence components that affect United States persons. December 1982, 15. *"Data acquired by electronic means is "collected" only when it has been processed into intelligible form"*. De titel van sectie 1881a heet voluit: *"Procedures for targeting certain persons outside the United States other than United States persons*." De betekenis van *targeting* wordt echter niet gedefinieerd in 50 USC

"(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against–
(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to–
(A) the national defense or the security of the United States; or
(B) the conduct of the foreign affairs of the United States."[251]

8. Vooral die laatste categorie staat een in principe ongelimiteerde inzameling van informatie toe. Dat is nog meer het geval aangezien de definitie van een 'buitenlandse macht' ook uitgebreid gedefinieerd wordt. De term houdt niet alleen buitenlandse regeringen, parlementsleden of internationale organisaties in, maar ook bijvoorbeeld "*een politieke organisatie in het buitenland, die niet substantieel bestaat uit Amerikaanse burgers*"[252] en "*een entiteit die gestuurd en gecontroleerd wordt door een buitenlandse overheid*".[253] Beide categorieën zouden in theorie bijvoorbeeld respectievelijk NGO's die anti-Amerikaanse betogingen organiseren of staatsbedrijven kunnen inhouden.

9. De Foreign Intelligence Surveillance Court (FISC) gaat na of de machtiging van de AG en DNI (zie para. 7) aan een aantal procedurele voorwaarden voldoet. De AG en DNI voegen een geschreven certificaat toe aan de machtiging die aantoont hoe men aan die procedurele voorwaarden voldoet. Die voorwaarden hebben voornamelijk als doel dat zo weinig mogelijk gegevens van Amerikaanse burgers intentioneel wordt verzameld.[254] Er zijn nergens in de Amerikaanse wetgeving gelijkaardige 'minimizatie procedures' voorzien die moeten voorkomen dat 'onschuldige' buitenlandse gegevens verzameld en bewaard kunnen worden. Het certificaat moet ook nergens vermelden welke specifieke faciliteiten, plaatsen of eigendommen precies het doelwit zijn van de SIGINT-verzameling.[255] De Amerikaanse overheid declassificeerde een document van 31 oktober 2011 dat de 'minimizatie procedures' beschreef die de NSA hanteerde om '*foreign intelligence* informatie' te verzamelen. Daaruit bleek dat communicaties van of over Amerikaanse

§ 1881. 50 USC § 1801 definieert *electronic surveillance* als *"the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes*". Een interpretatie zou dus kunnen zijn de gegevens van informatie pas gezien wordt als *targeting*, als het de *bedoeling* was om bepaalde informatie te verzamelen. Incidenteel verzamelde informatie wordt dan niet gezien als *targeting*.

251 50 USC § 1801(e).
252 50 USC § 1801(a)(5).
253 50 USC § 1801(a)(6).
254 50 USC § 1801(g).
255 50 USC § 1801(g)(2)(4).

burgers die niet met opzet werden verzameld tot vijf jaar bewaard mochten worden[256] en gedeeld mochten worden met buitenlandse overheden.[257]

10. Als de FISC zijn goedkeuring geeft, dan kunnen de AG en DNI op basis van een dergelijk breed certificaat, '*identifiers*' (bijvoorbeeld e-mailadressen of telefoonnummers)[258] doorgeven aan een Amerikaans bedrijf dat dan verplicht is om onmiddellijk alle "*informatie, faciliteiten of andere assistentie*" te geven om die SIGINT-verzameling te doen slagen.[259] Die bedrijven worden daarvoor financieel gecompenseerd, en kunnen in "*geen enkele rechtbank*" aansprakelijk worden gesteld voor het leveren van dergelijke informatie.[260] Een bedrijf kan in beroep gaan tegen een dergelijke vraag (bijvoorbeeld omdat de vraag te breed is)[261], waarna de FISC de vraag kan verwerpen of een finaal bevel tot medewerking kan uitspreken.[262]

I.1.3. Safe Harbour

11. Amerikaanse bedrijven kunnen dus verplicht worden om gegevens over te dragen aan de NSA, inclusief gegevens van en over Belgische klanten. Die eis naar Amerikaans recht kan botsen met de principes van het EU-US Safe Harbour akkoord uit 2000, waarbij Amerikaanse bedrijven vrijwillig de principes in dat akkoord kunnen onderschrijven. Bedrijven worden daar bijvoorbeeld geacht om aan hun klanten te kennen geven dat hun persoonlijke data aan een derde partij werd doorgegeven.[263] De Federal Trade Commission (FTC) ziet toe op de handhaving van het akkoord. Van deze principes mag afgeweken worden in naam van nationale veiligheid of omdat rechtshandhaving het vereist. De grote schaal waarop persoonlijke gegevens van Europese gebruikers van Amerikaanse bedrijven naar de NSA werden verstuurd binnen het PRISM-programma (zie para's 32-38), leidde er echter toe dat de Europese Commissie momenteel onderzoekt of het Safe Harbour akkoord niet herzien moet worden.[264]

---

256 Exhibit B, Minimization Procedures used by the National Security Agency in connection with acquisitions of foreign intelligence information pursuant to section 702 of the Foreign Intelligence Surveillance Act of 1978, as amended (www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%207 02.pdf), s.3(b)(1).

257 *Idem*, (s.8(a)).

258 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013, 4.

259 50 USC § 1802, (a)(4); 50 USC § 1881a(1) en (2).

260 50 USC § 1881a (h)(3).

261 In 2007 kreeg Yahoo een dergelijke *order* om data te geven. Yahoo vocht deze aan bij het Foreign Intelligence Surveillance Court of Review. De rechtbank verwierp echter Yahoo's tegenwerpingen. Die beslissing werd recent pas vrijgegeven. Zie https://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf.

262 50 USC § 1881a (h)(4).

263 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) Zie ook http://export.gov/safeharbor/eu/eg_main_018493.asp.

264 Commisaris Reding: "*The Safe Harbor agreement may not be so safe after all (.) It could be a loophole for data transfers because it allows data transfers from EU to U.S. companies-although*

12. Op 22 oktober 2013 stemde het Europese Parlement voor het toevoegen van een zogenaamde 'anti-FISA clausule', die bedrijven niet zou toestaan om zonder toelating van een *supervisory authority* persoonlijke data van Europese inwoners door te sturen naar een derde land op vraag van een rechtbank of een andere autoriteit in dat land. Die *supervisory authority* moet eerst nagaan of de transfer noodzakelijk is en in conformiteit met de nieuwe Europese databeschermingswetgeving. Het valt af te wachten of dit artikel de onderhandelingen met de Raad zal overleven.[265]

I.2. AARD EN SCHAAL VAN SIGINT-VERZAMELING DOOR DE NSA

13. Het is moeilijk om de totaliteit van de SIGINT-verzameling van de NSA in kaart te brengen. Enkele cijfers geven alvast een idee over de grootteorde. *The Guardian* citeert een NSA-rapport uit 2007 dat schat dat er op dat moment ongeveer 850 miljard ongedefinieerde *call events* in verschillende NSA-databases te vinden zijn, en ongeveer 150 miljard ongedefinieerde *internet records*. Volgens het document worden er elke dag één tot twee miljard *records* toegevoegd.[266] Een artikel uit *The Washington Post* stelde in 2010 dat de NSA per dag de inhoud en metadata van 1,7 miljard e-mails, telefoongesprekken en andere vormen van communicatie bewaarde, en dat een fractie daarvan in ongeveer 70 aparte databases werd bewaard.[267]

14. Die capaciteit is sindsdien exponentieel toegenomen. Slides van de NSA's interne Boundless Informant programma[268] die gepubliceerd werden door *The Guardian* tonen dat in de periode van een maand (maart 2013) de NSA's Global Access Operations divisie (GAO)[269] 97 miljard metadata van internet communicaties (e-mails, chats …) verzamelde en bijna 125 miljard metadata van telefoongesprekken die afkomstig waren uit meer dan 504 SIGINT Activity Designator (SIGADS).[270] Uit de slide blijkt dat België één van de

---

U.S. data protection standards are lower than our European ones. (…) I have informed ministers that the commission is working on a solid assessment of the Safe Harbor Agreement, which we will present before the end of the year" European Commission, Memo/13/710, 19/07/2013, http://europa.eu/rapid/press-release_MEMO-13-710_en.htm.

265 Zie artikel 43a van de "Unofficial consolidated version of the European Data Protection Regulation after the LIBE Committee vote provided by the rapporteur", 22 October 2013, beschikbaar op www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf Zie ook C., "The US surveillance programmes and their impact on EU citizens' fundamental rights", European Parliament, Directorate General for Internal Policies, 2013, 28.

266 www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

267 D. PRIEST, W. M. ARKIN, *The Washington Post* ("Secret America: A Hidden World, Growing Beyond Control"), http://projects.washingtonpost.com/top-secret-america/articles/a-hidden-world-growing-beyond-control/3/.

268 Meer informatie zie: NSA, Boundless Informant – Frequently Asked Questions (09-06-2012), zie www.theguardian.com/world/interactive/2013/jun/08/boundless-informant-nsa-full-text.

269 Dit houdt dus niet de metadata collectie in van andere NSA-divisies zoals TAO of SSO.

270 *Signals activity/address designators* – kunnen verwijzen naar een specifiek fysiek collectieplatform (zoals bijvoorbeeld een Amerikaanse legerbasis in het buitenland, een ambassade, een schip …), een virtueel dataverwerkingsplatform (PRISM staat bijvoorbeeld bekend als SIGAD US-984XN) of een ruimtesatelliet.

landen was van waaruit in absolute getallen het minst metadata werden verzameld.[271] De slide verraadt niet over hoeveel metadata het gaat, maar aan de hand van de kleurcode die België daar heeft, lijkt het dat er alvast op dat er minder metadata vanuit België wordt verzameld in vergelijking met bijvoorbeeld Nederland.

15. *Der Spiegel* publiceerde extra slides uit het programma in augustus 2013 die duidelijk maakten dat in december 2012 vanuit Nederland er ongeveer 1,8 miljoen metadata van telefoongesprekken verzameld werden.[272] In diezelfde periode werd er vanuit Frankrijk 70 miljoen metadata van telefoongesprekken verzameld[273], uit Spanje 60 miljoen en uit Italië 47 miljoen.[274]

16. Vanuit Duitsland werd er in dezelfde periode meer dan 500 miljoen metadata verzameld. Dat aantal is veel groter omdat het ook over internet-metadata gaat. Uit een document blijkt dat meer dan 471 miljoen metadata uit SIGAD US-987LA komen.[275] Volgens *Der Spiegel* gelooft de Bundesnachrichtendienst (BND) dat hiermee verwezen wordt naar de Bad Aibling site, een site die tot 2004 gerund werd door de NSA, maar daarna werd overgenomen door de BND. Vanuit die site verzamelt de BND buitenlandse SIGINT, vooral uit Afghanistan en het Midden Oosten. Die data wordt dan doorgespeeld naar de NSA.[276]

17. Volgens de NSA vervoert het internet iedere dag 1,826 petabytes aan informatie. Daarvan 'raakt' de NSA 1,6% 'aan', ongeveer 29 miljoen gigabyte per dag.[277] Van die 1,6%

---

271 www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining#.

272 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html.

273 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-6.html *Le Monde* publiceerde in oktober 2013 meer details waaruit het lijkt dat onder de codenaam DRTBOX 62,5 miljoen metadata werd verzameld van mobiele telefoongespreken en onder de codenaam WHITEBOX de metadata van 7,8 miljoen gesprekken van het openbare telefoonnet (*Public switched telephone network (PSTN)*). Doelwitten waren zowel mensen die geassocieerd werden met terroristische activiteiten alsook mensen uit de zakenwereld, de Franse politiek of de Franse zakenwereld. www.lemonde.fr/technologies/article/2013/10/21/france-in-the-nsa-s-crosshair-phone-networks-under-surveillance_3499741_651865.html Verschillende media berichtten dat er 70 miljoen Franse telefoongesprekken afgeluisterd werden. Dat is zeker een foute interpretatie van de Snowden-documenten. Zie hierover ook "DNI Statement on Inaccurate and Misleading Information in Recent Le Monde Article", 22 oktober 2013 (http://icontherecord.tumblr.com): "*The allegation that the National Security Agency collected more than 70 million "recordings of French citizens' telephone data" is false. (…) While we are not going to discuss the details of our activities, we have repeatedly made it clear that the United States gathers intelligence of the type gathered by all nations*."

274 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-5.html.

275 Www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-4.html.

276 Volgens *Der Spiegel* worden er vanuit Bad Aibling alleen al 62.000 e-mails per dag onderschept. www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of-data-to-the-nsa-a-914821.html.

277 '*Touch*' is geen term die wettelijk gedefinieerd is, maar impliceert informatie waar de NSA effectief naar kijkt (in tegenstelling tot de loutere verzameling van informatie). *The Wall Street Journal* hierover: "*One U.S. official says the agency doesn't itself "access" all the traffic within the*

wordt 0,025% geselecteerd om geëvalueerd te worden. Volgens de NSA "bekijkt het dus amper 0,00004% van alle internetverkeer per dag".[278] Een gewone berekening zou suggereren dat dat aantal 10 keer zo hoog ligt, waardoor de NSA dus 0,0004% van alle internetverkeer berekent, maar volgens de NSA is het originele cijfer correct.[279]Dat lijkt weinig, maar dat is nog een enorme hoeveelheid wetende dat bijvoorbeeld slechts 2,9% van alle webtraffiek in de VS bestaat uit communicaties.[280]

18. *The Guardian* beschreef een document van 26 december 2012 waarin de 'Special Source Operations' (SSO) divisie aankondigde dat het een nieuwe capaciteit (codenaam EVILOLIVE) zou verwerven om nog meer metadata te verzamelen van communicaties waarvan een partij niet-Amerikaans is (One-End Foreign (1EF) solution). De NSA zou nu meer dan de helft van alle metadata informatie die het verzamelt via haar SIGADS in haar eigen databases kunnen opslaan.[281] Een ander, niet vrijgegeven document spreekt over een ander metadata-verwervings-capaciteit genaamd SHELLTRUMPET, waarvan op 31 december 2012 een SSO-official zei dat dit programma net haar triljoenste metadata-record had verwerkt. De helft van die verwerkingen vond in 2012 plaats. Nog twee andere metadata-programma's (MOONLIGHTPAD en SPINNERET) werden verwacht operationeel te worden tegen september 2013.[282]

19. Een recent vrijgegeven uitspraak van de FISC uit 2011 suggereert dat 91% van de internetdata die de NSA verzamelt uit het PRISM programma komt.[283] De rest komt van zogenaamde '*upstream*' dataverwerking, en clandestiene missies uit het zogenaamde 'Specialized Reconnaissance Program' (SRP) die uitgevoerd kunnen worden samen met de CIA. *The Washington Post* gaf het budget van de 'US intelligence community' in 2013 vrij, en daaruit blijkt dat 2% van het totale budget gereserveerd werd voor twee gezamenlijke

---

surveillance system. The agency defines access as "things we actually touch," this person says, pointing out that the telecom companies do the first stage of filtering. http://online.wsj.com/article_email/SB10001424127887324108204579022874091732470-lMyQjAxMTAzMDIwMDEyNDAyWj.html.

278 N.S.A., "The National Security Agency: Missions, Authorities, Oversight and partnerships", 9 Augustus 2013, 6.

279 NSA woordvoerder V. VINES:"*Our figure is valid; the classified information that goes into the number is more complicated than what's in your calculation*". Zie www.thewire.com/politics/2013/08/nsa-better-data-collection-math/68490/.

280 In de VS bijvoorbeeld is '*real time entertainment*' (*streaming* sites zoals Netflix bijvoorbeeld) verantwoordelijk voor 62% van alle webtraffiek en *peer-to-peer file-sharing* (via sites zoals Bittorrent bijvoorbeeld) voor 10,5%. Zie J. JARVIS, *Buzzmachine*, 10 Augustus 2013 ("NSA by the numbers"), http://buzzmachine.com/2013/08/10/nsa-by-the-numbers/.

281 www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection "*This new system, SSO stated in December, enables vastly increased collection by the NSA of internet traffic. (…) The 1EF solution is allowing more than 75% of the traffic to pass through the filter," the SSO December document reads. "This milestone not only opened the aperture of the access but allowed the possibility for more traffic to be identified, selected and forwarded to NSA repositories.*"

282 www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.

283 Foreign Intelligence Surveillance Court, Foreign Intelligence Surveillance Court Memorandum Opinion and Order (J. Bates), 3 October 2011, 71. Zie www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa – deel 8.

CIA-NSA programma's. Het eerste programma heet CLANSIG ('*clandestine signals collection*'), dat een variëteit aan *black bag jobs* of *off-net* operaties dekt. Dat zijn zeer risicovolle clandestiene operaties waarbij toegang gezocht wordt tot bijvoorbeeld radiofrequenties en cruciale telecominfrastructuur van een land, maar ook de specifieke toegang tot de e-mails en computers van *high interest* doelwitten zoals buitenlandse overheden, militaire communicatiesystemen en grote multinationals. Het laatste decennium zijn er meer dan honderd van dergelijke *black bag jobs* uitgevoerd. In deze operaties wordt bijvoorbeeld *spyware* geïnstalleerd op computers of worden beveiligde telefoonlijnen, routers, glasvezelkabels, data switch centra en andere systemen 'afluisterbaar' gemaakt de CIA, waardoor de NSA toegang krijgt tot die gegevens. Dergelijke operaties hebben vooral plaatsgevonden in het Midden Oosten en Azië, vooral in China.[284] Het tweede gezamenlijke initiatief van de NSA en de CIA is de Special Collection Service (SCS), die officiële VS-gebouwen zoals ambassades en consulaten als uitvalsbasis gebruikt om in het geheim communicaties te onderscheppen, onder meer van (geëncrypteerd) diplomatiek verkeer in het land waar de ambassade of het consulaat gevestigd is.[285] SCS-personeel bezit diplomatieke status.[286] Hun operaties verlopen vaak vanuit een Secure Compartmented Intelligence Facility (SCIF) op de bovenste verdieping van een ambassade. De meeste diplomaten van een ambassade lijken niet te weten wat er in deze *staterooms* gebeurt.[287] Volgens *Der Spiegel* is de SCS actief in 80 landen, waaronder 19 Europese.[288] Tot nu toe vrijgegeven documenten en slides lijken te suggereren dat de SCS niet actief lijkt te zijn in België.[289] Het is de SCS die verdacht wordt van het afluisteren van de mobiele telefoon van Angela Merkel.[290]

I.3. 'UPSTREAM'-VERZAMELING IN DE VS

20. Via glasvezelkabels passeert meer dan 80% van het wereldwijde telefoon- en internetverkeer cruciale punten in de VS die uitgebaat worden door de drie grootste Ameri-

---

284 Bijvoorbeeld: "*In another more recent case, CIA case officers broke into a home in Western Europe and surreptitiously loaded Agency-developed spyware into the personal computer of a man suspected of being a major recruiter for individuals wishing to fight with the militant group al-Nusra Front in Syria, allowing CIA operatives to read all of his email traffic and monitor his Skype calls on his computer*": www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation.

285 US Intelligence 2013 budget http://apps.washingtonpost.com/g/page/national/inside-the-2013-us-intelligence-black-budget/420/#document/p13/a117314 Foreign Policy: "*For example, virtually every U.S. embassy in the Middle East now hosts a SCS SIGINT station that monitors, twenty-four hours a day, the complete spectrum of electronic communications traffic within a one hundred mile radius of the embassy site.* www.foreignpolicy.com/articles/2013/07/16/the_cias_new_black_bag_is_digital_nsa_cooperation?page=0,1).

286 Zie noot 99.

287 www.spiegel.de/fotostrecke/photo-gallery-spies-in-the-embassy-fotostrecke-103079-6.html.

288 www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html.

289 http://cpunks.files.wordpress.com/2013/10/20131027-191221.jpg?w=545 Oorsprong van de slide is geverifieerd door de auteur.

290 www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205-2.html.

kaanse telecom-operatoren (AT&T, Verizon en Sprint). Daar zit per definitie communicatieverkeer bij met een Belgische oorsprong of bestemming. De NSA's 'Special Source Operations' divisie controleert apparatuur die op deze punten wordt geplaatst, waardoor alle data die langs deze punten passeren, gekopieerd en gefilterd kunnen worden op basis van door de NSA ingestelde parameters.[291] De belangrijkste daarvan is een 'wettelijke' filter: alleen communicaties waarvan op zijn minst een deelnemer geen Amerikaan is, of zich niet in de VS bevindt, mogen in theorie doorgestuurd worden naar de NSA. Andere filters moeten ervoor zorgen dat alleen data met een *foreign intelligence*-waarde worden doorgestuurd naar de NSA. Programma's zoals XKEYSCORE stellen NSA-analisten in staat om deze *upstream data* te doorzoeken op basis van *strong selectors* (bijvoorbeeld een telefoonnummer, of een e-mailadres of een groep IP-adressen die toehoren aan een organisatie waarin de NSA geïnteresseerd is), *soft selectors* (zoals trefwoorden), of selectors die een bepaald type van geëncrypteerd trafiek detecteren (zoals Tor[292] of Virtual Private Network (VPN)-gebruik[293]).[294] Om deze beslissing te maken kan de NSA dus zowel naar de inhoud als naar de metadata van een communicatie kijken.[295] Informatie uit XKEYSCORE wordt dan naar tal van andere databases gestuurd. XKEYSCORE wordt in detail in paragrafen 28-31 behandeld.

21. Een gelekt document gepubliceerd door *The Washington Post* meldt dat FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), en SILVERZEPHYR (US-3273) allemaal *special source operations* zijn die data verwerven van dataverkeer dat pas-

---

291 *The Wall Street Journal*: "*There are two common methods used, according to people familiar with the system. In one, a fiber-optic line is split at a junction, and traffic is copied to a processing system that interacts with the NSA's systems, sifting through information based on NSA parameters. In another, companies program their routers to do initial filtering based on metadata from Internet "packets" and send copied data along. This data flow goes to a processing system that uses NSA parameters to narrow down the data further*". http://online.wsj.com/article/SB10001424127887324108204579025222244858490.html.
En verder: "*According to a U.S. official, lawyers at telecom companies serve as checks on what the NSA receives. "The providers are independently deciding what would be responsive," the official says. Lawyers for at least one major provider have taken the view that they will provide access only to "clearly foreign" streams of data–for example, ones involving connections to ISPs in, say, Mexico, according to the person familiar with the legal process. The complexities of Internet routing mean it isn't always easy to isolate foreign traffic, but the goal is "to prevent traffic from Kansas City to San Francisco from ending up" with the NSA, the person says",* in S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach"). Een deel van het bestaan van dit soort activiteiten werd al bekend in 2006 door AT&T klokkenluider Mark Klein (Declaration of Mark Klein in support of plaintiffs' motion for preliminary injunction. United States District Court, Northern District of California. 8 June 2006).

292 Tor is een netwerk van servers die gebruikers toelaten om anoniem te surfen. Zie hierover https://www.torproject.org/.

293 Vaak gebruikt door bedrijven om werknemers van thuis uit toegang te verschaffen – via een geëncrypteerde 'tunnel' tot het bedrijfsnetwerk.

294 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

295 Voor een technische analyse van XKeyscore zie http://arstechnica.com/information-technology/2013/08/building-a-panopticon-the-evolution-of-the-nsas-xkeyscore/.

seert door de VS, maar waarvan beide kanten niet-Amerikaans zijn.[296] Een andere gelekte slide spreekt over FAIRVIEW, STORMBREW, BLARNEY en OAKSTAR als *upstream* SIGADS.[297] Volgens *The Wall Street Journal* valt ook LITHIUM onder deze cluster.[298]

22. BLARNEY (US-984) is de SIGAD die initieel verwees naar *upstream data* die de NSA verkreeg via AT&T[299] maar lijkt later uitgebreid te zijn naar meerdere bedrijven.[300] Volgens *The Washington Post* wordt er nog altijd data uit BLARNEY verwerkt.[301] Een slide van een NSA-presentatie die te zien was in het Braziliaanse TV-programma Fantastico suggereerde dat BLARNEY zorgt voor "*collection against DNR and DNI FISA Court Order authorized communications*". DNR staat voor Dial Number Recognition, terwijl DNI staat voor Digital Network Intelligence. De slide vermeldt verder dat de hoofddoelen van BLARNEY "*diplomatic establishment, counterterrorism, counter proliferation, foreign government, economic, military en political/intention of nations*" zijn.[302] Volgens een andere slide startte BLARNEY al in 1978 om toegang te krijgen tot de communicaties van "*foreign establishments, agents of foreign powers and terrorists*".[303] *Der Spiegel* meldde eerder dat NSA-technici die voor het BLARNEY-programma werkten erin geslaagd waren om de VN's interne video teleconferentie systeem (VTC) te exploiteren.[304] Informatie uit BLARNEY werd volgens dezelfde slide verstuurd naar 'externe klanten' zoals het US Department of State, de CIA, de US UN Mission, the Joint Chiefs of Staff, Department of Homeland Security, DNI, 2nd parties to Five eyes, National Counterterorrism Center, White House, Defense Intelligence Agency, NATO, Office of Secretary of Defense en military commands (Army, EUCOM).[305] Het programma heeft veel weg van het NSA-programma dat beschreven wordt in de rechtszaak Jewel v. NSA.[306]

---

296 http://apps.washingtonpost.com/g/page/national/nsa-report-on-privacy-violations-in-the-first-quarter-of-2012/395/#document/p2/a114809.

297 www.washingtonpost.com/business/economy/the-nsa-slide-you-havent-seen/2013/07/10/32801426-e8e6-11e2-aa9f-c03a72e2d342_story.html?wprss=rss_national *The Washington Post* had eerder de namen 'STORMBREW' en 'OAKSTAR' gecensureerd.

298 http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html.

299 S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach").

300 Zie *The Washington Post*: "*BLARNEY's top-secret program summary describes it as "an ongoing collection program that leverages IC [intelligence community] and commercial partnerships to gain access and exploit foreign intelligence obtained from global networks*." www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_print.html.

301 *Idem*.

302 http://leaksource.files.wordpress.com/2013/09/blarney.jpg. *Der Spiegel* meldde eerder dat "*NSA technicians working for the Blarney program have managed to decrypt the UN's internal video teleconferencing (VTC) system*".

303 *Screengrab* van een segment dat werd getoond op http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large.

304 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

305 *Screengrab* van segment getoond op http://g1.globo.com/fantastico/noticia/2013/09/nsa-documents-show-united-states-spied-brazilian-oil-giant.html; https://pbs.twimg.com/media/BTxAU7ZIYAA3OW_.png:large.

306 Zie https://www.eff.org/files/filenode/jewel/jewel.complaint.pdf Volgens ex-NSA werknemer Thomas Drake is BLARNEY "*a key access program facilitated by these commercial arrange-*

I.4. 'UPSTREAM'-VERZAMELING BUITEN DE VS

23. Informatie uit glasvezelkabels die het grondgebied van een van de secundaire partners van de VS passeren (UK, Canada, Australië en Nieuw-Zeeland) worden ook met de VS gedeeld.[307] Volgens Duncan Campbell, deelt ook het Zweedse SIGINT-agentschap 'Försvarets radioanstalt' (FRA) upstream data die het verwerft via glasvezelkabels met Five Eyes. De data die zo verkregen zou worden zou bekend staan onder de codenaam SARDINE.[308] Campbell claimt dat ook de Deense *Forsvarets Efterretningstjeneste* (Danish Defence Intelligence Service) op deze manier informatie deelt met de NSA. De data die zo verkregen zou worden, zou bekend staan onder de codenaam DYNAMO.[309] De NSA heeft ook gelijkaardige samenwerkingsverbanden met buitenlandse telecombedrijven "*vooral in Europa en het Midden Oosten*" volgens een anonieme bron in *The Wall Street Journal*.[310] Volgens Glenn Greenwald sluit de NSA geen rechtstreekse samenwerkingsverbanden af met buitenlandse bedrijven, maar gebruikt het de toegang van een groot – tot nu toe onbekend – Amerikaans telecombedrijf dat samenwerkt met dergelijke buitenlandse bedrijven. Het Amerikaanse bedrijf in kwestie heeft direct toegang tot de telecominfrastructuur van haar partner, dat daarmee – onbewust – ook toegang geeft tot de NSA. Deze info komt dan in het FAIRVIEW programma, aldus Greenwald.[311] Andere glasvezelkabels zijn voor de VS legitieme doelwitten om clandestien internet- en telefoonverkeer te onderscheppen op basis van EO 12333.

24. Via het *upstream* programma werden e-mails van Franse telecombedrijven als Alcatel – Lucent automatisch onderschept. Het is niet duidelijk of de inhoud van alle e-mails van die adressen automatisch werd bijgehouden, enkel e-mails die bepaalde trefwoorden bevatten, en/of de metadata van dat e-mailverkeer.[312] Op basis van de functies en operaties die beide bedrijven uitvoeren, lijkt het niet onmogelijk dat gelijkaardige e-mails van werknemers van BICS, Belgacom of Tecteo op eenzelfde manier onderschept werden.[313]

---

ments that exploits the Internet data at these junctions. (…) BLARNEY is to the international Internet space as PRISM is to the domestic". www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

307 http://apps.washingtonpost.com/g/page/world/how-the-nsa-tried-to-collect-less/518/.

308 Duncan Campbell testimony: www.youtube.com/watch?v=ZX1tmizZLpc. Dit is geen verrassing in het licht van de 'FRA-wet' die Zweden in 2008 aannam, zie http://news.bbc.co.uk/2/hi/europe/7463333.stm.

309 Duncan Campbell testimony to the Council of Europe, 1 October 2013, zie www.duncancampbell.org/PDF/CoECultureCommittee1Oct2013.pdf, 19.

310 S. GORMAN en J. VALENTINO-DEVRIES, *The Wall Street Journal*, 20 Augustus 2013 ("New Details Show Broader NSA Surveillance Reach").

311 www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Eerder noemde ex-NSA werknemer Thomas DRAKE FAIRVIEW, een *umbrella programma* waaronder veel andere programma's resorteren. www.dailydot.com/news/fairview-prism-blarney-nsa-internet-spying-projects/.

312 www.lemonde.fr/technologies/article/2013/10/21/les-services-secrets-americains-tres-interesses-par-wanadoo-et-alcatel-lucent_3499762_651865.html).

313 Alcatel Lucent levert bijvoorbeeld cruciale infrastructuur voor onderwater glasvezelkabels. Zie hierover: www.alcatel-lucent.com/solutions/submarine-networks).

25. Een van de data die de SSO-divisie van de NSA collecteert via dergelijke 'upstream verzameling' zijn miljoenen contactlijsten of adresboeken van e-mail- en chatprogramma's alsook *screenshots* van een volledige e-mail-inbox. Contactlijsten van chatprogramma's kunnen soms de inhoud van een bepaald bericht bijhouden, en in de e-mail inbox van een persoon is ook vaak de eerste lijn van het bericht te zien.[314] Een PowerPoint presentatie van de NSA stelt dat op 10 januari 2012 op één dag 444.743 adresboeken van Yahoo werden verzameld, 105.068 van Hotmail, 82857 van Facebook, 33.697 van Gmail en 22.881 van andere providers. De Amerikaanse bedrijven in kwestie hebben – naar zij zeggen – ook geen weet van de collectie van dergelijke informatie.[315] Op jaarbasis zou dit neerkomen op het verzamelen van meer dan 250 miljoen adreslijsten per jaar.

26. De NSA geeft toe dat de veel van deze adresboeken geen '*foreign intelligence value*' hebben – zeker omdat men in 22% van de gevallen niet weet wie de eigenaar is van de adreslijst.[316] Maar een analyse van die data stelt de NSA in staat om 'geheime connecties' en relaties te zien van een veel kleinere groep van '*foreign intelligence*' doelwitten. Die lijsten worden dan in verschillende NSA-databases opgeslagen zoals MARINA, MAINWAY, PINWALE en CLOUDs. Volgens een *intelligence* bron van *The Washington Post* mag een NSA-analist deze databases niet doorzoeken, of informatie hieruit niet verspreiden tenzij hij/zij kan aantonen dat er zich in deze gegevens een *valid foreign intelligence* doelwit bevindt.[317]

27. Metadata die op basis van Executive Order 12333 wordt verzameld, mag sinds november 2010 gebruikt worden om aan '*contact chaining*' te doen om relaties tussen *foreign intelligence targets* en inwoners van de Five Eyes in kaart te brengen.[318] De data mag verder aangevuld worden met *enrichment data,* data uit voornamelijk publieke en commerciële bronnen zoals passagierslijsten, Facebook profielen, bank codes, kiesregistratie lijsten, GPS data van TomTom en Amerikaanse belastingdata.[319] Aangezien het hier

---

314 http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/.

315 Het hoge aantal Yahoo-adresboeken kan verklaard worden doordat Yahoo niet automatisch data encrypteert via *secure socket layer* (SSL) – in dit in tegenstelling tot de andere providers. Deels als antwoord op de onthullingen heeft Yahoo aangekondigd om vanaf januari 2014 ook 'SSL by default' aan te bieden. www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_2.html.

316 http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/).

317 Www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story_1.html.

318 www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html.

319 "*A top-secret document titled "Better Person Centric Analysis" describes how the agency looks for 94 "entity types," including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A. correlates 164 "relationship types" to build social networks and what the agency calls "community of interest" profiles, using queries like "travelsWith, hasFather, sentForumMessage, employs. (…) A 2009 PowerPoint presentation provided more examples of data sources available in the "enrichment" process, including location-based services like GPS and TomTom, online social networks, billing records and bank codes for transactions in the United States and overseas.*" In: www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

volgens de NSA louter om metadata en open bronnen gaat, is er geen toezicht van de FISC nodig om dergelijke profielen te maken.[320]

I.5. (UPSTREAM) DATA ORDENEN EN DOORZOEKEN MET XKEYSCORE

28. Een gelekte presentatie uit februari 2008 beschrijft XKEYSCORE (ook gekend als CrossKeyScore of XKS) als een *DNI exploitation system/analytic Framework*.[321] XKEYSCORE houdt gedurende drie tot vijf dagen[322] ongefilterde internet data bij ('*full take*'), en gedurende 30 dagen metadata, bij die verzameld worden van 150 SIGADS overal ter wereld.[323] Dat houdt niet alleen het verzamelen van *upstream* informatie via bijvoorbeeld onderwaterkabels in, maar ook informatie vanuit satellieten (Fornsat[324]) en vanuit diplomatieke en consulaire missies van de VS overal ter wereld (F6 sites).[325] In 2012 bevatte XKEYSCORE gedurende een periode van 30 dagen gemiddeld 41 miljard records[326] Volgens de slide laat een dergelijke *full-take* een analist onder meer toe om via metadata doelwitten te vinden die daarvoor niet gekend waren.[327] Een analist moet eerst aantonen dat hij voor 51% zeker is dat zijn zoekopdracht gaat over een buitenlands doelwit. Analisten kunnen XKEYSCORE dan doorzoeken *in real time*[328], en data doorsturen naar andere

320 *Idem*.

321 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

322 Soms kan dit soort data maar één dag bijgehouden worden: "*One document explains: "At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours."* In: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

323 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 6. Volgens NSA-expert Marc AMBINDER, die al voor de Snowden documenten over XKeyscore schreef, is Xkeyscore "*not a thing that DOES collecting; it's a series of user interfaces, backend databases, servers and software that selects certain types of metadata that the NSA has ALREADY collected using other methods*." In: http://theweek.com/article/index/247684/whats-xkeyscore.

324 Volgens Duncan CAMPBELL, de man die het bestaan van GCHQ onthulde in 1976, is dit de opvolger van Echelon. Het programma bestaat nog steeds, maar boette aan belang in aangezien veel telefoondata zich nu ook verplaatsen via glasvezelkabels. Voor Duncan CAMPBELL getuigenis in het Europese Parlement, zie www.youtube.com/watch?v=ZX1tmizZLpc.

325 Xkeyscore presentatie, gelekt op www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 5. Volgens AMBINDER verwijst 'F6' technisch gezien naar het hoofdkwartier van de Special Collection Service (SCS) in Beltsville, Maryland, die informatie verzamelt uit minstens 75 F6-sites die zich vooral bevinden in landen waar het onmogelijk is om informatie naar de NSA te sturen via gewone telefoonkabels of glasvezelkabels omdat de V.S. technisch gezien niet verondersteld wordt om daar aanwezig te zijn. De NSA erkent het bestaan van de SCS niet omdat de meeste personeelsleden als State Department officials werken. Zie http://theweek.com/article/index/247684/whats-xkeyscore en http://theweek.com/article/index/247761/5-nsa-terms-you-must-know.

326 ???

327 Xkeyscore presentatie, gelekt op www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 2.

328 *Idem*. Voor meer details over dit proces (inclusief andere originele slides) zie www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

databases zoals PINWALE, MARINA of TRAFFICTHIEF.[329] Daar wordt die ruwe informatie gedurende een langere periode opgeslagen.

29. De voorbeelden die in de slides aangehaald worden, tonen aan dat een analist via XKEYSCORE zeer veel data kan analyseren. XKEYSCORE kan de inhoud van elke http-activiteit lezen: dus elke e-mail en elke attachment en chatconversatie[330], alle metadata van een internetcommunicatie, alle surfgeschiedenis en alle *online* zoekopdrachten die een persoon uitvoert.[331] Verder kan het ook het gebruik van een bepaalde encryptie- of VPN-technologie detecteren[332] of nagaan welke taal iemand *online* gebruikt.[333] XKEYSCORE kan ook de IP-adressen nagaan van elke persoon die een door de analist gespecificeerde website bezoekt.[334] Met XKEYSCORE kan ook nagegaan worden wie de auteur is van een document dat *online* verstuurd werd.[335] Aan de hand van 'kwetsbaarheidprofielen' die geleverd worden door de NSA's Tailored Access Operations (TAO), kan XKEYSCORE ook gebruikt worden om 'exploiteerbare machines' in een bepaald land te vinden.[336] De inhoud van opgeslagen e-mails en Facebook-chats of privéberichten kan ook binnen XKEYSCORE gelezen worden door een analist die het programma DNI PRESENTER gebruikt.[337]

30. De slides, die uit 2008 dateren, laten zien dat XKEYSCORE op dat moment nog geen Voice over Internet Protocol (VoIP)[338] kon onderscheppen, maar het verwachtte in de toekomst ook meer metadata te onderscheppen zoals *exif tags*.[339]

---

329 *Idem*.

330 Xkeyscore kan dingen opzoeken zoals "*toon me elke Excel-spreadsheet uit Irak waarin Media Access Control Addresses te vinden zijn*" (23) of, "*toon me elk word-document dat de IAEA of Osama Bin Laden vermeldt*" (26), www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation,.

331 Xkeyscore houdt alle zoekopdrachten bij, of het gebruik van bijv. Google Maps. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 20.

332 Met XKeyscore is het bijvoorbeeld mogelijk om "*alle geëncrypteerde word-documenten uit Iran, of elk PGP-gebruik in Iran*" te tonen. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (16). Een analyst kan ook aan Xkeyscore vragen om het gebruik van bepaalde technologieën te detecteren, bijv. door te vragen: "*toon me alle VPN start-ups in land X, en geef me de data zodat ik de gebruikers van die service kan identificeren*". Zie: www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (17).

333 Xkeyscore kan ook gebruikt worden om aan *language tracking* te doen, via Xkeyscore's 'http activity plugin' die html language tags bijhoudt. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation (19).

334 *Idem*. Bijvoorbeeld: elke Belg die extremistische website X bezoekt.

335 www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 21.

336 Voor een technische analyse zie http://arstechnica.com/tech-policy/2013/08/nsas-internet-taps-can-find-systems-to-hack-track-vpns-and-word-docs/.

337 www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

338 Verwijst naar services zoals Skype en Apple's Facetime.

339 Xkeyscore presentatie, gelekt op www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation, 32. Een *exchangeable image file format* (exif) is een technische standaard die metadata van digitale camera's bijhoudt, zoals bijvoorbeeld de datum en tijd wanneer een digitale foto werd genomen.

31. De NSA erkende het bestaan van XKEYSCORE als een onderdeel van de NSA's *lawful foreign signals intelligence collection system*, maar benadrukte dat toegang tot XKEYSCORE gelimiteerd is en dat elke zoekopdracht door een analist *fully auditable* is. De NSA benadrukt dat meer dan 300 terroristen werden gevat op basis van intelligence die uit XKEYSCORE komt.[340]

I.6. PRISM: DOWNSTREAM VERZAMELING VAN SIGINT

32. Deels omdat steeds meer buitenlanders de diensten van Amerikaanse bedrijven begonnen te gebruiken, en deels omdat die bedrijven hun communicaties begonnen te encrypteren via SSL[341], besloot de NSA om met de belangrijkste van deze bedrijven een samenwerkingsverband te sluiten om gebruikersdata op een efficiënte en gestroomlijnde manier door te sturen naar de NSA.[342] Het resultaat van deze onderhandelingen was het PRISM-programma. Via PRISM kreeg de NSA – in vergelijking met de *upstream* collectie – op een gestructureerde manier *downstream* data van negen grote technologiebedrijven binnen: Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL en Apple.[343]

33. Alle PRISM-providers hebben een code gekregen. P1: Microsoft[344], P2: Yahoo, P3: Google[345], P4: Facebook, P5: PalTalk, P6: YouTube, P7: Skype[346], P8: AOL, PA: Apple.[347]

---

340 www.nsa.gov/public_info/press_room/2013/30_July_2013.shtml.

341 Een encryptieprotocol om communicatie op het internet te beveiligen.

342 C.C. MILLER, *The New York Times*, 7 june 2013 ("Tech companies concede to surveillance programme").

343 De meest volledige slideshow van PRISM werd in oktober gepubliceerd door *Le Monde*. www.lemonde.fr/technologies/article/2013/10/21/espionnage-de-la-nsa-tous-les-documents-publies-par-le-monde_3499986_651865.html.

344 *The Guardian* beschreef verder SSO documenten die aantoonden dat Microsoft en de FBI ervoor zorgden dat de NSA makkelijk de encryptie van outlook.com chats kon omzeilen. Een ander document toont aan dat de NSA toegang heeft tot e-mails van Hotmail, Windows Live en Outlook.com vooraleer die geëncrypteerd worden. www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

345 De NSA heeft hiermee toegang tot Gmail, Google voice and video chat, Google Drive files, Google's fotodienst Picasa Web, en (real time) surveillance van zoektermen die door een persoon worden ingetypt in Google. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html.

346 "*According to a separate "User's Guide for PRISM Skype Collection," that service can be monitored for audio when one end of the call is a conventional telephone and for any combination of "audio, video, chat, and file transfers" when Skype users connect by computer alone*". Zie: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html
Een ander document stelde dat "*Prism monitoring of Skype video production has roughly tripled since a new capability was added on 14 July 2012. (…) The audio portions of these sessions have been processed correctly all along, but without the accompanying video. Now, analysts will have the complete 'picture' it says*." www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

347 De providers startten hun deelname in PRISM op verschillende tijdstippen. Microsoft: 11/09/2007, Yahoo: 12/3/2008, Google: 14/01/2009, Facebook: 3/6/2009, PalTalk: 7/12/2009,

34. Er zijn negen grote types aan content die via PRISM worden verzameld, die ook weer een codeletter hebben gekregen. A= opgeslagen communicaties (zoals privéberichten op een sociale netwerksites, chat-geschiedenis, e-mails etc.), B: Instant Messaging (chat), C: RTN-EDC (notificatie in *real time* van een login op een account of een verstuurd bericht), D: RTN-IM (notificatie in *real time* voor een chat login of logout), E: E-mail, F: VoIP (services zoals Skype, inclusief videoconferencing), G: Full (Webforum), H: OSN (Online Social Networking information – foto's, *wallposts*, activiteiten op sociale media sites …) I: OSN informatie die geleverd wordt wanneer men zich inschrijft voor een OSN-dienst. J: video's.[348]

35. Het systeem lijkt als volgt te werken: een NSA-analist kan zelf de *selectors* (e-mailadres, telefoonnummer, naam, maar ook zoektermen) invoeren in een *Unified Targeting Tool*.[349] Die *selectors* worden bekeken door een overste, die nagaat of er 51% kans is dat het om een buitenlands doelwit gaat.[350] Als de NSA opgeslagen data (bijv. e-mails in een inbox) wil consulteren, dan moet de FBI een extra check doen om te zien of er geen Amerikanen bespioneerd worden. Als de NSA in '*real-time*' surveillance wil doen, dan is die extra check niet nodig. In beide gevallen gebruikt de FBI's Data Intercept Technology Unit (DITU) materiaal (*government equipment*) om informatie over die doelwitten te verkrijgen van een van de bedrijven die meedoen aan PRISM. De FBI stuurt dat materiaal dan door naar de CIA of de NSA.[351]

36. Als er informatie over een doelwit wordt verzameld, dan betekent dat ook dat informatie kan verzameld worden over iedereen waarmee het doelwit tot in de tweede graad mee gecommuniceerd heeft. Een eenvoudig hypothetisch voorbeeld toont aan dat informatie inwinnen over een doelwit in de praktijk betekent dat data van een enorm aantal mensen potentieel kan verzameld worden. Als een doelwit gecommuniceerd heeft met 700

Youtube: 24/9/2010, Skype: 6/2/2011, AOL: 31/3/2011, Apple: oktober 2012. PRISM startte dus maar na de aanname van de Protect America Act in 2007. www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1# In April 2013 heette het dat de toevoeging van Dropbox nakende was. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html.

348 www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#.

349 "*In another classified report obtained by The Post, the arrangement is described as allowing "collection managers [to send] content tasking instructions directly to equipment installed at company-controlled locations," rather than directly to company servers.*" Zie: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

350 Merk op dat de FISC alleen de certificaten jaarlijks onderzoekt (zie para. 9), niet de individuele zoektermen.

351 "*The information the NSA collects from Prism is routinely shared with both the FBI and CIA. A 3 August 2012 newsletter describes how the NSA has recently expanded sharing with the other two agencies. The NSA, the entry reveals, has even automated the sharing of aspects of Prism, using software that "enables our partners to see which selectors [search terms] the National Security Agency has tasked to Prism". The document continues: "The FBI and CIA then can request a copy of Prism collection of any selector …*". Zie: www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

mensen via Facebook of e-mail, en die mensen hebben op hun beurt ook elk gecommuniceerd met 700 mensen, dan kan de NSA gegevens verzamelen over 490.000 mensen.[352]

37. De NSA sorteert op haar beurt de verkregen data op basis van datatype, en haalt de ze nog eens door een filter om na te gaan of geen Amerikaanse gegevens worden bekeken. DNI content[353] en video worden doorgestuurd naar de PINWALE database.[354] Metadata van '*internet records*' worden verstuurd naar MARINA[355] en metadata van telefoongesprekken naar MAINWAY.[356] Een intern NSA bulletin gaf aan dat MAINWAY in 2011 per dag metadata binnen kreeg van 700 miljoen telefoongesprekken. Vanaf augustus 2011 kwamen daar nog eens 1,1 miljard metadata van telefoongesprekken extra bij per dag.[357]

38. Op 5 april 2013 waren er 117.675 actieve surveillance doelwitten in PRISM's *counterterrorism database*.[358] Volgens de vrijgegeven slides is PRISM de SIGAD waaruit de meeste ruwe informatie komt voor alle NSA-rapporten.[359] In 2012 verscheen PRISM-data

---

352 www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#
The Washington Post merkt verder op: "*it is true that the PRISM program is not a dragnet, exactly. From inside a company's data stream the NSA is capable of pulling out anything it likes, but under current rules the agency does not try to collect it all*." www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html
Verder: "*To collect on a suspected spy or foreign terrorist means, at minimum, that everyone in the suspect's inbox or outbox is swept in. Intelligence analysts are typically taught to chain through contacts two "hops" out from their target, which increases "incidental collection" exponentially*." Zie: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_3.html.

353 Zoals forum posts, chats, e-mails … of simpel gezegd: "internet content".

354 Pinwale houdt de inhoud van communicaties bij voor een periode van vijf jaar. Die informatie lijkt te komen op basis van op voorhand ingestelde *dictionary tasked terms* die het onder andere krijgt uit Xkeyscore en PRISM. www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu.

355 Marina wordt in een Xkeyscore slide beschreven als "*user activity meta-data with front end full take feeds and back-end selected feeds*". Hierover: www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data?CMP=twt_gu *The Guardian* quote uit een document waarin Marina verder wordt beschreven. "*The Marina metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target," the analysts' guide explains. "This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development." (…) "Of the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of DNI metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection*." In: www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents.

356 www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/?hpid=z1#.

357 www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all.

358 Ter vergelijking: de Terrorist Identities Datamart Environment (TIDE) van de Amerikaanse overheid telde in december 2011 740.000 'records', waarbij eenzelfde persoon een aantal keer kan voorkomen wegens een foute spelling van zijn/haar naam. www.dni.gov/files/Tide_Fact_Sheet.pdf.

359 Dat wordt ook bevestigt door de FISC, zie para.19. "*According to the slides and other supporting materials obtained by The Post, "NSA reporting increasingly relies on PRISM" as its leading*

in 1.477 items van de Amerikaanse President's Daily Intelligence Brief.[360] DNI-director Clapper bevestigde het bestaan van PRISM (zonder het programma bij naam te noemen), en noemde het "*een van de belangrijkste bronnen*" van de NSA.[361]

I.7. FINANCIËLE DATA

39. Volgens documenten die *Der Spiegel* kon inzien, heeft de NSA een '*Follow the money*'-tak die internationale geldstromen – vooral in Afrika en het Midden Oosten – in de gaten houdt. Die informatie komt terecht in een database, genaamd TRACFIN, die in 2011 al 180 miljoen datasets had over banktransfers, kredietkaarttransacties en geldtransfers. Volgens *Der Spiegel* houdt de NSA dit soort data gedurende vijf jaar bij.[362]

40. Nog steeds volgens *Der Spiegel* heeft de NSA een grondige kennis van de interne processen van maatschappijen zoals Visa en Mastercard (zoals '*payment authorisation processes*' en interne geëncrypteerde communicaties[363]), en houdt het ook alternatieve betaalmethodes zoals Bitcoin in het oog. Volgens *Der Spiegel* verzamelt de NSA via het DISHFIRE-programma informatie over transacties die met kredietkaarten worden uitgevoerd van meer dan 70 banken wereldwijd – vooral in 'crisisgebieden', inclusief in landen als Italië, Spanje en Griekenland. DISHFIRE is actief sinds de lente van 2009. De transacties van Visa-klanten in Europa, het Midden Oosten en Afrika werden ook geanalyseerd om financiële associaties bloot te kunnen leggen.[364] Door deze kennis werden verschillende Arabische banken op de *blacklist* van de US Treasury geplaatst.[365]

---

source of raw material, accounting for nearly 1 in 7 intelligence reports." In: www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

360 www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_1.html.

361 www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa.

362 www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html.

363 "*According to the presentation, the NSA was previously only able to decrypt payment transactions by bank customers, but now they have access to the internal encrypted communication of the company's branch offices. This "provides a new stream of financial data and potentially encrypted internal communications" from the financial service provider, the analysts concluded with satisfaction. This bank data comes from countries that are of "high interest." It's interesting to note that the targeted company is also one of the many SWIFT service partners.*" In: www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html.

364 "*Furthermore, the author concluded, thanks to network analyses and the use of the XKeyscore spying program, NSA analysts had stumbled across the encrypted traffic of a large financial network operator in the Middle East.*" In: www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430-2.html.

365 *"In one case, the NSA provided proof that a bank was involved in illegal arms trading -- in another case, a financial institution was providing support to an authoritarian African regime".* In: www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html.

41. Andere documenten tonen aan dat de NSA's Tailored Access Operations (TAO) divisie sinds 2006 clandestien toegang heeft verworven tot de interne data trafiek van de Society for Worldwide Interbank Financial Telecommunication (SWIFT).[366] Dat is opmerkelijk, aangezien de VS een akkoord heeft met de EU om SWIFT-data te delen – maar dat akkoord laat niet het versturen van *bulk data* toe.[367] Na deze onthullingen stemde het Europese Parlement op 23 oktober 2013 in met de opschorting van het Terrorist Finance Tracking Program (TFTP Agreement).[368] In een statement liet Commissaris Malmström weten dat het TFTP-akkoord niet zal opgeschort worden.[369]

I.8. METADATA VAN AMERIKAANSE TELEFOONGESPREKKEN

42. In Amerika spitst het NSA-debat zich vooral toe op het verzamelen van Amerikaanse telefoondata door de NSA, onder meer op basis van de *business records* sectie 215 die door de Patriot Act geïntroduceerd werd in FISA.[370] Op basis van deze sectie kon de VS de grootste Amerikaanse telecom-operatoren verplichten om alle metadata van telefoongesprekken met een Amerikaans begin- of eindpunt ter beschikking te stellen van de NSA. Volgens de NSA kunnen deze data enkel geconsulteerd worden voor anti-terreurdoeleinden. Een consultatie kan enkele beginnen met een telefoonnummer dat eerder geassocieerd werd met een buitenlandse terroristische organisatie (*a seed*).[371]

I.9. SMARTPHONE DATA

43. Volgens *Der Spiegel* heeft de NSA de capaciteit om een grote waaier aan smartphonedata te verkrijgen van *high interest targets*.[372] De NSA had toegang tot de contactlijsten, call logs, sms-trafiek, drafts van sms'en en locatie-informatie van de mobiele platformen van Apple (IOS), Google (Android) en Blackberry.[373] De NSA heeft bijvoorbeeld toegang

---

366 www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html "*Since then, it has been possible to read the "SWIFT printer traffic from numerous banks.*"

367 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:195:0005:0014:EN:PDF.

368 European Parliament resolution of 23 October 2013 on the suspension of the TFTP agreement as a result of US National Security Agency surveillance (2013/2831(RSP)), zie: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2013-0449+0+DOC+XML+V0//EN.

369 European Commission, Memo, 23 October, zie: http://europa.eu/rapid/press-release_MEMO-13-928_en.htm.

370 Zie para 6.

371 N.S.A., The National Security Agency: Missions, Authorities, Oversight and partnerships, 9 Augustus 2013, 5.

372 Zie ook para. 19.

373 "*The presentation notes that the acquisition of encrypted BES (Blackberry Services) communications requires a "sustained" operation by the NSA's Tailored Access Operation department in order to "fully prosecute your target. (.) The alleged telecommunications surveillance has been a targeted activity that was performed without the smartphone makers' knowledge.*" In: M. ROSENBACH, L. POITRAS en H. STARK, *Der Spiegel*, 9 September 2013 ("iSpy: How the NSA Accesses Smartphone Data").

tot 38 iPhone applicaties zoals het gebruik van de ingebouwde kaartfunctie, voicemail en foto's, Google Earth, Yahoo en Facebook Messenger.[374]

I.10. PNR-DATA

44. Via het Passenger Name Records (PNR) akkoord uit 2012 verkrijgt het US Department of Homeland Security (DHS) PNR-data van passagiers die van de EU naar de VS vliegen. Die data bestaat uit informatie die een passagier gegeven heeft aan de luchtvaartmaatschappij zoals de naam van de passagier en zijn eventuele medepassagiers, hun adressen en telefoonnummers, reisdata, eindbestemming, ticket informatie, de manier van betalen, credit card nummer, bagage informatie enz. De volledige lijst kan teruggevonden worden in de annex bij het akkoord.[375] DHS mag die data delen met binnenlandse diensten[376] en derde landen.[377] De data worden gebruikt ter preventie, opsporing en berechting van terroristische misdrijven en ernstige grensoverschrijdende misdaden.[378] Na zes maanden worden alle persoonlijke data gemaskeerd, en na vijf jaar worden de data in een 'slapende' database gestoken. De data mogen gedurende tien jaar gebruikt worden ter preventie van grensoverschrijdende misdaad, en vijftien jaar voor terrorisme.[379]

I.11. NSA-INSPANNINGEN TEGEN ENCRYPTIE

45. *The New York Times* publiceerde een *briefing sheet* van de NSA aan het GCHQ uit 2010 over een programma genaamd BULLRUN, waarin de NSA suggereert dat de meest gebruikte encryptie-protocollen die verantwoordelijk zijn voor de beveiliging van de wereldwijde handel, banksystemen, medische data en internet surfgedrag (zoals het zenden van e-mails, online opzoekingen, chats en online telefoongesprekken) door de NSA gekraakt of omzeild konden worden. Het gaat over TLS/SSL[380], https[381], SSH[382], VPNs[383] en geëncrypteerde chats[384] en VOIP communicaties.[385] De specifieke technische details

374 *Idem*.
375 http://register.consilium.europa.eu/pdf/en/11/st17/st17434.en11.pdf, 36.
376 *Idem*, artikel 16.
377 *Idem*, artikel 17.
378 *Idem*, artikel 4.
379 *Idem*, artikel 8.
380 Transport Layer Security/Secure sockets layer. De meest gebruikte manier om informatie te verzenden over het internet en interne servers. HTTPS is beveiligd door TLS/SSL toe te passen op een website.
381 Hypertext transfer protocol secure. Manier om financiële informatie en paswoorden veilig te versturen van een computer naar een netwerk. Sites zoals Facebook, Twitter en Gmail gebruiken vaak https 'by default'. Herkenbaar aan het slotje voor de https in de web-browser.
382 Secure Shell. De manier voor Linux en Max gebruikers om toegang te krijgen tot een computer vanop afstand.
383 Virtual Private Network. Vaak gebruikt door bedrijven om werknemers van thuis uit toegang te verschaffen – via een gencrypteerde 'tunnel' tot het bedrijfsnetwerk.
384 Een voorbeeld is het Adium programma, waarmee 'end to end' encryptie mogelijk is, waarbij de data niet kan gedecrypteerd worden op enig punt gedurende de transfer.
385 Verwijst naar services zoals Skype en Apple's Facetime.

over wat er precies werd gekraakt werden tot nu toe niet vrijgegeven.[386, 387] Het bestaan van deze decryptiemogelijkheden én het gebruik van alle geëxploiteerde data (zowel *plaintext* als metadata) die uit deze mogelijkheden voortkwamen, werden geclassificeerd als Exceptionally Controlled Information (ECI), een *level* hoger dan 'Top Secret'.[388]

46. Een budgetaanvraag uit 2012 onthulde verder het bestaan van het Sigint Enabling Project dat erop gericht is om in het geheim Amerikaanse en buitenlandse internetbedrijven te beïnvloeden het design van hun producten aan te passen zodat deze kunnen geëxploiteerd worden. Het programma omvat een hele reeks activiteiten: (1) Samenwerking met bedrijven om 'achterpoortjes' te installeren in commerciële encryptie systemen, IT-systemen, netwerken en *endpoint communication devices* die gebruikt worden door 'doelwitten'.[389] Die samenwerking kan vrijwillig zijn[390], of afgedwongen worden door FISA-dwangbevelen.[391] (2) Het beïnvloeden van technische standaarden en specificaties voor commerciële *public key technologies*, inclusief de standaard uit 2006 van het National Institute of Standards and Technology.[392] (3) Het voortzetten van de samenwerking met grote *telecommunications carriers*.[393] De meest controversiële manier is echter het clandestien stelen van encryptie-sleutels. NSA-documenten tonen aan dat de NSA een interne database heeft (de Key Provisioning Service), die de encryptiesleutels bevat van specifieke commerciële producten. Als een bepaalde sleutel niet aanwezig is, dan gaat een aanvraag naar de Key Recovery Service, waarvan beweerd wordt dat die sleutels verkrijgt door in te breken in de servers van de bedrijven die de sleutel gemaakt hebben. Om deze methode geheim te houden, zou de NSA alleen gedecrypteerde boodschappen met andere diensten delen als de sleutels verkregen werden door legale middelen.[394]

---

386 www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us Experts hebben opgemerkt dat de documenten niet tonen welke geëncrypteerde systemen de NSA gekraakt heeft door pure wiskunde, en welke door hacking of samenwerking van ontwikkelaars. Een systeem als Pretty Good Privacy (PGP) zou nog altijd werken. Voor meer info zie (de links) hierin: www.washingtonmonthly.com/political-animal-a/2013_09/the_nsa_is_mostly_not_breaking046760.php of www.newyorker.com/online/blogs/elements/2013/09/the-nsa-versus-encryption.html.

387 www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

388 www.theguardian.com/world/interactive/2013/sep/05/nsa-classification-guide-cryptanalysis.

389 www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

390 "*In one case, after the government learned that a foreign intelligence target had ordered new computer hardware, the American manufacturer agreed to insert a back door into the product before it was shipped, someone familiar with the request told The Times*." In: www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

391 www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

392 *Idem*.

393 www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html?ref=us.

394 www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?pagewanted=3&_r=1&hp&&pagewanted=all.

47. Op 4 oktober 2013 onthulden *The Guardian* en *The Washington Post* hoe de NSA sinds 2006 probeerde om gebruikers van het Tor-netwerk te identificeren en te bespioneren.[395] Tor is een netwerk van servers die gebruikers toelaten om anoniem te surfen.[396] Gebruikers kunnen dat netwerk via speciale, complexe software gebruiken, maar een alternatieve, gemakkelijkere manier om Tor te gebruiken is het downloaden van de Tor Browser Bundle (TBB) – een versie van Firefox die automatisch data verzendt over het Tor-netwerk. Uit de documenten blijkt dat de NSA in 2007 TBB-gebruikers kon onderscheiden van gewone Firefox gebruikers[397], maar dat het er in 2007 nog niet in geslaagd was om het Tor-netwerk zelf te hacken. Een NSA-presentatie uit juni 2012 stelt dat de NSA nooit in staat zal zijn om alle Tor-gebruikers tegelijkertijd te de-anonimiseren, en dat de NSA ook geen technieken heeft die toestaan om een specifieke gebruiker op verzoek te de-anonimiseren. Door manuele analyse is het echter mogelijk om een 'zeer kleine fractie' van Tor gebruikers te de-anonimiseren.[398] Slides van de NSA's Tailored Access Operations (TAO) beschrijven hoe de NSA Javascript-kwetsbaarheden in Firefox exploiteerde via de programma's EGOTISTICALGOAT en EGOTISTICALGIRAFFE.[399] Deze kwetsbaarheden zouden verdwenen zijn met de meest recente *update* van Firefox in januari 2013[400], maar het is onduidelijk of de NSA dit intussen al omzeild heeft.[401]

48. Onder de codenaam Quantum plaatste de NSA geheime Quantum-servers op belangrijke plaatsen van de infrastructuur van het internet, waardoor de NSA een *man in the middle* aanval kon uitvoeren op Tor-gebruikers.[402] Dit betekent dat deze servers sneller kunnen reageren dan andere websites, waardoor ze de gebruiker naar een geïnfecteerde imitatie van de gevraagde website kunnen sturen die op een FoxAcid-server staat. De servers in dit FoxAcid-systeem worden gerund door TAO, en kunnen op verschillende manieren computers voor lange periodes besmetten.[403] Het bezoek van de homepage van

---

395 *The Washington Post* plaatste een document uit 2006 van 49 pagina's online dat beschrijft welke methodes potentieel de grootschalige de-anonymisatie van Tor gebruikers zouden toelaten. In: http://apps.washingtonpost.com/g/page/world/nsa-research-report-on-the-tor-encryption-program/501/. James Clapper statement op de onthullingen: http://icontherecord.tumblr.com/post/63103784923/dni-statement-why-the-intelligence-community.

396 www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.

397 http://apps.washingtonpost.com/g/page/world/nsa-slideshow-on-the-tor-problem/499/#document/p5/a124608.

398 www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document?utm_source=hootsuite&utm_campaign=hootsuite.

399 www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.

400 www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

401 "*In anticipation of a new release of Firefox, one agency official wrote in January that a new exploit was under development: "I'm confident we can have it ready when they release something new, or very soon after:)."*
In: www.washingtonpost.com/world/national-security/secret-nsa-documents-show-campaign-against-tor-encrypted-network/2013/10/04/610f08b6-2d05-11e3-8ade-a1f23cda135e_story_2.html.

402 B. SCHNEIER: "*More specifically, they are examples of "man-on-the-side" attacks*". www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

403 *"After identifying an individual Tor user on the internet, the NSA uses its network of secret internet servers to redirect those users to another set of secret internet servers, with the codename FoxAcid, to infect the user's computer. FoxAcid is an NSA system designed to act as a matchma-*

een FoxAcid-server zou niet direct tot besmetting leiden; daarvoor is een door TAO gecreëerde specifieke URL voor nodig. Die URL zou de FoxAcid server in staat stellen om precies te weten welk doelwit de FoxAcid server bezoekt.[404] FoxAcid is een algemeen CNE-systeem dat gebruikt wordt voor verschillende digitale aanvalsvormen. Het wordt dus voor veel meer gebruikt dan om Tor-gebruikers te identificeren. Documenten uit *Der Spiegel* suggereren bijvoorbeeld dat de Belgacom-aanval (deels) via Quantumservers zou uitgevoerd zijn.[405]

II. HET BRITSE GOVERNMENT COMMUNICATIONS HEADQUARTERS (GQHQ)

II.1. HET BRITSE WETTELIJKE KADER VOOR HET INZAMELEN VAN INFORMATIE OVER BUITENLANDSE

Doelwitten

49. De Intelligence Services Act uit 1994 zette voor het eerst de functies uit van het Government Communications Headquarters (GCHQ). Het Britse SIGINT-agentschap heeft onder meer als mandaat om "*elektromagnetische, akoestische en andere emissies, alsook ieder toestel dat zulke emissies produceert*" te monitoren of te storen.[406] Het agentschap moet informatie over die emissies doorsturen naar het Britse leger, de regering en andere diensten[407] als dat nodig is voor de nationale veiligheid van de UK (waarbij specifiek verwezen wordt naar de defensie- en buitenlandse politiek van de UK), het economische welzijn van de UK (met betrekking tot de handelingen en intenties van personen buiten de Britse eilanden) en ter ondersteuning van de preventie en het opsporen van ernstige misdaden.[408]

50. De UK heeft geen specifieke wetgeving die exclusief het gebruik van *foreign intelligence* reguleert, maar de Regulation of Investigatory Powers Act (RIPA) maakt een onderscheid tussen 'interne' en 'externe' surveillance, waarbij die laatste categorie refereert naar surveillance van communicaties waarvan op zijn minst een uiteinde buiten de UK ligt.[409] In deze gevallen moet GCHQ geen bevelschrift aanvragen op naam van een specifieke

---

ker between potential targets and attacks developed by the NSA, giving the agency opportunity to launch prepared attacks against their systems. Once the computer is successfully attacked, it secretly calls back to a FoxAcid server, which then performs additional attacks on the target computer to ensure that it remains compromised long-term, and continues to provide eavesdropping information back to the NSA". In: www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity.

404 *Idem.*

405 *Idem.*

406 Intelligence Services Act 1994, Chapter 13, s3, (1)(a).

407 Intelligence Services Act 1994, Chapter 13, s3, (1)(b).

408 Intelligence Services Act 1994, Chapter 13, s3, (2).

409 RIPA, s20.

persoon of een specifieke locatie[410], maar kan het een bevelschrift vragen om bijvoorbeeld data van een externe communicatielink te onderscheppen, zoals bijvoorbeeld een specifieke glasvezelkabel die tussen de UK en het Europese vasteland loopt.[411] Ter illustratie, alle glasvezelkabels die aan land komen in België zijn verbonden met een landingspunt in de UK. De Tangerine-kabel verbindt Broadstairs met Oostende; Concerto verbindt Zeebrugge met Sizewell en Thorpeness en de Pan-European Crossing verbindt Bredene met Dumpton Gap. De grote SeaMeWe-3 kabel, waarvan Belgacom deels eigenaar is, verbindt Oostende met Goonhilly Downs in de UK, maar heeft ook landingspunten in Saudi Arabië, Maleisië en China.

51. Een dergelijk breed bevelschrift wordt dan uitgevaardigd door de Secretary of State, die in een 'certificaat' beschrijft welk materiaal precies noodzakelijk is om onderzocht te worden[412] in het belang van de UK's nationale veiligheid, om ernstige misdaden te voorkomen of op te sporen of om het economische welzijn van de UK veilig te stellen.[413] De inhoud van de certificaten is geheim, maar volgens documenten die *The Guardian* heeft ingezien, zijn deze heel breed geformuleerd, en laten deze toe om materiaal te onderscheppen over wijde thema's zoals de politieke intenties van buitenlandse overheden, de militaire toestand van andere landen, terrorisme, internationale drugshandel en fraude. Volgens *The Guardian* zijn er minstens tien van die certificaten.[414] Volgens RIPA is zo'n bevelschrift initieel drie maanden geldig[415], maar het bevelschrift kan elke zes maand hernieuwd worden.[416] Telecombedrijven kunnen verplicht worden om mee te werken met de interceptie van deze communicaties.[417]

---

410 RIPA, s.8.4. Interceptie wordt als volgt gedefinieerd in s.2.2: "*A person intercepts a communication in the course of its transmission by means of a telecommunication system if, and only if, he- (a) so modifies or interferes with the system, or its operation, (b) so monitors transmissions made by means of the system, or (c) monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system, as to make some or all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication.*"

411 "*Lawyers at GCHQ speak of having 10 basic certificates, including a "global" one that covers the agency's support station at Bude in Cornwall, Menwith Hill in North Yorkshire, and Cyprus. Other certificates have been used for "special source accesses" – a reference, perhaps, to the cables carrying web traffic. All certificates have to be renewed by the foreign secretary every six months.*" In: www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

412 RIPA, s8.4(b).

413 RIPA s.5(3)a-c. *The Guardian* quote een GCHQ document als volgt: "*The certificate is issued with the warrant and signed by the secretary of state and sets out [the] class of work we can do under it … cannot list numbers or individuals as this would be an infinite list which we couldn't manage.*" In: www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world.

414 *The Guardian* quote een interne GCHQ memo uit oktober 2011: *"[Our] targets boil down to diplomatic/military/commercial targets/terrorists/organised criminals and e-crime/cyber actors*". In: www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

415 RIPA, s9.6.c.

416 RIPA s9.6.b. Voor meer informatie over s(8)4 warrants, zie: UK Home Office, Interception of Communications Code of Practice. TSO, London, 22-27, op https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/97956/interception-comms-code-practice.pdf.

417 RIPA, s.12.

52. Het moet opgemerkt worden dat het niet duidelijk is wat er precies in het bevelschrift en het certificaat moet staan. Onder meer hierover is de wet onduidelijk. Het Intelligence Security Committee (ISC), dat toezicht houdt over GCHQ, heeft aangekondigd dat "*meer gedetailleerde beleidslijnen en procedures in het leven zijn geroepen zodat GCHQ de Human Rigts Act van 1998 naleeft*". De ISC gaat nu onderzoek doen naar de 'complexe interactie tussen de ISA, de Human Rights Act en RIPA en de procedures die dit regelen.[418]

53. De wet staat GCHQ ook toe om vanop afstand in te breken in computersystemen om op die manier data te verkrijgen.[419] Op basis van sectie 7 ISA is iedere actie van GCHQ buiten de UK vrijgesteld van burgerlijke of strafrechtelijke aansprakelijkheid indien deze gebeurt op basis van een machtiging van de Secretary of State.

II.2. AARD EN SCHAAL VAN DE BRITSE GEGEVENS-INZAMELING

54. Volgens *The Guardian* startte GCHQ begin 2007 met de voorbereidingen voor het Mastering the Internet (MTI) project in de basis in Bude.[420] Het doel was om buitenlandse *upstream* data te verzamelen door *deep packet inspection* materiaal te plaatsen op de onderwaterkabels wanneer die de Britse kust raakte.[421] In mei 2009 berichtten *The Register* en *The Sunday Times* dat de financiering van MTI was goedgekeurd in oktober 2007. Meer dan één miljard pond zou de komende drie jaar uitgetrokken worden om die *upstream* collectie mogelijk te maken.[422] GCHQ erkende het bestaan van MTI, maar benadrukte dat het geen technologie aan ontwikkelen was die het mogelijk zou maken om al het Internet- en telefoongebruik *in de UK* te monitoren.[423]

55. Op een onbekend moment tussen 2010 en 2011 slaagde GCHQ in haar opzet, en begon het de uitbaters van de commerciële glasvezelkabels via een bevelschrift te verplichten om mee te werken als *intercept partners*. Dit afgedwongen samenwerkingsproces wordt '*special source exploitation*' genoemd, en de '*intercept partners*' worden vergoed

---

418 Intelligence and Security Committee of Parliament, Statement on GCHQ's alleged interception of communications under the US PRISM Programme. 17 juli 2013, zie: http://isc.independent.gov.uk/news-archive/17july2013.

419 Zie Computer Misuse Act 1990, s.10; RIPA, s32 en ISA, s.5.

420 Naast MTI is er ook een programma dat Global Telecoms Exploitation heet, maar het is niet duidelijk wat daarmee bedoeld wordt. Zie: www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

421 www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet. Een eerste experimenteel project om dat te bereiken stond bekend als het Cheltenham Processing Centre (CPC). Vanaf maart 2010 werd naar dit project als een gezamenlijk GCHQ/NSA-initiatief verwezen genaamd TINT.

422 Volgens die berichten zouden Lockheed Martin en Detica meehelpen om MTI te ontwikkelen. Sinds 2008 werden inderdaad jobadvertenties aangeboden die te maken hadden met het MTI-contract www.theregister.co.uk/2009/05/03/gchq_mti/; www.timesonline.co.uk/tol/news/politics/article6211101.ece.

423 (Eigen nadruk) www.telegraph.co.uk/technology/news/5271796/Government-not-planning-to-monitor-all-web-use.html.

voor de kosten die dit meebrengt.[424] De namen van de samenwerkende bedrijven werden later bekend gemaakt door de *Suddeütsche Zeitung*. Ze stonden alle zeven bekend onder een andere codenaam: BT (Remedy), Verizon Business (Dacron), Vodafone Cable (Gerontic), Global Crossing (Pinnage), Level 3 (Little), Viatel (Vitreous) en Interoute (Streetcar).[425] De glasvezelkabel die aankomen in België (zie para. 50) worden allen uitgebaat door een van deze bedrijven.

56. Die *upstream* informatie wordt via het TEMPORA-programma eerst gefilterd om internet trafiek dat veel volume inneemt (zoals downloads van films of muziek) uit te sluiten, waardoor het volume met ongeveer 30% daalt.[426] De overblijvende *upstream*-informatie wordt gefilterd op basis van 'harde selectors' (zoals telefoonnummers en e-mailadressen) en 'zachte selectors' (zoals zoektermen). Volgens *The Guardian* werden 40.000 van deze selectors gekozen door GCHQ en 31.000 door de NSA.[427] Die baseren zich op de brede certificaten om die *selectors* zelf te kiezen. De ongefilterde data wordt weggesmeten, en de metadata die overblijft wordt bijgehouden gedurende dertig dagen en inhoud gedurende drie dagen.[428] Een bron van *The Guardian* lijkt te suggereren dat alle 'gefilterde' data gelogd worden en ingezien kan worden door de UK's Interception Commissioner, maar het is onduidelijk of dit gaat over alle informatie die wordt opgeslagen na de *selector*-filtering, of alleen die data die effectief gebruikt wordt.[429] Deze data kan dan – onder andere – retroactief onderzocht worden op zoek naar verdachten die nog niet bekend waren bij de Britse of Amerikaanse inlichtingendiensten.[430]

57. Voor het overige kan alle *upstream*-informatie verzameld worden die ook door de NSA verzameld wordt via haar *upstream*collectie (zie para 29): inhoud van e-mails, browsergeschiedenis, Facebook-berichten, documenten die als attachment werden toegevoegd etc. Hier moet opgemerkt worden dat analisten ook kunnen beslissen om alle metadata en inhoud van de contacten van een doelwit te verzamelen als zij dat proportioneel achten.[431] Minstens 300 GCHQ-analisten en 250 NSA-analisten hebben directe toegang tot de data van TEMPORA.[432] Veel metadata wordt ook opgeslagen door de NSA.[433] In februari 2011 meldde de NSA in een document dat GCHQ nu "*meer metadata verwerkte*" dan de NSA.[434] In 2012 kon GCHQ 600 miljoen 'telefoon events' per dag verwerken, tapte het 200 glasvezelkabels af en was het in staat om van 46 van die kabels tegelijkertijd data te verwerken. *The Guardian* schatte dat GCHQ daarmee in theorie toegang heeft tot 21,6 petabytes per

424 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
425 www.theguardian.com/business/2013/aug/02/telecoms-bt-vodafone-cables-gchq.
426 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
427 *Idem*.
428 www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work Het is interessant dat GCHQ in bepaalde gevallen zelfs paswoorden als metadata beschouwd.
429 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
430 www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.
431 "*If analysts believe it is proportional, they can look at all the traffic – content and metadata – relating to all of the target's contact*." In: www.theguardian.com/uk/2013/jun/23/mi5-feared-gchq-went-too-far.
432 www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.
433 www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.
434 www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet.

dag – 192 keer de inhoud van alle boeken de zich in de British Library of Congress bevinden.[435]

II.3. DE MALWARE BIJ BELGACOM

58. Op 21 juni 2013 vindt Belgacom *malware* op haar intern computersysteem. Nadat hulp van onder meer toeleveranciers Microsoft en HP geen soelaas brachten, wordt op 25 juni de Nederlandse firma Fox-IT ingehuurd om naar de malware te kijken.[436] Na verder onderzoek van Fox-IT dient Belgacom vervolgens op 19 juli 2013 een klacht in tegen onbekenden bij het federale parket wegens frauduleuze toegang tot zijn interne computersystemen. Dat onderzoek wordt geleid door de gerechtelijke politie van Brussel (Regional Computer Crime Unit) met de (technische) steun van de Federal Computer Crime Unit (FCCU) en Algemene Dienst inlichting en veiligheid (ADIV).[437] De voorzitter van de Privacycommissie besluit in september om in samenwerking met Belgacom en het Belgisch Instituut voor Postdiensten en Telecommunicatie (BIPT), een apart onderzoek in te stellen naar wat er precies is gebeurd. Belgacom communiceert in een persbericht op 16 september 2013 dat in het weekend van 14 en 15 september "*een onbekend virus*" verwijderd werd. Volgens Belgacoms is er "*tot dusver geen enkele aanwijzing van impact op de klanten of hun gegevens*".[438] De kostprijs van de schoonmaakoperatie wordt tot dan op vijf miljoen euro geschat.[439]

59. Volgens een persbericht van het parket wijst de aanval, gezien "*de inzet van belangrijke financiële en logistieke middelen door de inbreker*" en "*de technische complexiteit ervan*" in de richting van "*state-sponsored cyberspionage gericht op het verzamelen van strategische informatie*".[440] Later bevestigt Belgacom dat 124 van de 26.600 apparaten[441]

---

435 www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa?CMP=twt_fd *The Guardian* meldt verder: "*The system seems to operate by allowing GCHQ to survey internet traffic flowing through different cables at regular intervals, and then automatically detecting which are most interesting, and harvesting the information from those. The documents suggest GCHQ was able to survey about 1,500 of the 1,600 or so high-capacity cables in and out of the UK at any one time, and aspired to harvest information from 400 or so at once – a quarter of all traffic. As of last year, the agency had gone halfway, attaching probes to 200 fibre-optic cables, each with a capacity of 10 gigabits per second. In theory, that gave GCHQ access to a flow of 21.6 petabytes in a day, equivalent to 192 times the British Library's entire book collection*". In: www.theguardian.com/uk/2013/jun/21/how-does-gchq-internet-surveillance-work.

436 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Zie: www.youtube.com/watch?v=ayR6CAuNE4w.

437 M. EECKHAUT en P. DE LOBEL, *De Standaard*, 17 September 2013 ("Natuurlijk zat de NSA hier achter").

438 Belgacom, Belgacom onderneemt actie in het kader van haar IT-beveiliging. 16 september 2013. Zie www.belgacom.com/be-nl/newsdetail/ND_20130916_Belgacom.page.

439 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 2013 ("Op het randje van de catastrofe").

440 M. EECKHAUT en P. DE LOBEL, *De Standaard*, 17 September 2013 ("Natuurlijk zat de NSA hier achter").

441 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Zie: www.youtube.com/watch?v=ayR6CAuNE4w.

die aangesloten zijn op het interne Windows-systeem van Belgacom werden gecompromitteerd[442] door wat experts een *advanced persistent threat* noemen.[443] De omschrijving van de symptomen van de *malware*, valt onder het geheim van het gerechtelijk onderzoek, maar de FCCU heeft de *malware* in de mate van het mogelijke vrijgeven zodat andere (Belgische en Europese) instellingen na kunnen gaan of ze zijn besmet. Informatie is onder meer gedeeld met het permanente Computer Emergency Response Team (CERT-EU) van de EU.

60. *De Standaard* meldt op basis van "*bronnen dicht bij het dossier"* en "*in kringen van de veiligheidsdiensten*" dat de NSA achter de aanval zit, en dat de NSA het in het bijzonder gemunt had op de activiteiten van Belgacom International Carrier Services (BICS), een dochteronderneming van Belgacom.[444] Belgacom heeft 57,6% van BICS in handen, Swisscom 22,4% en het Zuid-Afrikaanse MTN 20%. BICS levert diensten aan verschillende telecomoperatoren in verschillende landen, en baat onder meer – samen met een groep andere bedrijven – de TAT-14, SEA-ME-WE3 en SEA-ME-WE4 onderwater-glasvezelkabels uit (zie ook para. 50). Op die manier zou bijv. telefoon- en internetverkeer vanuit Syrië, Yemen en Afghanistan onderschept kunnen worden. Dat was een van de redenen achter de aanval die door *De Standaard* werd aangehaald in haar eerste berichtgeving.[445] In een mededeling zegt BICS op 16 september 2013 dat er geen enkele aanwijzing is "*dat ons telecomnetwerk, langs waar ons communicatieverkeer loopt, door spionageoperaties werd getroffen. Het is ons intern informaticasysteem dat geïntegreerd is met dat van Belgacom dat gehackt werd"*.[446]

61. Op 20 september 2013 publiceerde *Der Spiegel* ongedateerde slides uit de Snowden-documenten waarin GCHQ's 'Network Analyses Centre' vertelt over de successen die behaald werden in 'Operation Socialist'. Belgacom stond in de operatie bekend onder de naam Merion Zeta. In deze operatie lijkt het erop dat werknemers die sleutelposities bezetten bij BICS via door de NSA-gecontroleerde Quantum-servers naar een andere NSA-gecontroleerde server werden geleid (Fox Acid server), waarbij die laatste op hun beurt een kwetsbaarheid in de browser van het doelwit gebruikte om *malware* op de computer van het slachtoffer te installeren. (zie ook para 48). Het ultieme doel van 'Operation Socialist' was volgens de slides van *Der Spiegel* om Belgacom's core GRX router te exploiteren om van daar *man in the middle* aanvallen te kunnen uitvoeren op doelwitten die met hun smartphone aan het *roamen* zijn.[447] Volgens de slides was GCHQ erg dicht bij dit

442 X., *De Standaard*, 16 september 2013 ("Bellens: 'Geen aanwijzing dat Belgacomklanten zijn getroffen'").

443 DOD, *De Standaard*, 17 september 2013 ("Zeg nooit 'virus' tegen advanced persistent attack"). www.standaard.be/cnt/dmf20130916_00745157. Voor meer informatie, zie bijvoorbeeld https://www.damballa.com/knowledge/advanced-persistent-threats.php.

444 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 september 2013 ("NSA verdacht van hacken Belgacom").

445 M. EECKHAUT en P. DE LOBEL, *De Standaard*, 17 September 2013 ("Natuurlijk zat de NSA hier achter").

446 G. QUOISTIAUX, *Trends*, 16 september 2013 ("BICS, succesvolle dochter van Belgacom en doelwit NSA").

447 www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663.html. Voor een meer technische achtergrond; zie https://www.troopers.de/wp-content/uploads/2011/10/TR12_TelcoSecDay_Langlois_Attacking_GRX.pdf.

doel.[448] BICS heeft wereldfaam in het aanbieden van 3GRX-diensten, die een lokale telefoonoperator onder meer moet toelaten aan haar klanten om te *roamen* in meer dan 190 landen.[449] De VPN-verbindingen van BICS en MyBICS, de online toepassing waarlangs het contact met klanten verloopt, werden ook als interessante doelwitten gezien.

62. Na de onthullingen in *Der Spiegel* citeerde *De Standaard* bronnen dicht bij het gerechtelijk onderzoek die op basis van "*de handtekening van de malware*" en "*vooral de plaats waar de sporen heen leiden*" nog steeds overtuigd zijn dat de aanval uit de VS komt. Volgens de speurders is Amerika de belangrijkste bestemming, en leiden er slechts "*in zeer beperkte mate*" sporen naar het Verenigd Koninkrijk.[450] Op vraag van Premier Di Rupo heeft de Belgische Veiligheid van de Staat nu officieel haar Britse tegenhanger om uitleg gevraagd.[451]

63. Op basis van 'verschillende bronnen' meldt de Nederlandse zender NOS op 3 oktober dat eind 2011 "*een team van GCHQ (…) het hart van Belgacom aan heeft gevallen*" via *named pipes*, een geavanceerde manier om vrijwel onzichtbaar communicatie te versturen over een netwerk. Volgens de NOS "*bevestigen loggegevens dat het om Engeland gaat: tijdens Engelse feestdagen en lunchtijd is er duidelijk minder spionageactiviteit*".[452] De NOS beweert dat "*nadat het netwerk gekraakt werd*", de Britten "*bijna onbeperkte toegang hadden tot het Belgacom netwerk*".[453] Eerder vertelde een andere bron aan *De Standaard* dat degene die dit deed, alles kon "*wat de hoogst geplaatste netwerkbeheerder bij Belgacom kon* (…) *Het had alle sleutels, alle paswoorden en de volledige controle*".[454] De NOS beweert ook dat "*een ander team*" vervolgens op zoek ging naar "*specifieke informatie*". De informatie werd vervolgens gedeeld met de NSA.[455] Volgens "*bronnen bij het onderzoek*" hebben de verantwoordelijken "*een beetje overal zitten rondkijken en gepakt wat ze konden*".[456] Volgens *De Standaard* levert BICS diensten waar tal van belangrijke klanten gebruik van maken: Swift, Electrabel, bpost, Belgocontrol, de Navo in Evere, de Europese Commissie en het Europese Parlement in Brussel en Straatsburg, het Supreme Headquarters Allied Powers Europe (SHAPE) in Bergen, maar ook bijvoorbeeld het hoofdkwartier van de Allied Air Command van de Navo in Ramstein.[457] Tijdens een hoorzitting in het Europees Parlement ontkenden twee topmannen van Belgacom dat de Britse geheime dienst toegang zou hebben gehad tot telefoonnetwerken van Europese instellingen. Volgens Bel-

448 www.spiegel.de/fotostrecke/photo-gallery-operation-socialist-fotostrecke-101663-3.html.
449 www.bics.com/sites/default/files/mosaic/3GRX_web.pdf.
450 N. VANHECKE, *De Standaard*, 21 september 2013 ("Operatie socialist: succes!").
451 K. VAN DE PERRE, *De Morgen*, 4 oktober 2013 ("België vraag uitleg aan Britten over Belgacom-hacking").
452 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html.
453 NOS Journaal, 3 oktober 2013, 20u CET. Zie http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html.
454 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 2013 ("Op het randje van de catastrofe").
455 NOS Journaal, 3 oktober 2013, 20u CET, zie http://nos.nl/uitzendingen/12720-nos-journaal-3-oktober-2013-2000u.html.
456 P. DE LOBEL en N. VANHECKE, *De Standaard*, 21 September 2013 ("Op het randje van de catastrofe").
457 *Idem*.

gacom is er via hun systeem "*geen overflow geweest naar systemen van klanten. Dus ook niet naar systemen van de Europese instanties*".[458]

64. Het is echter op dit moment onmogelijk om met zekerheid te zeggen welke data er precies onderschept werden. Zowel Belgacom[459], de FCCU[460], als Frank Robben[461], co-rapporteur van het Belgacom-rapport van de Privacycommissie, hebben verklaard dat het virus zelf encryptietechnieken gebruikte om te verhullen welke gegevens er precies gecompromitteerd werden. Volgens de NOS is het "*niet meer te achterhalen wie er precies is afgeluisterd en welke informatie er precies is verkregen. Om daar achter te komen, was meer tijd nodig geweest. Maar dat kon niet, omdat Belgacom het netwerk zo snel mogelijk weer operationeel wilde hebben*".[462] Het is ook onduidelijk hoe lang het virus al aanwezig was. Op een persconferentie van 16 september 2013 zegt het hoofd van Belgacom dat "*hij geen enkel idee heeft"* van wanneer het virus zich op Belgacoms netwerk bevindt. Volgens *Der Spiegel* blijkt uit een (tot nu toe ongepubliceerd) document dat toegang mogelijk was sinds 2010.[463] Volgens *De Standaard* en de *NOS* was het virus al aanwezig sinds 2011.[464]

65. Op 18 oktober 2013 meldt Belgacom dat doorgedreven controles nieuwe onregelmatigheden aan het licht brachten op een router bij BICS. "*Het eerste onderzoek wijst erop dat er wijzigingen zijn aangebracht in de software van de router, wat gebeurd kan zijn tijdens de recente digitale inbraak*".[465] Belgacom sloot niet meer uit dat gegevens van klanten zijn gehackt. "*Het lopende onderzoek zal moeten uitwijzen of er impact is geweest op de gegevens van klanten"*, aldus Belgacom in *Le Soir.*[466] Op 23 oktober bericht Belga dat ook Tecteo het slachtoffer is geworden van een cyberaanval die gelijkaardig lijkt te zijn aan die op telecomoperatoren Belgacom, France-Telecom en Wanadoo. Dat zegt het bedrijf. Het is momenteel nog te vroeg om te zeggen of er informatie is gehackt bij de groep of bij de filialen VOO of RESA.[467]

II.4. BRITSE INSPANNINGEN TEGEN ENCRYPTIE

66. De Britse tegenhanger van het BULLRUN-programma (zie para 45) werd EDGEHILL genoemd. Documenten die *The Guardian* kon inkijken suggereren dat de UK nog niet zo ver staat als de VS en slechts op een *case-by-case* basis informatie kon decrypteren.

---

458 http://nos.nl/artikel/558285-spionage-belgacom-omvangrijker.html.

459 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013. Zie www.youtube.com/watch?v=ayR6CAuNE4w.

460 N. VANHECKE, *De Standaard*, 20 september 2013 ("Info over malware Belgacom verspreid").

461 Belgacom GCHQ Affair – EP/LIBE hearing on surveillance 3 October 2013, verkrijgbaar op www.youtube.com/watch?v=ayR6CAuNE4w.

462 http://nos.nl/artikel/558286-hoe-belgacom-werd-gekraakt.html.

463 www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html.

464 M. EECKHAUT, P. DE LOBEL, N. VANHECKE, *De Standaard*, 16 september 2013 ("NSA verdacht van hacken Belgacom").

465 www.belgacom.com/be-nl/newsdetail/ND_20131017_Belgacom.page.

466 X., Belga, 19 oktober 2013 ("Belgacom sluit hacking gegevens klanten niet meer uit").

467 X., *Belga*, 23 oktober 2013 ("Ook Tecteo slachtoffer van spionage").

Het oorspronkelijke doel van EDGEHILL was om de geëncrypteerde internettrafiek van drie grote internetbedrijven te ontcijferen en 30 VPN-types. Tegen 2015 hoopte GCHQ de geëncrypteerde internettraffiek van 15 grote internetbedrijven ontcijferd te hebben, en 300 VPN-types.[468] Een ander programma, genaamd CHEESY NAME, was erop gericht om bepaalde encryptiesleutels (bekend als *certificates*) te kraken met behulp van GCHQ 'supercomputers'.[469] GCHQ richtte ook een *Humint Operations Team* (HOT) op dat verantwoordelijk is voor het identificeren, rekruteren en runnen van informanten (*covert agents*) in the globale telecom industrie, onder andere om zo toegang te krijgen tot bepaalde sleutels.[470]

67. Documenten die in een programma van Fantastico werden getoond, suggereren dat GCHQ's *network exploitation unit* programma's gebruikten (FLYING PIG en HUSH PUPPY) die TLS/SSL netwerken konden monitoren. De programma's lijken te zijn opgestart omdat steeds meer e-mailproviders zoals Yahoo, Google of Hotmail, SSL-encryptie gebruikten waardoor die berichten niet meer leesbaar waren via de directe *upstream* collectie. Minstens één document toont dat zowel de NSA als GCHQ hun toevlucht zochten tot *man in the middle attacks* om de encryptie te omzeilen.[471] FLYING PIG lijkt ook informatie te kunnen tonen over het gebruik van Tor (Tor Events).[472]

68. Een document van 10 oktober 2012 beschrijft hoe GCHQ in operatie MULLENIZE erin geslaagd is via *user agent staining* individuele gebruikers te herkennen op een IP-adres dat simultaan gebruikt wordt door veel gebruikers. Dat is bijvoorbeeld het geval in een internet café, maar ook in bepaalde regio's gebruiken duizenden gebruikers ook één IP-adres. De techniek staat ook toe om individuele Tor-gebruikers te herkennen. In een periode van twee maanden slaagde GCHQ er in om op deze manier ongeveer 200 computers te besmetten met unieke *stains*.[473]

---

468 "*GCHQ's phrasing of beating "30" then "300" VPNs suggest it's done on a case-by-case basis, rather than a blanket capability. It's also worth noting that just because the NSA can, say, beat SSL in some (or many, or most) cases, it doesn't mean they can do it all the time, especially as they often seem to circumvent rather than directly beat security.*" In: www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-revelations-encryption-expert-chat. *The Guardian* meldt ook het volgende: "*Analysts on the Edgehill project were working on ways into the networks of major webmail providers as part of the decryption project. A quarterly update from 2012 notes the project's team "continue to work on understanding" the big four communication providers, named in the document as Hotmail, Google, Yahoo and Facebook, adding "work has predominantly been focused this quarter on Google due to new access opportunities being developed*". www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

469 *Idem*.

470 *Idem*.

471 "*The document illustrates with a diagram how one of the agencies appears to have hacked into a target's Internet router and covertly redirected targeted Google traffic using a fake security certificate so it could intercept the information in unencrypted format".* www.slate.com/blogs/future_tense/2013/09/09/shifting_shadow_stormbrew_flying_pig_new_snowden_documents_show_nsa_deemed.html.

472 *Idem*.

473 Http://apps.washingtonpost.com/g/page/world/gchq-report-on-mullenize-program-to-stain-anonymous-electronic-traffic/502/.

III. OPSOMMING VAN DE IN OPEN BRONNEN VERSCHENEN CASUSSEN VAN SPIONAGEACTIVITEITEN TEN AANZIEN VAN POLITIEKE ACTIVITEITEN VAN ZOGENAAMDE 'BEVRIENDE LANDEN'

III.1. (VERMEENDE) SPIONAGEACTIVITEITEN LOS VAN DE SNOWDEN-CASE

69. In deze lijst wordt gefocust op het bespioneren van bevriende landen door de VS of de UK Het bespioneren van Europese landen die deel uitmaakten van het Warschau Pact tijdens de Koude Oorlog worden niet meegeteld. De historische voorbeelden zijn illustratief.

70. De Britse historicus Richard Aldrich heeft beschreven hoe de voorloper van GCHQ sinds 1940 de diplomatieke communicaties afluisterde van haar geallieerde partners, onder andere de Vrije Fransen onder leiding van De Gaulle, Turkije, Spanje en een twintigtal andere landen.[474] Op *adhoc* basis werd diplomatieke informatie uit Italië, Frankrijk, Spanje, Portugal, Japan en West-Duitsland met de VS gedeeld.[475]

71. Op 21 februari 1967 onthulde de Britse krant de *Daily Express* hoe bedrijven zoals Western Union en Cable & Wireless alle internationale telegrammen en telexen, inclusief materiaal van buitenlandse ambassades, naar de Britse overheid bracht, waarop deze gekopieerd werden. Volgens Aldrich ging deze traditie terug tot WO I – en had het VK dus voor een periode van meer dan vijftig jaar toegang tot alle diplomatieke verkeer van alle ambassades vanop haar grondgebied.[476]

72. Volgens Aldrich onderschepte de Nederlandse dienst diplomatieke communicaties van België en Duitsland in de jaren 1980.[477]

73. In 2006 kwam het 'top secret' jaarrapport van 1985-1986 boven water van het Government Communications Security Bureau (GCSB), Nieuw Zeeland's sigint agentschap. Het rapport vermeldde de landen en agentschappen die Nieuw Zeeland dat jaar bespioneerd had, inclusief diplomatieke communicaties van de VN, Egypte, Japan, de Filippijnen, verschillende eilanden in de Stille Oceaan, Frankrijk, Vietnam, de Sovjet Unie, Noord Korea, Oost Duitsland, Laos en Zuid Afrika.[478] De Franse geheime dienst had in 1985 de 'Rainbow Warrior' van Greenpeace doen zinken, en de GCSB schakelde dat jaar de hulp in van de NSA en GCHQ om bronnen in Frankrijk te bespioneren.[479]

---

474 R. ALDRICH, *GCHQ. The uncensored story of Britain's most secret intelligence agency*, Harper Press, London, 2010, 28; 52-53.
475 R. ALDRICH, *o.c.*, 44.
476 R. ALDRICH, *o.c.*, 238-240.
477 R. ALDRICH, *o.c.*, 604.
478 H. BAIN, *Sunday Star*, 15 januari 2006 ("Lange's secret papers reveal USA's bully tactics").
479 R. ALDRICH, *o.c.*, 446.

74. Alastair Campbell, Director of Communications and Strategy voor Tony Blair tussen 1997 en 2003 beschreef in zijn memoires hoe Britse veiligheidsagenten twee 'bugs' ontdekten in de hotelkamer die bedoeld was voor Tony Blair tijdens zijn bezoek aan New Delhi in oktober 2001.De bugs werden toegeschreven aan de Indische geheime dienst.[480]

75. In 1999 verschenen er verschillende rapporten in de Amerikaanse pers die stelden dat zowel de NSA als GCHQ de UNSCOM-missie met wapeninspecteurs van de VN hadden geïnfiltreerd om gevoelige sigint-operaties te ondernemen in Irak. Niet alle informatie die op deze manier gevonden werd, werd gedeeld met UNSCOM.[481] Volgens VN-hoofdinspecteur Hans Blix, was dergelijke informatie uiterst valabel voor een potentiële latere inval.[482]

76. In 2003 publiceerde *The Observer* een volledige memo van de NSA aan GCHQ waarin het die laatste om hulp vroeg om de toenmalige niet-permanente leden van de VN-Veiligheidsraad (Angola, Kameroen, Chili, Bulgarije en Guinea) af te luisteren om inzicht te krijgen in de houding van die landen tegenover een potentiële resolutie van de Veiligheidsraad om een militaire interventie tegen Irak goed te keuren.[483]

77. Rond hetzelfde tijdstip, in februari 2003, werd er in het Justus Lipsius gebouw van de Europese Raad afluisterapparatuur gevonden in die delen van het gebouw die gebruikt werden door de Britse, Franse, Duitse en Spaanse delegaties. Onderzoek suggereerde dat de apparatuur al in het gebouw was geplaatst sinds haar constructie in 1993. Hoewel nooit onomstotelijk bewezen, wezen een aantal indicatoren in de richting van Israël als de verantwoordelijke voor de spionage.[484]

78. In 2004 verklaarde voormalig Brits minister Clare Short op BBC Radio 4's Today programma dat ze regelmatig sigint had gehoord waarop conversaties van VN Secretaris Generaal Kofi Annan in zijn privé-kantoor in het VN-hoofdkwartier in New York te horen waren net voor de oorlog in Irak begon in 2003.[485]

79. In 2004 werd er afluisterapparatuur gevonden in het 'Salon Francais' in het Palais des Nations van de VN in Geneve. Het salon was een van de kamers die in september 2003 gebruikt werden om private onderhandelingen te voeren over de kwestie Irak. Er werd nooit een verantwoordelijke gevonden.[486]

---

480 A. CAMPBELL, *The Blair Years: The Alastair Campbell diaries,* Knopf Doubleday Publishing Group, 2011, 577.

481 C. LYNCH, *Boston Globe*, 6 januari 1999 ("US used UN to spy on Iraq, aides say"); B. GELLMAN, *The Washington Post*, 6 January 1999 ("Annan suspicious of UNSCOM probe").

482 H. BLIX, *Disarming Iraq: The search for weapons of mass destruction,* Bloomsbury, 2005, 36-37.

483 De memo stelde verder: "*We have a lot of special UN-related diplomatic coverage (various UN delegations) from countries not sitting on the UNSC right now that could contribute related perspectives/insights/whatever.*" X., *The Observer*, 2 maart 2003 ("US plan to bug Security Council: the text"). Zie ook www.theguardian.com/world/2003/mar/02/iraq.unitednations1.

484 Zie onder meer VAST COMITÉ I, *Activiteitenverslag 2010,* Intersentia, Antwerpen, 2010, 6-14.

485 C. SHORT, *An honourable deception? New Labour, Iraq and the misuse of power,* Free Press, 2005, 242-243.

486 B. WHITAKER, *The Guardian*, 18 december 2004 ("Bugging device found at UN offices").

80. In december 2004 werd er gesuggereerd dat de NSA tientallen telefoongesprekken van Mohamed ElBaradei, het hoofd van het Internationale Atoomagentschap (IAEA), met Iraanse diplomaten had afgeluisterd. De *Washington Post* suggereerde dat er naar materiaal werd gezocht om ElBaradei af te zetten als hoofd van het IAEA.[487]

III.2. ONTHULLINGEN UIT DE SNOWDEN-DOCUMENTEN

81. Volgens *Der Spiegel* wordt er vanuit 80 Amerikaanse ambassades en consulaten clandestien sigint onderschept door de Special Collection Service.[488] Dit team is ook verantwoordelijk voor top-secret surveillance-operaties in andere ambassades en consulaten die bij de NSA gekend zijn onder de naam STATEROOM.[489]

82. *Der Spiegel* beschreef in wat voor soort informatie de NSA geïnteresseerd is inzake de EU. EU informatie die gerelateerd is aan de economische stabiliteit en handelspolitiek kreeg een '3' op een prioriteitenschaal van 1 (hoogste interesse) tot 5 (laagste interesse). Informatie die gerelateerd was aan energy security, voedselproducten en technologische innovatie kreeg een 5.[490] Der Spiegel gaf details vrij over hoe de NSA de 'ambassador's room' bespioneerde op de 31ste verdieping van de EU's delegatie aan de VN in New York, die bij de NSA gekend is onder de codenaam 'Apalachee'. De NSA had toegang tot de bouwplannen van het gebouw, en infiltreerde het interne VPN-netwerk tussen de EU-missie aan de VN in New York en Washington. Die laatste stond gekend onder de codenaam MAGOTHY. Zowel de EU-missies in Washington en New York werden afgeluisterd. In de EU-missie in New York werden ook harde schijven gekopieerd, en in Washington werd het interne computernetwerk geïnfiltreerd.[491]

83. De NSA is bij de VN vooral geïnteresseerd in alles wat te maken heeft met wapencontrole in de IAEA (prioriteit 1), buitenlandse politiek (prioriteit 2) en mensenrechten, oorlogsmisdaden, milieuzaken en ruwe materialen (allen prioriteit 3). De NSA heeft een eigen team in de VN die onder cover van diplomaat werken. Ze worden versterkt door een team uit Washington voor iedere sessie van de Algemene Vergadering. De NSA luisterde ook mee naar de videoconferenties van VN-diplomaten.[492]

---

487 D. LINZER, *The Washington Post*, 12 december 2004 ("IAEA Leader's phone tapped"). El Baradei had de Amerikaanse intelligence inzake Irak ernstig betwijfeld, en nam in die periode ook een zeer voorzichtige houding aan ten opzichte van Iran.

488 Zie paragraaf 19.

489 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625.html.

490 "*Of particular note, the data systems of the EU embassies in America are maintained by technicians in Brussels; Washington and New York are connected to the larger EU network. Whether the NSA has been able to penetrate as far as Brussels remains unclear. What is certain, though, is that they had a great deal of inside knowledge from Brussels.*" www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

491 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

492 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

84. Der Spiegel onthulde ook het ontstaan van het RAMPART-T programma waaronder de NSA sinds 1991 de communicaties van staatshoofden en hun directe omgeving uit meer dan twintig landen onderschept om de President en zijn national security adviseurs beter te kunnen informeren. Der Spiegel meldde dat niet alleen doelwitten in China en Rusland geviseerd werden, maar ook in Oost-Europese staten.[493]

85. The Guardian meldde dat de 38 ambassades en missies als doelwitten beschouwd werden in een NSA-document van september 2010. Daar zijn geen West-Europese gebouwen bij, maar wel de eerder genoemde EU-missies, en de ambassades van de Frankrijk, Italië en Griekenland, alsook de ambassades van Japan, Mexico, Zuid Korea, India[494] en Turkije. Ook de Franse en Griekse missie bij de VN werden bespioneerd.[495] Le Monde gaf op 18 Oktober een document vrij dat aangaf dat 'close access' collectie op Amerikaans grondgebied tegen buitenlandse diplomatieke doelwitten bekend stond als SIGAD US-3136. Een suffix van twee letters daarnaast duidt op de specifieke locatie en missie. Het document van 10 September 2010 beschrijft een 15-tal manieren waarop informatie kon worden verkregen.[496] 'Close acces' collectie van diplomatie bronnen buiten de VS staat bekend als SIGAD US-3137 met een suffix van twee letters.

86. *Der Spiegel* beschreef verder hoe de NSA informatie uit de Franse diplomatie exploiteert. Een intern NSA-document uit juni 2010 beschreef hoe de NSA succesvol toegang had verkregen tot het VPN-netwerk van het Franse Ministerie van Buitenlandse Zaken, dat alle Franse ambassades en consulaten verbind met Parijs, en (interne) sub-domeinen van de 'diplomatie.gouv.fr' URL. NSA-agenten installeerden *bugs* in de Franse ambassade in Washington en in de Franse missie in New York. Nog steeds volgens *Der Spiegel*, is de

---

493 www.spiegel.de/international/world/secret-nsa-documents-show-how-the-us-spies-on-europe-and-the-un-a-918625-2.html.

494 Voor meer info zie S. SAXENA, *The Hindu,* 25 September 2013 ("NSA planted bugs at Indian missions in D.C., U.N.").

495 "*The US intelligence service codename for the bugging operation targeting the EU mission at the United Nations is "Perdido". The operation against the French mission to the UN had the covername "Blackfoot" and the one against its embassy in Washington was "Wabash". The Italian embassy in Washington was known to the NSA as both "Bruneau" and "Hemlock".The eavesdropping of the Greek UN mission was known as "Powell" and the operation against its embassy was referred to as "Klondyke".*" www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

496 HIGLANDS: collection from implants, VAGRANT: collection of computer Screens, MAGNETIC: sensor collection of magnetic emanations, MINERALIZE: collection from LAN implant, OCEAN: optical collection system for raster-based computer screens, LIFESAVER: imaging of the hard drive, GENIE: multi-stage operatoins; jumping the airgap etc.; BLACKHEART: collection from an FBI implant, PBX: Public Branch Exchange Switch, CRYPTO ENABLED: collection derived from AO's efforts to enable crypto, DROPMIRE (1) passive collection of emanations using an antenna (2) laser printer collection, purely proximal access, DEWSWEEPER: USB hardware host tap that provides covert link over USB link into a target network. Operates w/RF delay sybsytem to provide wireless bridge into target network. RADON: bi-directional host tap that can inject Ethernet packets onto the same target. Allows bi-direction exploitation of denied networks using standard on-net tools. Tegen de Franse missies werden bijvoorbeeld de HIGHLAND, VAGRANT en PBX technieken gebruikt. https://www.documentcloud.org/documents/807030-ambassade.html#document/p1.

NSA is vooral geïnteresseerd in Frankrijks buitenlandse politiek, vooral wapenhandel, en Frankrijks economische politiek.[497]

87. Een document van 17 mei 2006 dat gepost werd op de website van Globo meldde dat de International Security Issues (ISI) missie binnen de NSA verantwoordelijk is voor dertien individuele staten in drie continenten. Die dertien landen hebben met elkaar gemeen dat ze belangrijk zijn voor de VS inzake economie, handel en buitenlandse politiek. De 'Western Europe and Strategic Partnerships division' binnen die missie focust zich voornamelijk "*op de buitenlandse politiek en handelsactiviteiten van België, Frankrijk, Duitsland, Italië, Spanje als ook Brazilië, Japan en Mexico*". Deze divisie geeft ook *key intelligence* over 'militaire en intelligence activiteiten in enkele van deze landen'. De 'Aegean and Ukraine division' houdt zich bezig met alle aspecten van Turkije – 'governmental/leadership, military and intelligence'. ISI werkt samen met F6 en *second and third party* buitenlandse partners die zowel 'waardevolle analytische inzichten als technische capaciteiten' bevatten.[498] Volgens *Le Monde* verwijzen nummers die beginnen met US-98 (zoals US-985D (Frankrijk), US-987 (Duitsland)) naar SIGADS op het territorium van *third party* partners van de NSA. Die bestaan volgens *Der Spiegel* onder meer uit Frankrijk, Duitsland, Oostenrijk, Polen en België.[499] Hetzelfde document maakte melding van het feit dat de 'ISI' actief samenwerkt met de "*Combating Proliferation (CP, S2G) and Counterterrorism (CT, S2I) product lines to incorporate financial intelligence analysis into their mission build-out plans*".[500]

88. Een document van augustus 2010 bevestigt dat de NSA de communicaties onderschepte van acht leden van de VN Veiligheidsraad. Alleen Frankrijk, Japan, Mexico en Brazilië werden expliciet genoemd. Doel was om de US missie aan de VN (en andere Amerikaanse diensten) van de meest *up-to-date* informatie te voorzien over hun stemintenties en onderhandelingsposities over een VN-resolutie over sancties tegen Iran.[501]

89. Een bericht in *Globo* bevestigde hoe de NSA Latijns-Amerikaanse landen als Mexico, Venezuela, Argentinië, Colombia, Ecuador, Panama, Costa Rica, Nicaragua, Honduras, Chili, El Salvador en Peru bespioneerde. De NSA was geïnteresseerd in de olie-politiek van Venezuela, de energie- en drugspolitiek van Mexico en de Colombiaanse positie tegenover

---

497 X., *Der Spiegel*, 1 september 2013 ("'Success Story': NSA targeted French Foreign Ministry").

498 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html.

499 www.spiegel.de/fotostrecke/photo-gallery-nsa-documentation-of-spying-in-germany-fotostrecke-99672-3.html.

500 "*The idea is to integrate financial analysis with traditional target efforts as opposed to working the target from two separate perspectives, as is done in NSA Washington. ISI's long-term goal is to introduce financial analysis a part of the Intelligence Analysis curriculum so any target can be enriched with the use of financial intelligence*." In: http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html In die zin is het misschien interessant om op te merken dat volgens sommige bronnen van *De Standaard* er problemen zouden zijn vastgesteld bij de FOD Financiën, waarbij onderzocht werd of het om dezelfde malware als bij Belgacom gaat. Topman Hans D'Hondt van Financiën sprak echter formeel tegen dat zijn diensten gehackt of besmet zouden zijn. In: N. VANHECKE, P. DE LOBEL, *De Standaard*, 4 oktober 2013 ("Vrees voor massale besmetting").

501 http://epoca.globo.com/tempo/noticia/2013/07/spies-bdigital-ageb.html.

de FARC. Door het gebruik van XKEYSCORE kon een 'buitenlander' opgespoord worden door de taal die hij gebruikte om te communiceren.[502]

90. Een top-secret document uit November 2010, gepubliceerd door *Der Spiegel*, toont dat de NSA's TAO-divisie geslaagd was in operatie FLATLIQUID om toegang te krijgen tot de publieke e-mail account van de toenmalig Mexicaanse president Felipe Calderon om "*inzicht te krijgen in Mexico's politieke systeem en interne stabiliteit*". De account werd ook gebruikt door leden van Calderon's kabinet.[503] Gedurende een periode van twee weken in de vroege zomer van 2012 lanceerde de NSA ook een intensieve 'structurele surveillance' campagne tegen huidig president Enrique Pena Nieto. Op basis van zijn communicatiepatronen werd bepaald wie negen van zijn dichtste adviseurs waren. De gegevens van deze personen werden in de DISHIRE database gestoken, waarna ook hun communicaties onderschept werden. Op die manier werden bijvoorbeeld 85.489 sms'en onderschept. Doel van de operatie was om te bepalen of Mexico een nieuwe strategie zou aannemen vis-a-vis de drugskartels.[504] De NSA is vooral geïnteresseerd in de drughandel (niveau 1), de leiders van Mexico, Mexico's economische stabiliteit, militaire capaciteiten, mensenrechten en internationale handelsrelaties (niveau 3) en contraspionage (niveau 4). Om die doelen te bereiken voerde TAO in augustus 2009 'Operatie Whitetamale', waarmee het toegang kreeg tot de e-mails van verschillende hoge ambtenaren in Mexico's 'Public Security Secretariat' dat zich onder andere bezighoudt met drugshandel en mensenhandel. Via operatie EVENINGEASEL tapte de SCS divisie van de NSA vanuit de ambassade in Mexico stad telefoonconversaties af en las het sms'en die verstuurd werden via Mexico's mobiele telefoonnetwerk.[505]

91. Het Braziliaanse nieuwsprogramma Fantastico op de zender *Globo* toonde een slideshow waarin de communicatiepatronen tussen Braziliaans president Dilma Roussef, haar voornaamste adviseurs en derden werden getoond.[506] Volgens Glenn Greenwald had het desbetreffende NSA programma toegang tot het volledige communicatienetwerk van de Braziliaanse presidente en haar staff in kaart te brengen, inclusief telefoonconversaties, e-mails en uitwisselingen op sociale netwerk sites.[507]

92. DNI Clapper reageerde door te zeggen dat het 'geen geheim is dat de Intelligence community informatie verzamelt over economische en financiële zaken, en de financie-

---

502 http://oglobo.globo.com/mundo/espionagem-dos-eua-se-espalhou-pela-america-latina-8966619.

503 www.spiegel.de/fotostrecke/photo-gallery-nsa-hacked-into-mexican-president-s-email-account-fotostrecke-102797-2.html.

504 www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

505 www.spiegel.de/international/world/nsa-hacked-email-account-of-mexican-president-a-928817.html.

506 http://g1.globo.com/fantastico/noticia/2013/09/veja-os-documentos-ultrassecretos-que-comprovam-espionagem-dilma.html.

507 Y. MARULL, *AFP*, 2 september 2013 ("Brazil, Mexico summon US envoys over spy claims"). Een vertegenwoordiger van het State Department zei: "*while we are not going to comment publicly on every specific alleged intelligence activity, as a matter of policy we have made clear that the United States gathers foreign intelligence of the type gathered by all nations*".

ring van terrorisme'. Volgens Clapper verzamelt de VS dit soort informatie onder meer om de VS en haar partners *early warnings* te geven over internationale financiële crisissen die een negatief effect zouden kunnen hebben op de wereldeconomie.[508]

93. Een dag later melde Fantastico dat de NSA ook het interne computernetwerk van de Braziliaanse oliemaatschappij Petrobras als een spionagedoelwit zag. Een presentatie uit mei 2012 die als doel had om nieuwe NSA-agenten op te leiden in manieren om toegang te verkrijgen tot private computernetwerken, vermeldde de maatschappij als doelwit. Het is niet duidelijk welke informatie precies werd gezocht of verkregen, maar *Globo* suggereert dat dit over informatie kon gaan zoals details over de meest waardevolle ongeëxploiteerde olievelden die binnenkort door Petrobras zouden aangeboden worden in een veiling, of over informatie over *state-of-the art ocean-floor exploration* technologie. De presentatie werd (nog) niet online gezet.[509] Dezelfde presentatie melde ook dat Google, Franse diplomaten die toegang hadden tot het privé netwerk van het ministerie van Buitenlandse Zaken van Frankrijk[510] en SWIFT gezien werden als doelwitten.

94. Een GCHQ-slideshow toont hoe GCHQ data verzamelde van de smartphones, inclusief Blackberries, van verschillende diplomatieke delegaties op de G20 meeting in Londen in 2009.[511] Die data kon bijna in 'real time' doorgestuurd worden naar analisten, die briefings konden maken voor Britse ministers, inclusief Gordon Brown.[512] Op basis van deze informatie werden ook twintig nieuwe 'e-mail selectors' gevonden.[513] GCHQ ging heel ver om dergelijke diplomatieke informatie in te winnen. Zo werd een vals internetcafé opgezet waar *key-loggers* alles konden zien wat een délégué intypte op een computer. Een ander document toonde aan dat GCHQ succesvol het netwerk van het Zuid-Afrikaanse Ministerie van Buitenlandse Zaken had gekraakt, waardoor onder meer briefings onderschept konden worden voor délégués op de G20 en G8 meetings. Ook wordt melding gemaakt van GCHQ-pogingen om geëncrypteerde telefoongesprekken van Medvedev en andere Russische délégués te onderscheppen wanneer deze zich in Londen bevonden. GCHQ bespioneerde ook de Turkse Minister van Financiën op de meeting, alsook vijftien

---

508 Statement by Director of National Intelligence James R. Clapper on Allegations of Economic Espionage, 8 september 2013, zie: http://icontherecord.tumblr.com/post/60712026846/statement-by-director-of-national-intelligence. "*What we do not do, as we have said many times, is use our foreign intelligence capabilities to steal the trade secrets of foreign companies on behalf of – or give intelligence we collect to – US companies to enhance their international competitiveness or increase their bottom line.*"

509 www.reuters.com/article/2013/09/09/us-usa-security-snowden-petrobras-idUSBRE98817N20130909.

510 www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

511 "*The document refers to a tactic which was "used a lot in recent UK conference, eg G20" (…) the tactic is defined in an internal glossary as "active collection against an email account that acquires mail messages without removing them from the remote server". A PowerPoint slide explains that this means "reading people's email before/as they do*". In: www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.

512 Gordon Brown zat de G20 voor en wou vooruitgang boeken op twee fronten: de coordinatie van de globale economisch heropleving om een nieuwe recessie te voorkomen en een overeenkomst om *global economic governance* te versterken en internationale financiële institutions te hervormen.

513 www.theguardian.com/uk/interactive/2013/jun/16/gchq-surveillance-the-documents.

andere leden van zijn delegatie. GCHQ probeerde ook een nieuwe techniek uit op de meeting die het telefoonverkeer van alle deelnemers in kaart bracht.[514]

95. De UK plande een operatie om verschillende delegaties op de Commonwealth 'Heads of Government' meeting te bespioneren in Trinidad in 2009 om de UK extra diplomatieke informatie te geven. Een document beschrijft bijvoorbeeld hoe sigint moest verzameld worden over Zuid Afrika's opinie over Zimbabwe vooraleer Prime Minister Brown een ontmoeting had met Zuma. Het is niet duidelijk of er effectief sigint verzameld werd.[515]

BIJLAGE: AFKORTINGEN EN BEGRIPPEN

1EF solution	One-End Foreign solution
ADIV	Algemene Dienst inlichting en veiligheid
AG	Attorney General
BICS	Belgacom International Carrier Services
BIPT	Belgisch Instituut voor Postdiensten en Telecommunicatie
BND	Bundesnachrichtendienst (DE)
CERT-EU	Computer Emergency Response Team
CLANSIG	clandestine signals collection
CIA	Central Intelligence Agency
CNE	Computer Network Exploitation
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DITU	Data Intercept Technology Unit van de FBI
DNI	(1) Director of National Intelligence in de V.S. (James Clapper), (2) Digital Network Intelligence
DNR	Dialed Number Recognition
ECI	Exceptionally Controlled Information
EO 12333	Executive Order 12333
ECI	Exceptionally Controlled Information
EXIF	Exchangeable image file format
FAA	FISA Amendments Act
FBI	Federal Bureau of Investigation
FCCU	Federal Computer Crime Unit
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
Five eyes	De SIGINT-agentschappen van de V.S., de U.K, Australië, Canada en Nieuw Zeeland
Fornsat	Informatie afkomstig van satellieten
FTC	Federal Trade Commission
FRA	Försvarets radioanstalt (Zweeds SIGINT-agentschap)

514 www.theguardian.com/uk/2013/jun/16/gchq-intercepted-communications-g20-summits.
515 www.theguardian.com/world/2013/jun/16/uk-intelligence-agencies-spy-commonwealth-delegates.

F6-sites	Diplomatieke en consulaire missies van de VS
GAO	Global Access Operations-divisie (NSA)
GCHQ	Government Communications Headquarters (UK)
HOT	Humint Operations Team
IM	Instant Messaging
ISA	Intelligence Services Act (UK)
ISC	Intelligence Security Committee
Metadata	Metadata – soms ook 'communications data' of 'traffic data' genoemd, is de informatie die gecreëerd wordt wanneer data verzonden wordt. De precieze inhoud is afhankelijk van het type data dat verzonden wordt en hangt ook soms af van de lokale wetgeving. – Voor *vaste telefoonlijnen*: nummers die gebeld werden via dat toestel, alsook de datum en de tijd waarop een nummer gebeld en opgebeld werd. Soms ook de naam en het adres van de persoon die het contract van de vaste lijn heeft afgesloten. – *Mobiele telefoons*: (1) nummers die gebeld of ge-sms't werden via dat toestel, (2) de datum en de tijd waarop een nummer gebeld of opgebeld werd of een sms stuurde of ontving, (3) de locatie van waar er gebeld of ge-sms't werd, en waar die communicatie ontvangen werd. (4) Soms ook de naam en het adres van de persoon die het contract van de vaste lijn heeft afgesloten. (5) Soms ook het International Mobile Subscriber Identity (IMSI) nummer en (6) het International Mobile station Equipment Identity (IMEI) nummer. (6) Soms ook de nummer van de telefoonkaart die gebruikt werd. – *Voice over Internet Protocol (VoIP), e-mail, chat, Facebookberichten*: (1) online gebruikersnaam, login naam of accountnaam waarmee iemand belt, gesprekken ontvangt, e-mails verzendt, chatberichten verstuurd (2) het IP adres van de computers die gebruikt werden, (3) de tijd en datum van de communicatie. Sommige landen lijken ook de onderwerp-lijn van e-mails als metadata te zien. – *Internet surfgedrag:* (1) IP adres van het toestel waarmee iemand online gaat (2) de tijd en datum van het in- en uitloggen, en een lijst van webdomeinen die bezocht werden.
NCtC	National Counterterorrism Center
MTI	Mastering the Internet
NSA	National Security Agency
OSN	Online Social Networking
PNR	Passenger Name Records
PSTN	Public switched telephone network
RIPA	Regulation of Investigatory Powers Act (UK)
SCIF	Secure Compartmented Intelligence Facility
SCS	Special Collection Service
SHAPE	Supreme Headquarters Allied Powers Europe
SIGAD	Signals activity/address designators – kunnen verwijzen naar een specifiek fysiek collectieplatform (zoals bijvoorbeeld een Amerikaanse

	legerbasis in het buitenland, een ambassade, een schip.), een virtueel dataverwerkingsplatform (PRISM staat bijvoorbeeld bekend als SIGAD US-984XN) of een ruimtesatelliet.
SIGINT	Signals Intelligence
SRP	Specialized Reconnaissance Program
SSL	Secure Sockets Layer
SSO	Special Source Operations
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAO	Tailored Access Operations
TBB	Tor Browser Bundle
TFTP	Terrorist Finance Tracking Program
TIDE	Terrorist Identities Datamart Environment
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video teleconferencing systeem
XKS	Xkeyscore

BIJLAGE E.
ADVIES OVER DE IN BELGIË GELDENDE REGELS TER BESCHERMING VAN DE PRIVACY TEN AANZIEN VAN MIDDELEN DIE TOELATEN OP GROTE SCHAAL GEGEVENS VAN IN BELGIË VERBLIJVENDE PERSONEN, ORGANISATIES, ONDERNEMINGEN OF INSTANTIES (OF DIE ENIGE LINK HEBBEN MET BELGIË) TE ONDERSCHEPPEN EN TE EXPLOITEREN

Annemie Schaus
Gewoon hooglerares
Vice-rector academisch beleid
Université libre de Bruxelles

I. KORTE BESCHRIJVING VAN DE BEKENDE CONTEXT VAN DE MASSALE ONDERSCHEPPING VAN PERSOONSGEGEVENS[516]

Enorme hoeveelheden persoonsgegevens werden onderschept door het programma *PRISM*, dat inlichtingen verzamelt op een nooit geziene schaal en niveau en waarvan het doel veel verder reikt dan het bestrijden van terrorisme of economische spionage.

Hoewel er onduidelijkheid blijft bestaan over de precieze feiten en vooral de rol van bepaalde betrokkenen, lijkt iedereen het eens over de omvang van de onderschepping, monitoring en exploitatie van persoonsgegevens. Na de eerste onthullingen over *PRISM* bevestigde de directeur van het *NSA* namelijk dat de dienst zowel binnen als buiten de Verenigde Staten metagegevens over communicatie verzamelt bij alle grote operatoren en deze metagegevens gedurende vijf jaar opslaat in een database.[517]

Het is ook bewezen dat het *GCHQ* hetzelfde type intercepties heeft verricht en dat grote operatoren van communicatienetwerken of sociale netwerken[518] grote hoeveelheden persoonsgegevens hebben bezorgd aan het *NSA*.

---

516 Zie het verslag van Mathias Vermeulen, "De Snowden-revelaties, massale datacaptatie en politieke spionage. Open bronnenonderzoek", 25 november 2013.

517 *Le programme de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE,* Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burger en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR; zie ook het verslag van Mathias Vermeulen.

518 Onder andere *Facebook, Twitter, Microsoft, Google, Yahoo!, PalTalk, YouTube, Skype, AOL* en*Apple;* zie het verslag van Mathias Vermeulen.

II. TOEPASSELIJKE WETGEVING

Eerst en vooral moet er op worden gewezen dat er niet wordt getwijfeld aan de verenigbaarheid van het bestaan van de inlichtingendiensten met het Europees Verdrag tot bescherming van de rechten van de mens.[519] Zoals het Europees Hof voor de Rechten van de Mens benadrukte, kan de bescherming van de mensenrechten het bestaan van inlichtingendiensten vereisen, op voorwaarde dat hun methodes de fundamentele beginselen inzake de bescherming van de mensenrechten in acht nemen:"*Quel que soit le système de surveillance retenu, la Cour doit se convaincre de l'existence de garanties adéquates et suffisantes contre les abus. Cette appréciation ne revêt qu'un caractère relatif: elle dépend de toutes les circonstances de la cause, par exemple la nature, l'étendue et la durée des mesures éventuelles, les raisons requises pour les ordonner, les autorités compétentes pour les permettre, exécuter et contrôler, le type de recours fourni par le droit interne*".[520, 521]

Het Hof benadrukt dat de bewegingsruimte van de Verdragsluitende Staten niet onbeperkt is om personen binnen hun jurisdictie te onderwerpen aan maatregelen van geheime monitoring. In het besef dat de democratie dreigt te worden miskend of zelfs vernietigd in een poging haar te beschermen, wijst het Hof erop dat de Staten niet om het even welke maatregelen mogen nemen die ze geschikt achten in naam van de strijd tegen spionage en terrorisme.

Ter zake moeten de beginselen van legaliteit, finaliteit en proportionaliteit in acht worden genomen zodra het legitiem doel is vastgesteld.[522] Dit betekent dat het juridisch arsenaal om de privacy en de persoonsgegevens te beschermen in acht moet worden genomen (A), maar ook de soevereiniteit van de Staat op het grondgebied waarvan de persoonsgegevens worden verzameld, opgeslagen en verwerkt (B). Voor zover de feiten die ons zijn voorgelegd dat mogelijk maken, zullen we analyseren in hoeverre de regels toepasselijk zijn op het massaal verzamelen van persoonsgegevens waarvan wij kennis hebben gekregen. Tot slot geven we een overzicht van de eventuele rechtsmiddelen (C).

A. NALEVING VAN HET RECHT OP EERBIEDIGING VAN HET PRIVÉLEVEN EN BESCHERMING VAN PERSOONSGEGEVENS

In deze zaak kunnen verschillende wetsbepalingen ter bescherming van het recht op eerbiediging van het privéleven van toepassing zijn; die bepalingen *vullen elkaar aan*. We

519 Hierna EVRM.

520 EHRM, *Klass en anderen tegen Duitsland* van 6 september 1978; EHRM, *Vereniging weekblad Bluf! tegen Nederland* van 9 februari 1995 (vrije vertaling).

521 "Welk monitoringsysteem er ook wordt gebruikt, het Hof moet zich vergewissen van het bestaan van passende en voldoende garanties tegen misbruiken. Deze beoordeling is slechts van relatieve aard: ze is afhankelijk van alle omstandigheden van de zaak, zoals de aard, de omvang en de duur van eventuele maatregelen, de vereiste redenen om daartoe het bevel te geven, de bevoegde overheden om toelating te geven voor die maatregelen, ze uit te voeren en te controleren, het type verhaal krachtens het intern recht" (vrije vertaling).

522 Terwijl de bestrijding van terrorisme een geldig doel kan vormen, geldt dat niet noodzakelijk voor de economische profilering van individuen.

zullen die bepalingen beknopt toelichten, gaande van de bepaling met de meest algemene draagwijdte tot de bepaling met een specifieker doel, i.e. artikel 17 van het Verdrag inzake burgerrechten en politieke rechten (1); artikel 8 van het EVRM (2); Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens (3) en het recht van de Europese Unie: artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie (4), Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens [523] (zoals aangevuld door Richtlijn 2002/58/EG van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie) (5) en Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van openbaar beschikbare elektronische communicatiediensten of van openbare communicatienetwerken en tot wijziging van Richtlijn 2002/58/EG [524] (6). Tot slot moet verwezen worden naar het territoriaal toepassingsgebied van de Belgische wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens [525, 526]; het is niet duidelijk of die voorwaarden in casu vervuld zijn. In het kader van deze studie kunnen we deze wetgeving dus niet specifiek analyseren. Voor zover ze aansluit bij de bepalingen van internationaal recht en het ter zake toepasselijk Europees recht uitvoert, zijn de onderstaande analyses ook van toepassing op de bewuste wetgeving.

Vervolgens bekijken we hoe de eerbiediging van de normen inzake de bescherming van persoonsgegevens het voorwerp is geweest van het *Safe Harbor*-akkoord tussen de EU en de Verenigde Staten (7).

Op het vlak van de doorgifte, de monitoring, de controle en de bewaring van persoonsgegevens door middel van nieuwe technologieën moet – zoals Cécile de Terwangne en Jean-Noël Colin benadrukken [527] – privacy niet worden geïnterpreteerd in de klassieke betekenis, namelijk in die van bescherming van de persoonlijke, intieme, familiale of vertrouwelijke levenssfeer. Overeenkomstig de evolutie van het recht en de technologieën moet privacy worden begrepen als de mogelijkheid tot zelfbeschikking en autonomie en het vermogen van het individu om existentiële of informatieve keuzes te maken.[528] In overeenstemming met het Handvest van de grondrechten van de Europese Unie[529] gaat het om informatieve zelfbeschikking, i.e. het recht van het individu om kennis te hebben

523 Hierna "Richtlijn 95/46".

524 Hierna "Richtlijn 2006/24".

525 Hierna "WBPL".

526 De WBPL is van toepassing op de verwerking van persoonsgegevens wanneer de verwerking wordt verricht in het kader van de effectieve en daadwerkelijke activiteiten van een vaste vestiging van de verantwoordelijke voor de verwerking op het Belgisch grondgebied, zoals aangegeven door artikel 3*bis*, 1°.

527 *Défis pour la vie privée et la protection des données posés par la technologie,* Verslag, Namen FNDP, februari 2011.

528 Voor de expliciete erkenning van een recht op zelfbeschikking of persoonlijke autonomie zoals vervat in het recht op eerbiediging van het privéleven van artikel 8 EVRM, zie EHRM, *Evans tegen Verenigd Koninkrijk,* arrest van 7 maart 2006 (bevestigd door de Grote Kamer in zijn arrest van 10 april 2007); *Tysiac tegen Polen*, arrest van 20 maart 2007; *Daroczy tegen Hongarije*, arrest van 1 juli 2008.

529 Zie *infra* en de volgende voetnoot.

van de gegevens die op hem betrekking hebben en die worden bijgehouden, de kanalen te beheersen via dewelke die gegevens worden gecommuniceerd en het ongepast of bedrieglijk gebruik ervan te beletten. Op dit gebied is persoonlijke levenssfeer dus niet beperkt tot een zoeken naar privacy, maar gaat het om de beheersing door elk individu van zijn 'informatiebeeld'.[530] Dit gezegd zijnde en zoals het EHRM benadrukt, *"la protection des données à caractère personnel joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la Convention"*.[531, 532] Het is in deze betekenis dat persoonlijke levenssfeer hier moet worden begrepen.

1. Artikel 17 van het Internationaal verdrag inzake burgerrechten en politieke rechten[533]

Artikel 17 van het IVBPR is de enige internationale bepaling met universele draagwijdte die het recht op eerbiediging van het privéleven garandeert. Net als de zusterbepalingen van dit artikel 17, die van dezelfde periode dateren, verwijst dit artikel nergens naar persoonsgegevens als onderdeel van het recht op eerbiediging van het privéleven. Echter wordt die privacy, die beschermd wordt door Artikel 17, op de proef gesteld door nieuwe inmengingen die mogelijk gemaakt worden door nieuwe technologieën. Daarom spoort de 35ste internationale conferentie van commissarissen voor privacy en gegevensbescherming de Staten ertoe aan algemene opmerking nr. 16 van het IVBPR van 1988 aan te nemen, om zo de bescherming van het privéleven te versterken.[534] Die opmerking stimuleert de creatie van een wereldwijd rechtskader voor de bescherming van persoonsgegevens en van de persoonlijke levenssfeer. De Verenigde Staten hebben deze opmerking niet aangenomen en dat is de reden waarom tal van voorstellen tot doel hebben om artikel 17 van het IVBPR zelf aan te passen aan het digitale tijdperk[535], aangezien de Verenigde Staten dat Verdrag hebben getekend. Anderen stellen voor om een bijkomend protocol aan te nemen op basis van Algemene Opmerking nr. 16 zoals goedgekeurd door de Algemene Vergadering van de Verenigde Naties in 1996.[536]

Onlangs heeft de derde Commissie van de Algemene Vergadering van de Verenigde Naties een tekst aangenomen over het recht op eerbiediging van het privéleven in het digi-

---

530 Paul De Hert, Katja de Vries en Serge Gutwirth, Observatienota over het arrest van het Duits federaal Grondwettelijk Hof van 27 februari 2008, *Revue du droit des technologies et de l'information,* 2009, p. 87. In dit arrest kent het Hof op basis van het algemeen recht van persoonlijkheid een volkomen nieuw fundamenteel recht toe op de bescherming van "de vertrouwelijkheid en de integriteit van de technologische informatiesystemen". Dit nieuw fundamenteel recht inzake informatietechnologie moet lacunes in de bestaande fundamentele rechten aanvullen.

531 EHRM, *S. en Marper tegen Verenigd Koninkrijk* van 4 december 2008.

532 "speelt de bescherming van persoonsgegevens een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privéleven en het familie- en gezinsleven zoals bekrachtigd door artikel 8 van het Verdrag" (vrije vertaling).

533 Hierna "IVBPR".

534 www.unhchr.ch/tbs/doc.nsf/0/7dc7e7821c5da97680256523004a423d?Opendocument.

535 www.franceonu.org/IMG/pdf/Vie_privee_FR.pdf.

536 Http://droitdu.net/2013/10/35eme-conference-internationale-des-commissaires-a-la-protection-des-donnees-et-de-la-vie-privee-une-volonte-duniformiser-la-protection-des-donnees-personnelles/.

tale tijdperk.[537] Ze beveelt de bescherming van de persoonlijke levenssfeer aan van personen, zowel offline als online, en vraagt alle Lidstaten om "het recht op eerbiediging van het privéleven in acht te nemen en te beschermen, meer bepaald in de context van de digitale communicatie".[538] De interpretatie die vandaag aan artikel 17 van het IVBPR kan worden gegeven, is dat de bescherming van dit artikel betrekking heeft op persoonsgegevens.

2. Artikel 8 van het EVRM

Artikel 8 van het EVRM verzekert aan eenieder het recht op eerbiediging van het privéleven. Het Europees Hof voor de Rechten van de Mens heeft de draagwijdte van het concept 'privéleven' uitdrukkelijk uitgebreid tot de bescherming van persoonsgegevens. Voor het Hof speelt de bescherming van persoonsgegevens een fundamentele rol voor de uitoefening van het recht op eerbiediging van het privéleven zoals bekrachtigd door artikel 8.[539] Het Hof oordeelt dat *"la protection offerte par l'article 8 serait affaiblie de manière inacceptable si l'usage des techniques scientifiques modernes dans le système de la justice pénale était autorisé à n'importe quel prix et sans une mise en balance attentive des avantages pouvant résulter d'un large recours à ces techniques, d'une part, et des intérêts essentiels s'attachant à la protection de la vie privée, d'autre part."*[540, 541]

Volgens het Hof brengt artikel 8 de verplichting mee dat het intern recht voorziet in passende garanties om elk ongepast en onrechtmatig gebruik van persoonsgegevens te voorkomen. De nationale wetgeving moet ook verzekeren dat de gegevens relevant en niet excessief zijn ten opzichte van de doeleinden waarvoor ze zijn opgeslagen en dat ze slechts worden bewaard gedurende de periode die vereist is voor de doeleinden waarvoor ze zijn opgeslagen, in een vorm die de identificatie van personen mogelijk maakt.

Het Hof wijst erop dat *"dans ce contexte comme dans celui des écoutes téléphoniques, de la surveillance secrète et de la collecte secrète de renseignements, il est essentiel de fixer des règles claires et détaillées régissant la portée et l'application des mesures et imposant un minimum d'exigences concernant, notamment, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures destinées à préserver l'intégrité et la confidentialité des données et les procédures de destruction de celles-ci, de manière à ce que les justiciables disposent de garanties suffisantes contre les risques d'abus et d'arbitraire […]"*[542]

---

537 www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1&Lang=F.

538 Artikel 4 van de tekst van de derde Commissie van de Algemene Vergadering van de Verenigde Naties.

539 Zie document "Case law of the European Court of Human Rights concerning the protection of personal data", DP(2013)CASE LAW, 30 januari 2013 [niet beschikbaar in het Nederlands], www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/DP%202013%20Case%20 Law_Eng%20%28final%29.pdf.

540 EHRM, *S. en Marper tegen Verenigd Koninkrijk* van 4 december 2008.

541 "de bescherming geboden door artikel 8 op onaanvaardbare wijze zou worden verzwakt indien het gebruik van moderne wetenschappelijke technieken in het systeem van het strafrecht zou worden toegelaten tegen gelijk welke prijs en zonder nauwgezette afweging van enerzijds de voordelen die kunnen voortvloeien uit een grootschalig gebruik van die technieken en anderzijds de essentiële belangen van de bescherming van het privéleven" (vrije vertaling).

542 "het in deze context, net als in die van het afluisteren van telefoongesprekken, het geheim toezicht en de geheime inzameling van inlichtingen, van wezenlijk belang is om duidelijke en gedetailleerde regels vast te leggen die de draagwijdte en de toepassing van de maatregelen vastleggen en een minimum aan vereisten opleggen betreffende meer bepaald de duur, de

Aldus oordeelde het Hof dat de opslag door een overheidsinstantie van gegevens over de persoonlijke levenssfeer van een individu een inmenging vormde in het recht op eerbiediging van zijn privéleven zoals gewaarborgd door artikel 8, lid 1 van het EVRM, en verduidelijkte dat het gebruik van die gegevens er weinig toe doet, meer bepaald in de volgende bewoordingen:

> "De opslag door een overheidsinstantie van gegevens over de persoonlijke levenssfeer van een individu vormt een inmenging in de betekenis van artikel 8. Het later gebruik van de opgeslagen informatie is van weinig tel." (vrije vertaling).[543]

De inzameling en de bewaring van gegevens moeten dus de garanties inhouden die noodzakelijk zijn om het recht op eerbiediging van het privéleven van de individuen te beschermen.[544]

Op 1 juli 2008 veroordeelde het Hof (in een zaak met gelijkaardige feiten) het Verenigd Koninkrijk wegens inbreuk op artikel 8 voor het illegaal onderscheppen van communicatie te land door de inlichtingendienst *GCHQ,* van 1990 tot 1998. Het *GCHQ* onderschepte alle communicatie te land (fax, e-mail, telex en informatica) vanuit en naar de Ierse Republiek via de toren van *Capenhurst,* die binnen een kerncentrale ligt en 24 uur per dag operationeel is. De toren van *Capenhurst* diende niet alleen om informatie over terrorisme te verzamelen, maar werd ook gebruikt in het kader van economische spionage en voor het onderscheppen van diplomatieke communicatie van Ierland en persoonlijke communicatie van vooraanstaande Ieren, met behulp van specifieke lijsten van telefoonnummers of systemen van stemherkenning.[545]

Het EHRM is ook van mening dat de Staten verplicht zijn om een doeltreffende procedure in te voeren die het de belanghebbenden mogelijk maakt toegang te hebben tot de documenten die de veiligheidsdiensten over hen verzamelen.[546]

De grootschaligheid van de interceptie, waarbij zonder onderscheid te werk wordt gegaan, de monitoring, het gebruik en de bewaring van persoonsgegevens waarvan in deze zaak sprake is, zijn in alle opzichten duidelijk strijdig met artikel 8; de gelaakte maatregelen hebben op onbepaalde wijze betrekking op private of publieke natuurlijke of rechtspersonen; de slachtoffers zijn meestal niet-identificeerbaar; deze maatregelen steunen op geen enkele geldige wettelijke basis en miskennen integendeel het recht dat van toepassing is op de doorgifte van persoonsgegevens; ze staan kennelijk niet in verhouding tot de beoogde doelstellingen, die zelf ook niet gedefinieerd zijn.

Omdat sommige actoren die aan dit systeem zouden hebben deelgenomen privépersonen zouden kunnen zijn, past het te benadrukken dat artikel 8 van het EVRM een horizontaal effect kan hebben.

---

opslag, het gebruik, de toegang door derden, de procedures met het oog op het beschermen van de integriteit en de vertrouwelijkheid van de gegevens en de procedures tot vernietiging van die gegevens, zodat de rechtsonderhorigen voldoende garanties genieten tegen de risico's van misbruik en willekeur […]" (vrije vertaling).

543 EHRM, *Leander tegen Zweden* van 26 maart 1987; *Kopp tegen Zwitserland* van 25 maart 1998; *Amann tegen Zwitserland* van 16 februari 2000; *Association '21 Décembre 1989' en anderen tegen Roemenië* van 24 mei 2011.

544 EHRM, *Rotaru tegen Roemenië* van 4 mei 2000.

545 EHRM, *Liberty en andere ngo's tegen het Verenigd Koninkrijk* van 1 juli 2008.

546 EHRM, *Joanna Szulc tegen Polen* van 13 november 2012.

Al in 1979 benadrukte het Europees Hof voor de Rechten van de Mens immers het volgende:

> *"Si l'article 8 a essentiellement pour objet de prémunir l'individu contre les ingérences arbitraires des pouvoirs publics, il ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences: à cet engagement plutôt négatif s'ajoutent des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux".*[547, 548]

In het arrest *Soderman tegen Zweden* van 12 november 2013 wijst het Hof erop dat wanneer een bijzonder belangrijk aspect van het bestaan of de identiteit van een individu op het spel staat of de betrokken activiteiten betrekking hebben op een van de intiemste aspecten van het privéleven, de Staat nog minder bewegingsruimte heeft om de verplichting voor de particulieren te reglementeren.[549]

In hun activiteiten die afbreuk kunnen doen aan het recht op eerbiediging van het privéleven van individuen of publieke of private rechtspersonen vormt de eerbiediging van het privéleven duidelijk een verplichting voor providers van sociale netwerken, voor handelsondernemingen die actief zijn op het gebied van de nieuwe technologieën en voor andere verantwoordelijken voor de verwerking van persoonsgegevens, onder voorbehoud welteverstaan van een onderzoek in elk bijzonder geval van de territoriale werkingssfeer van de activiteit van die providers.[550]

3. Verdrag nr. 108 tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens

Verdrag nr. 108 van de Raad van Europa tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens is het enige bindende specifieke rechtsinstrument voor alle Lidstaten van de Raad van Europa op dit gebied. De beginselen zijn de volgende:

- beginsel van eerlijkheid, rechtmatigheid en evenredigheid met het doel (gegevens opgeslagen voor expliciete en legitieme doeleinden die niet worden gebruikt op een manier die onverenigbaar is met die doeleinden);
- beginsel van kwaliteit van de gegevens (relevant, passend, actueel, bewaard voor beperkte duur);
- specifieke regeling voor gevoelige gegevens;
- vereiste inzake veiligheid;
- recht op toegang, rectificatie en beroep;
- mogelijkheid tot afwijking in naam van doorslaggevende publieke of private belangen.

---

547 EHRM, *Airey tegen Ierland* van 9 oktober 1979.

548 "Hoewel artikel 8 voornamelijk tot doel heeft het individu te beschermen tegen de willekeurige inmenging van het openbaar gezag, beperkt het zich er niet toe aan de Staat te bevelen zich te onthouden van dergelijke inmenging: deze veeleer negatieve verbintenis gaat gepaard met positieve verplichtingen die inherent zijn aan de daadwerkelijke eerbieding van het privé-, familie- en gezinsleven. Die verplichtingen kunnen impliceren dat er maatregelen worden getroffen met het oog op de eerbiediging van het privéleven tot in de onderlinge relaties tussen individuen" (vrije vertaling).

549 Zie ook o.a. EHRM, *I.B. tegen Griekenland* van 3 oktober 2013.

550 Voor Richtlijn 95/46, zie *infra*.

In 2001 werd het Verdrag aangevuld met een bijkomend protocol betreffende de toezichthoudende autoriteiten en de grensoverschrijdende gegevensstromen. Het Verdrag nr. 108 is een van de beste rechtsinstrumenten om individuen te beschermen tegen de risico's die gepaard gaan met elektronische monitoring. Het verleent namelijk uitgebreide rechten, zoals een recht van toegang, verbetering of schrapping van persoonsgegevens.

Momenteel wordt het Verdrag gemoderniseerd[551] teneinde de leemtes te vullen die het jammer genoeg nog bevat ten opzichte van de technologische uitdagingen, meer bepaald met betrekking tot de extraterritoriale toepassing.[552]

4. Artikelen 7 en 8 van het Handvest van de grondrechten van de Europese Unie

Artikel 7 waarborgt het recht op eerbiediging van het privéleven in aansluiting op de overige instrumenten die de mensenrechten beschermen. Artikel 8 heeft een meer originele draagwijdte en bepaalt dat eenieder recht heeft op bescherming van de hem betreffende persoonsgegevens en dat deze gegevens eerlijk moeten worden verwerkt, voor bepaalde doeleinden en op basis van een gerechtvaardigde grondslag (toestemming of andere grondslag waarin de wet voorziet), alsook dat eenieder recht heeft op toegang tot en rectificatie van de over hem verzamelde gegevens. Artikel 7 bekrachtigt dus een autonoom recht op bescherming van persoonsgegevens.

Zoals advocaat-generaal Pedro Cruz Villalon onderstreept in zijn conclusies van 12 december ll.[553], bekrachtigt artikel 8 van het Handvest het recht op bescherming van persoonsgegevens als een recht dat zich onderscheidt van het recht op eerbiediging van het privéleven. Terwijl de bescherming van persoonsgegevens ertoe strekt de eerbiediging van het privéleven te waarborgen, is ze vooral onderworpen aan een autonome regeling die voornamelijk wordt gedefinieerd door Richtlijn 95/46, Richtlijn 2002/58, Verordening nr. 45/2001 en Richtlijn 2006/24, alsook, op het domein dat valt onder de politiële en justitiële samenwerking in strafzaken, door kaderbesluit 2008/977/JBZ.[554]

Omdat de 'privésfeer' de kern van de 'persoonlijke levenssfeer' vormt, valt omgekeerd niet uit te sluiten dat een regelgeving die het recht op bescherming van persoonsgegevens in overeenstemming met artikel 8 van het Handvest beperkt, niettemin kan worden geacht een buitensporige inbreuk op artikel 7 van het Handvest te vormen.[555]

Natuurlijk berust het recht op bescherming van persoonsgegevens op het fundamenteel recht op eerbiediging van het privéleven. Net als het HJEU kunnen we zeggen dat "*les*

---

551 Voorstel tot modernisering van het Raadgevend comité van het Verdrag tot bescherming van personen ten opzichte van de geautomatiseerde verwerking van persoonsgegevens, 18 december 2012, STE nr. 108 (T-PD); zie ontwerpaanbeveling www.coe.int/t/dghl/standardsetting/dataprotection/tpd_documents/T-PD %282013%295rev_fr_Projet%20de%20Rec.%20emploi.pdf; Over de herziening van *Verdrag nr. 108* Staat van de werkzaamheden in uitvoering: www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_fr.asp.

552 *Rapport sur les lacunes de la Convention n° 108 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel face aux développements technologiques,* Cécile de Terwangne, Jean-Philippe Moiny, Yves Poullet en Jean-Marc Van Gyzeghem, November 2010, Bureau van het Raadgevend Comité van het Verdrag nr. 108.

553 Conclusies van advocaat-generaal Pedro Cruz Villalon van 12 december 2013 in de zaken C-293/12 en C-494/12 die hangende zijn voor het HJEU.

554 Zie *infra*.

555 Conclusies van advocaat-generaal Pedro Cruz Villalon, voornoemd.

articles 7 et 8 de la Charte sont étroitement liés, au point de pouvoir être considérés comme établissant un "droit à la vie privée à l'égard du traitement des données à caractère personnel"[556, 557]

5. Richtlijn 95/46/EG van 24 oktober 1995

Richtlijn 95/46 van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, die in oktober 1998 in werking is getreden, is de basisnorm in het afgeleid communautair recht. Richtlijn 95/46 heeft tot doel aan de Lidstaten de verplichting op te leggen het recht op eerbiediging van de persoonlijke levenssfeer van natuurlijke personen ten aanzien van de verwerking van hun persoonsgegevens te waarborgen teneinde het vrije verkeer van die gegevens tussen de Lidstaten mogelijk te maken.

Bijgevolg legt ze de inachtneming op van regels die de voorwaarden van rechtmatigheid van de verwerking van persoonsgegevens bepalen, met vermelding van de rechten van personen wiens gegevens worden ingezameld en verwerkt (recht op informatie, recht op toegang en rectificatie of recht van verzet en recht op beroep, en recht op de vertrouwelijkheid en veiligheid van de verwerking).

Deze richtlijn werd aangevuld door Richtlijn 2002/58 van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie, die de vertrouwelijkheid van elektronische communicatie waarborgt. De verplichting om deze vertrouwelijkheid te waarborgen ligt bij de aanbieders van voor het publiek toegankelijke elektronische-communicatiediensten. Ze brengt voor de Lidstaten ook de verplichting mee, behoudens uitzondering, om de vertrouwelijkheid te waarborgen van niet alleen de communicatie, maar ook de verkeersgegevens van abonnees en gebruikers van elektronische-communicatiediensten. Artikel 6 verplicht aanbieders van elektronische-communicatiediensten ertoe om verkeersgegevens met betrekking tot abonnees en gebruikers die worden verwerkt en opgeslagen, te wissen of anoniem te maken.

– *Beginselen*

Richtlijn 95/46 heeft tot doel de rechten en vrijheden van personen te beschermen ten opzichte van de verwerking van persoonsgegevens, door beginselen vast te stellen tot bepaling van de rechtmatigheid van die verwerkingen.

Die beginselen[558] hebben betrekking op:

– de kwaliteit van de gegevens: persoonsgegevens moeten meer bepaald eerlijk en rechtmatig worden verwerkt en moeten worden ingezameld om welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden. Bovendien moeten ze nauwkeurig zijn en zo nodig worden bijgewerkt;

---

556 Arresten C-92/09 en C-93/09 van 9 november 2010.

557 "artikelen 7 en 8 van het Handvest nauw met elkaar zijn verbonden, in die mate dat ze kunnen worden geacht een recht op eerbiediging van het privéleven ten aanzien van de verwerking van persoonsgegevens te vestigen" (vrije vertaling).

558 Zie synthese van de wetgeving op: http://europa.eu/legislation_summaries/information_society/data_protection/l14012_nl.htm (december 2013).

- de *toelaatbaarheid* van de gegevensverwerking: persoonsgegevens mogen alleen worden verwerkt indien de betrokkene daarvoor zijn ondubbelzinnige toestemming heeft verleend of wanneer de verwerking noodzakelijk is:
- voor de uitvoering van een overeenkomst waarbij de betrokkene partij is; of
- om een wettelijke verplichting na te komen waaraan de verantwoordelijke voor de verwerking onderworpen is; of
- ter vrijwaring van een vitaal belang van de betrokkene; of
- voor de vervulling van een taak van algemeen belang; of
- voor de behartiging van het gerechtvaardigd belang van de verantwoordelijke voor de verwerking;
- bijzondere categorieën van verwerking: verboden is de verwerking van persoonsgegevens waaruit de raciale of etnische afkomst, de politieke opvattingen, de godsdienstige of levensbeschouwelijke overtuiging, of het lidmaatschap van een vakvereniging blijkt, alsook de verwerking van gegevens die de gezondheid of het seksuele leven betreffen. Deze bepaling is onder voorbehoud voor bijvoorbeeld het geval waarin de verwerking noodzakelijk is met het oog op de verdediging van de vitale belangen van de betrokkene of voor de doeleinden van preventieve geneeskunde of medische diagnose;
- informatie van de personen die betrokken zijn bij de gegevensverwerking: bepaalde gegevens (identiteit van de verantwoordelijke voor de verwerking, doeleinden van de verwerking, ontvangers van de gegevens …*)* moeten door de verantwoordelijke voor de verwerking worden verstrekt aan de persoon bij wie hij gegevens betreffende die persoon verzamelt;
- het recht van toegang van die personen tot de gegevens: elke betrokkene moet het recht hebben om van de verantwoordelijke voor de verwerking de volgende zaken te verkrijgen:
- uitsluitsel omtrent het al dan niet bestaan van verwerkingen van gegevens betreffende hem en verstrekking van de gegevens die zijn verwerkt;
- de rectificatie, de uitwissing of de afscherming van de gegevens waarvan de verwerking niet overeenstemt met de bepalingen van deze richtlijn, met name op grond van het onvolledige of onjuiste karakter van de gegevens, net als kennisgeving van deze wijzigingen aan derden aan wie de gegevens zijn verstrekt;
- *uitzonderingen en beperkingen*: de reikwijdte van de beginselen betreffende de kwaliteit van de gegevens, de informatieverstrekking aan de betrokkene, het recht van toegang en de openbaarheid van de verwerkingen kan worden beperkt ter vrijwaring, onder meer, van de veiligheid van de Staat, de landsverdediging, de openbare veiligheid, het vervolgen van strafbare feiten, een belangrijk economisch en financieel belang van een Lidstaat of van de EU of de bescherming van de betrokkene;
- het recht van verzet tegen gegevensverwerking: de betrokkene moet het recht hebben zich om gerechtvaardigde redenen te verzetten tegen de verwerking van gegevens die op hem betrekking hebben. De betrokkene moet zich, op verzoek en kosteloos, ook kunnen verzetten tegen de verwerking van gegevens met het oog op direct marketing. Tot slot moet de betrokkene worden ingelicht voordat persoonsgegevens aan derden worden verstrekt voor direct marketing en moet hij het recht ter kennis gebracht krijgen zich tegen deze verstrekking te kunnen verzetten;• de vertrouwelijkheid en beveiliging van de verwerking: eenieder die handelt onder het gezag van de verantwoorde-

lijke voor de verwerking of van de verwerker alsmede de verwerker zelf, die toegang heeft tot persoonsgegevens, mag deze slechts in opdracht van de verantwoordelijke voor de verwerking verwerken. Voorts moet de verantwoordelijke voor de verwerking passende maatregelen nemen om persoonsgegevens te beveiligen tegen vernietiging, hetzij per ongeluk, hetzij onrechtmatig, tegen verlies, vervalsing, niet-toegelaten verspreiding of toegang;

– aanmelding van de verwerking bij een toezichthoudende autoriteit: de verantwoordelijke voor de verwerking moet de nationale toezichthoudende autoriteit van tevoren kennis geven van de uitvoering van een verwerking. Na ontvangst van de kennisgeving voert de toezichthoudende autoriteit voorafgaande onderzoeken uit naar mogelijke risico's voor de rechten en vrijheden van de betrokkenen. De openbaarheid van de verwerkingen moet worden gewaarborgd en de toezichthoudende autoriteit moeten een register bijhouden van de aangemelde verwerkingen.

Eenieder kan zich tot de rechter wenden wanneer de rechten die hem worden gegarandeerd door het op de betrokken verwerking toepasselijke nationale recht geschonden worden. Bovendien hebben personen die schade hebben geleden ten gevolge van een onrechtmatige verwerking van hun persoonsgegevens het recht vergoeding van de geleden schade te verkrijgen.

– *Territoriale werkingssfeer*

Deze richtlijn brengt verplichtingen mee voor de aanbieders van internettoegang, zoekmachines, sociale netwerken en andere aanbieders van communicatiediensten die verantwoordelijk zijn voor de verwerking van persoonsgegevens. In ieder afzonderlijk geval kan de omvang van de aansprakelijkheid van de verantwoordelijke voor de gegevensverwerking worden geanalyseerd, meer bepaald ten aanzien van de territoriale werking van Richtlijn 95/46. Krachtens artikel 4 van de richtlijn moet een Staat zijn wetgeving inzake de bescherming van persoonsgegevens ter uitvoering van deze richtlijn toepassen indien de verantwoordelijke voor de verwerking vestiging heeft op zijn grondgebied of in functie van de plaats van de middelen voor de gegevensverwerking, dit wil zeggen indien de middelen voor gegevensverwerking op het grondgebied van deze Staat bevinden.
De werkgroep 'Artikel 29'[559] benadrukte in zijn advies 5/2009 over de bescherming van gegevens door online sociale netwerken[560] dat

> "De richtlijn gegevensbescherming is in de meeste gevallen van toepassing op aanbieders van sociale-netwerkdiensten, ook als hun hoofdkantoor buiten de EER is gevestigd."

Ook een van de voornaamste conclusies van advies 1/2008 over gegevensbescherming en zoekmachines bepaalt dat de richtlijn inzake gegevensbescherming algemeen van toepassing is op de verwerking van persoonsgegevens door zoekmachines, ook al staat hun hoofdkantoor buiten de EER, en dat het aan de betreffende zoekmachines toekomt duide-

559 Deze werkgroep werd opgericht krachtens artikel 29 van Richtlijn 95/46. Het is een Europees adviesorgaan, van wie de taken worden beschreven in artikel 30 van de Richtlijn en in artikel 15 van Richtlijn 2002/58.

560 Groep 29, WP 163 "Advies 5/2009 over online sociale netwerken" van 12 juni 2009.

lijk te maken welke rol zij spelen in de EER en hoe ver hun verantwoordelijkheden overeenkomstig de richtlijn reiken.[561]

De doorgifte van persoonsgegevens van een Lidstaat naar een derde land met een passend niveau van bescherming is toegelaten. Dergelijke doorgiftes zijn echter niet toegelaten wanneer ze bestemd zijn voor een derde land dat niet over een dergelijk niveau van bescherming beschikt, behoudens afwijkingen die op beperkende wijze worden opgesomd.

Bijgevolg past het om de verantwoordelijkheid van elke speler te bepalen in functie van precieze feiten.

– *Uitsluitingen van de materiële werkingssfeer*

Artikel 3, lid 2 van voornoemde richtlijn geeft een van de grenzen van de *materiële werkingssfeer* van de richtlijn aan en bepaalt:

> "De bepalingen van deze richtlijn zijn niet van toepassing op de verwerking van persoonsgegevens:
> – *die met het oog op de uitoefening van niet binnen de werkingssfeer van het Gemeenschapsrecht vallende activiteiten geschiedt zoals die bedoeld in de titels V en VI van het Verdrag betreffende de Europese Unie en in ieder geval verwerkingen die betrekking hebben op de openbare veiligheid, defensie, de veiligheid van de Staat (waaronder de economie van de Staat, wanneer deze verwerkingen in verband staan met vraagstukken van Staatsveiligheid), en de activiteiten van de Staat op strafrechtelijk gebied".*

De bescherming van persoonsgegevens in het kader van de openbare veiligheid en het strafrecht wordt dus geregeld in verschillende specifieke instrumenten. Het gaat met name om instrumenten waarbij gemeenschappelijke informatiesystemen op Europees niveau worden ingesteld, zoals de Schengenuitvoeringsovereenkomst met specifieke gegevensbeschermingsbepalingen die gelden voor het Schengeninformatiesysteem (SIS); de overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie tot oprichting van een Europese Politiedienst; het besluit van de Raad betreffende de oprichting van Eurojust en de beschikkingen van het interne reglement van Eurojust betreffende de verwerking en bescherming van persoonsgegevens; de Overeenkomst op grond van artikel K.3 van het Verdrag betreffende de Europese Unie inzake het gebruik van informatica op douanegebied, met de gegevensbeschermingsbepalingen die van toepassing zijn op het douane-informatiesysteem, en de Overeenkomst betreffende de wederzijdse rechtshulp in strafzaken tussen de Lidstaten van de Europese Unie.[562] Op 27 november 2008 keurde de Raad kaderbesluit 2008/977/JBZ van de Raad goed over de bescherming van persoonsgegevens die worden verwerkt in het kader van de politiële en gerechtelijke samenwerking in strafzaken. Deze is echter alleen van toepassing op de doorgifte van gegevens tussen Lidstaten (artikelen 26 en 13).

---

561 Groep 29, WP 148 "Advies 1/2008 over gegevensbescherming en zoekmachines" van 4 april 2008.

562 HJEU, arresten C-317/04 en C-318/04 van 30 mei 2005, conclusies van advocaat-generaal LEGER, punt 41.

6. *Richtlijn 2006/24/EG betreffende de bewaring van gegevens die zijn gegenereerd of verwerkt in verband met het aanbieden van elektronische communicatiediensten*

Richtlijn 2006/24 is in deze belangrijk omdat ze wijzigingen aanbrengt aan richtlijnen 95/46 en 2002/58 door te bepalen dat de Lidstaten een verplichting moeten opleggen inzake het verzamelen en bewaren van verkeers- en lokalisatiegegevens, namelijk door aan de aanbieders van openbaar beschikbare elektronische communicatiediensten of openbare communicatienetwerken verplichtingen op te leggen inzake de bewaring van de verkeers- en lokalisatiegegevens die zij bepaalt, teneinde hun beschikbaarheid te waarborgen "voor het onderzoeken, opsporen en vervolgen van zware criminaliteit zoals gedefinieerd in de nationale wetgevingen van de Lidstaten". Aldus wijkt deze richtlijn af van de afwijkende regels zoals vastgesteld door artikel 15, lid 1 van Richtlijn 2002/58 die de mogelijkheid regelen, voor de Lidstaten, om de reikwijdte van het recht op bescherming van persoonsgegevens en, algemener, het recht op eerbiediging van het privéleven in het specifieke kader van de levering van elektronische communicatiediensten of openbare communicatienetwerken te beperken om de redenen zoals bepaald in artikel 13, lid 1 van Richtlijn 95/46.
Richtlijn 2006/24 heeft tot doel een harmonisatie tot stand te brengen van de regelgevingen van de Lidstaten betreffende de bewaring van verkeers- en lokalisatiegegevens inzake elektronische communicatie en legt bijgevolg aan de Lidstaten die niet over dergelijke regelgeving zouden beschikken, een verplichting op om de voornoemde gegevens te verzamelen en te bewaren.
Volgens advocaat-generaal Pedro Cruz Villalon (12 december 2013) is deze verplichting die de richtlijn aan de Lidstaten oplegt in strijd met het Handvest van de grondrechten.[563] Het HJEU moet nog een arrest vellen.
Het is interessant om de motivering van de advocaat-generaal hier over te nemen[564]:

> "72. Dat neemt niet weg dat het verzamelen en vooral het bewaren, in gigantische databases, van de talloze gegevens die zijn gegenereerd of verwerkt in het kader van het grootste deel van de gebruikelijke elektronische communicatie van de burgers van de Unie, een duidelijke inmenging in hun privéleven vormt, ook al worden daarmee enkel de voorwaarden geschapen om achteraf hun persoonlijke alsook beroepsmatige activiteiten te kunnen controleren. Het verzamelen van deze gegevens creëert de voorwaarden voor een toezicht dat, ook al wordt dit slechts met terugwerkende kracht uitgevoerd bij de exploitatie van de gegevens, niettemin, zolang de gegevens worden bewaard, het recht van de burgers van de Unie op vertrouwelijkheid van hun persoonlijke levenssfeer permanent bedreigt. Het opgewekte vage gevoel van gecontroleerd worden leidt bijzonder acuut tot de vraag wat de bewaringstermijn van de gegevens is.
> *73. Dienaangaande moet ten eerste rekening worden gehouden met het feit dat de gevolgen van deze inmenging worden verveelvoudigd door de plaats die de elektronische communicatiemiddelen in de moderne samenleving hebben ingenomen, of het nu gaat om digitale mobiele netwerken dan wel om internet, en het massale en intensieve gebruik ervan door een zeer groot deel van de Europese burgers op alle terreinen van hun privé- of beroepsactiviteiten.*
> *74. De betrokken gegevens, zo wil ik nogmaals benadrukken, zijn geen persoonsgegevens in de klassieke zin des woords die verband houden met precieze informatie over de identiteit van perso-*

563 Conclusies in de zaken C-293/12 en C-494/12 die hangende zijn voor het HJEU.
564 De verwijzingen zijn weggelaten met het oog op de leesbaarheid; zie de verwijzing in de vorige voetnoot.

nen, maar in feite 'gekwalificeerde' persoonsgegevens, die, wanneer zij worden geëxploiteerd, een belangrijk deel van het gedrag van een persoon, dat strikt onder zijn privéleven valt, op getrouwe en uitputtende wijze in kaart kunnen brengen of zelfs een volledig en precies beeld kunnen schetsen van zijn privé-identiteit.
75. De intensiteit van deze inmenging wordt des te duidelijker door factoren die het risico vergroten dat de bewaarde gegevens, ondanks de verplichtingen die door richtlijn 2006/24 aan zowel de lidstaten zelf als de aanbieders van elektronische communicatiediensten worden opgelegd, worden gebruikt voor onrechtmatige doeleinden die potentieel inbreuk maken op het privéleven, of ruimer, voor frauduleuze of zelfs kwaadwillende doeleinden.
76. Deze gegevens worden namelijk niet bewaard door de autoriteiten zelf of zelfs maar onder hun directe toezicht, maar door de aanbieders van elektronische communicatiediensten, op wie het merendeel van de verplichtingen rust die als waarborg van de bescherming en de veiligheid van de gegevens moeten dienen."

En verder:

"102. De duidelijke inmenging in recht op eerbiediging van het privéleven die de lidstaten, als gevolg van de constitutieve werking van richtlijn 2006/24 geacht worden op te nemen in hun eigen rechtsorde, lijkt aldus buiten verhouding te staan tot enkel de noodzaak om de werking van de interne markt te waarborgen, ook al worden dit verzamelen en bewaren overigens als geschikte en zelfs noodzakelijke middelen beschouwd ter bereiking van de uiteindelijke doelstelling van de richtlijn, namelijk ervoor zorgen dat de gegevens beschikbaar zijn voor het opsporen en vervolgen van zware criminaliteit. Samenvattend zou richtlijn 2006/24 de evenredigheidstoets niet doorstaan op basis van de redenen die de keuze van haar rechtsgrondslag rechtvaardigden. Paradoxaal genoeg zouden de redenen die haar sauveerden vanuit het oogpunt van de rechtsgrondslag, de redenen zijn waarom zij geen stand houdt in het licht van de evenredigheid."

Alvorens te besluiten:

"131. Concluderend meen ik dat richtlijn 2006/24 in haar geheel onverenigbaar is met artikel 52, lid 1, van het Handvest, aangezien de beperkingen die zij aan de uitoefening van de grondrechten stelt door de opgelegde verplichting tot het bewaren van gegevens, niet gepaard gaan met de onmisbare beginselen die hebben te gelden voor de waarborgen waarmee de toegang tot deze gegevens en de exploitatie ervan behoren te zijn omkleed."

7. Safe Harbor-akkoord ('veilige haven') – Beschikking van de Commissie van 26 juli 2000[565]

De normen inzake bescherming van de persoonlijke levenssfeer in Europa enerzijds en de Verenigde Staten anderzijds verschillen duidelijk van elkaar en meer bepaald in de Ver-

[565] Beschikking van de Commissie van 26 juli 2000 overeenkomstig Richtlijn 95/46/EG van het Europees Parlement en de Raad, betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen voor de bescherming van de persoonlijke levenssfeer en de daarmee verband houdende vaak gestelde vragen, die door het ministerie van Handel van de Verenigde Staten zijn gepubliceerd document C(2000) 2441 (http://eur lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:NL:PDF).

enigde Staten biedt het recht op eerbiediging van het privéleven zoals hierboven omschreven nagenoeg geen bescherming voor wie niet in de VS verblijft.[566]

Het bleek dan ook noodzakelijk om een rechtskader te creëren dat geschikt is om de doorgifte van gegevens *voor commerciële doeleinden* van de Europese Economische Ruimte[567] naar de Verenigde Staten mogelijk te maken.

Dit rechtskader was des te noodzakelijker omdat, zoals we hebben gezien, de specifieke regels van Richtlijn 95/46 betreffende het uitwisselen van gegevens met derde Staten de doorgifte verbiedt van persoonsgegevens buiten Staten die geen lid zijn van de EER en die minder bescherming van persoonsgegevens zouden bieden dan de EER.

De Verenigde Staten beschikken over een systeem voor de bescherming van de gegevens van hun burgers dat niet voldoet aan dezelfde normen degene die binnen de EER zijn aangenomen. Zonder het *Safe Harbor*-systeem hadden de door Richtlijn 95/46 ingestelde vereisten een obstakel kunnen vormen voor de trans-Atlantische uitwisselingen en transacties, omdat het gebrek aan naleving van de Europese regels betreffende persoonsgegevens door een Amerikaanse onderneming de commerciële onderhandelingen had kunnen vertragen of opschorten of zelfs had kunnen leiden tot gerechtelijke vervolgingen in geval van schending van de toepasselijke regels.

Het rechtskader van de 'veilige haven' of *Safe Harbor* slaat de brug tussen beide visies op de eerbiediging van het privéleven door een gemeenschappelijke noemer in het leven te roepen die Amerikaanse ondernemingen en organisaties in acht moeten nemen en die de doorgifte van persoonsgegevens mogelijk maakt met inachtneming van het recht van de EER.

Het *Safe Harbor*-akkoord werd gesloten tussen de Amerikaanse *Federal Trade Commission* (*FTC*) en de Europese Commissie met als doel Amerikaanse ondernemingen in staat stellen te certificeren dat ze de EER-wetgeving in acht nemen om aldus de toelating te verkrijgen persoonsgegevens voor commerciële doeleinden door te geven van de EER naar de Verenigde Staten.

Bijlage I van de beschikking van 26 juli 2000 bepaalt dat "persoonsgegevens en persoonlijke informatie gegevens zijn over een specifieke of een identificeerbare persoon die binnen de werkingssfeer van de richtlijn vallen, vanuit de Europese Unie door een organisatie in de Verenigde Staten worden ontvangen en in de een of andere vorm zijn vastgelegd."

Indien een Amerikaanse onderneming schriftelijk verklaart de Veiligehavenbeginselen te onderschrijven, dan zou de Europese onderneming in principe persoonsgegevens naar die onderneming moeten kunnen uitvoeren.

– *Beginselen*

Het rechtskader van *Safe Harbor* berust op zeven beginselen die de onderneming die de certificering wenst te verkrijgen in acht moet nemen. Deze beginselen worden uitvoerig beschreven in Bijlage I van de Beschikking van de Commissie van 26 juli 2000 betreffende

566 Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burgers en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR.

567 Hierna "EER"; *Safe Harbor* werd opgenomen in het akkoord over de EER, zodat IJsland, Liechtenstein en Noorwegen niet worden beschouwd als derde Staten bij de toepassing van deze norm.

de gepastheid van de bescherming geboden door de Veiligehavenbeginselen en zijn grotendeels geïnspireerd op de beginselen van Richtlijn 95/46:
- Kennisgeving: in kennis stellen van personen,
- Keuze: de mogelijkheid voor de betrokkene om zich te verzetten tegen een doorgifte aan derden of tegen het gebruik van de gegevens om andere doeleinden, de expliciete toestemming van de personen voor het verzamelen van gevoelige informatie,
- Verdere doorgifte: de beginselen inzake kennisgeving en keuze zouden van toepassing moeten zijn op de doorgifte van gegevens aan derden,
- Beveiliging: maatregelen tot bescherming van de gegevens,
- Integriteit van de gegevens: kwaliteit en gepastheid van de gegevens,
- Toegang: het recht op toegang, correctie, verwijdering van gegevens,
- Rechtshandhaving: recht op verhaal, procedures van opvolging en sancties.[568]

Op te merken valt echter dat de beginselen worden omschreven in vage bewoordingen die open staan voor een interpretatie die bovendien onderworpen is aan het Amerikaans recht.

Het proces berust op een systeem van vrijwillige zelfcertificering door Amerikaanse ondernemingen en voorziet in een hernieuwing van de certificering om de twaalf maanden. De onderneming die een certificering wenst te verkrijgen, moet aan de *Federal Trade Commission* een jaarlijkse schriftelijke verklaring bezorgen waarin ze bevestigt de Veiligehavenbeginselen in acht te nemen. De *Federal Trade Commission* heeft de taak het certificeringsprogramma te beheren en te waken over de uitvoering ervan. Ze kan vorderingen in rechte instellen tegen een onderneming die in gebreke blijft of administratieve boetes opleggen aan ondernemingen die ondanks hun verklaring de Veiligehavenbeginselen *de facto* niet in acht nemen.

Eens de Amerikaanse onderneming een *Safe Harbor*-certificering heeft verkregen, wordt ze toegevoegd aan de lijst van geaccrediteerde ondernemingen die de *Federal Trade Commission* bijhoudt. De lijst telt 3.246 ondernemingen en kan worden geraadpleegd op de website van de Federal Trade Commission.[569]

Het *Safe Harbor*-systeem bepaalt ook dat de klachten van EER-burgers tegen een Amerikaanse onderneming of organisatie betreffende de bescherming van persoonsgegevens voor een Amerikaans rechtscollege moeten worden ingediend (behoudens enkele uitzonderingen).

In de praktijk gaat het er echter anders aan toe, zoals blijkt uit de recente studie in opdracht van het Europees Parlement over het *Safe Harbor-systeem:* "De Amerikaanse onderhandelaars van het ministerie van handel hebben nauw samengewerkt met de Amerikaanse commerciële lobby's om een lijst van 'vaak gestelde vragen' op te stellen die het voor Amerikaanse ondernemingen mogelijk maken het Veiligehavenakkoord op zodanige wijze te interpreteren dat de rechten van de EU inzake de bescherming van de persoonlijke levenssfeer worden beperkt en die aangeven hoe ze de regels inzake identificeerbare gegevens kunnen omzeilen, het recht op toegang kunnen weigeren en zich kunnen onttrekken aan elke plicht tot finaliteit of elk verzoek tot schrapping. De veilige haven is

---

568 Voor een gedetailleerde beschrijving van de 7 beginselen, zie Bijlage I van de beschikking van de Commissie van 26 juli 2000 (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:NL:PDF).

569 http://export.gov/safeharbor/ (eind september 2013).

zo complex gebleken dat er jarenlang geen enkele EU-burger is geweest die alle stappen van het bureaucratisch proces om klacht in te dienen heeft doorlopen." (vrije vertaling).[570]

Richtlijn 95/46 en de *Veiligehavenbeginselen* hebben geen betrekking op persoonsgegevens die worden verwerkt in het kader van de politiële en justitiële samenwerking in strafzaken[571], wat alle politie-, gerechts- en inlichtingenbestanden omvat. Artikel 1 van de Beschikking van de Commissie van 26 juli 2000 betreffende de gepastheid van de bescherming geboden door de Veiligehavenbeginselen bepaalt immers dat de beschikking alleen van toepassing is op activiteiten die binnen de werkingssfeer van Richtlijn 95/46 vallen.

Voorts bepaalt Bijlage I lid 4 van voornoemde beschikking dat "de naleving van de beginselen kan worden beperkt: a) voor zover dit nodig is om aan de *eisen van de nationale veiligheid*, het algemeen belang en de rechtshandhaving van de Verenigde Staten te voldoen; b) door wettelijke of bestuursrechtelijke bepalingen of rechtspraak die tegenstrijdige verplichtingen of uitdrukkelijke machtigingen scheppen, mits een organisatie die van een dergelijke machtiging gebruikmaakt, kan aantonen dat de niet-naleving van de beginselen beperkt is tot de mate die nodig is om de met de machtiging beoogde hogere legitieme belangen te waarborgen; c) indien de richtlijn of de wetgeving van de betrokken lidstaat uitzonderingen of afwijkingen toestaat, mits deze ook in vergelijkbare contexten worden toegepast."

De uitwisseling van persoonsgegevens tussen de Europese Unie en de Verenigde Staten voor rechtshandhavingsdoeleinden, met inbegrip van het voorkomen en bestrijden van terrorisme en andere vormen van zware criminaliteit, is, althans in theorie, geregeld in een aantal overeenkomsten op EU-niveau. Het gaat om de overeenkomst inzake wederzijdse rechtshulp, de overeenkomst inzake het gebruik en de doorgifte van persoonsgegevens van passagiers (PNR), de overeenkomst inzake de verwerking en doorgifte van gegevens betreffende het financiële-berichtenverkeer ten behoeve van het programma voor het traceren van terrorismefinanciering (TFTP), evenals de overeenkomst tussen Europol en de Verenigde Staten.

– *Lacunes*

Als gevolg van de verschillende onthullingen die we hier analyseren met betrekking tot Amerikaanse programma's voor het verzamelen van inlichtingen op grote schaal is het vertrouwen dat vooral op grond van de Veiligehavenbeginselen was opgebouwd, ernstig aan het wankelen gebracht. Die onthullingen hebben het besef doen ontstaan dat de huidige bescherming van persoonsgegevens ontoereikend is en dat het noodzakelijk is om de bestaande regels, die *ernstige lacunes* vertonen, te herbekijken en te versterken.

Sinds de *FISA* werd geamendeerd en uitgebreid, meer bepaald in 2008, kunnen Amerikaanse ondernemingen er namelijk toe worden gedwongen om aan het NSA elektronische informatie over niet-Amerikanen te bezorgen. Artikel 702 van de FISA[572] vormt een algemene volmacht die het de Amerikaanse autoriteiten mogelijk maakt om gegevens te

---

570 Le programme de surveillance des Etats-Unis et leurs effets sur les droits fondamentaux des citoyens de l'UE, Nota van het Directoraat-generaal intern beleid, Beleidsondersteunende afdeling C: Rechten van de burger en constitutionele zaken, IPOL-LIBE_NT(2013)474405_FR. http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT%28 2013%29474405_FR.pdf.

571 Artikel 25 van Richtlijn 95/46.

572 Foreign Intelligence Surveillance Act van 1978 (beschrijft de procedures van fysieke en elektronische monitoring evenals het verzamelen van informatie bij vreemde mogendheden, hetzij

verzamelen en informatie te onderscheppen die betrekking heeft op de buitenlandse aangelegenheden van de Verenigde Staten, terwijl de persoonsgegevens van Amerikanen een betere bescherming genieten. De mogelijke omvang van een dergelijke bevoegdheidsoverdracht komt vandaag op duidelijke en onevenredige wijze naar voren in het licht van de onthullingen van Snowden en de technologische ontwikkelingen die de captatie van immense hoeveelheden gegevens op wereldniveau mogelijk maken.

Op 27 november 2013 publiceerde de Europese Commissie[573] het resultaat van haar overleg in (1) een strategiedocument (mededeling) over trans-Atlantische gegevensstromen waarin de problemen en risico's worden uiteengezet die voortvloeien uit de onthullingen over Amerikaanse programma's voor het verzamelen van inlichtingen, alsook de stappen die moeten worden ondernomen om deze problemen aan te pakken, (2) een analyse van de werking van 'Safe Harbor' (veilige haven) dat het doorgeven van gegevens voor commerciële doeleinden tussen de EU en de VS regelt, en (3) een verslag van over de bevindingen van de EU-VS-werkgroep (MEMO/13/1059) over gegevensbescherming, die in juli 2013 is opgericht.

Uit dit rapport blijkt ook dat grote bedrijven die actief zijn in de nieuwe technologieën en die aan de operatie *PRISM* hebben deelgenomen over een *Safe Harbor*-certificering beschikken, zodat we kunnen besluiten dat het *Safe Harbor*-systeem kan worden beschouwd als een belangrijk kanaal voor persoonsgegevens dat tot de grootschalige inzameling van gegevens door het NSA heeft geleid.

Hoewel deze praktijken door de Amerikaanse wet zijn toegelaten, zijn ze niet voorzien in het rechtskader van de *Safe Harbor*, zodat ze plaats hebben gevonden bij inbreuk op dit akkoord en op de beschikking van de Commissie die het akkoord formaliseert in het Europees rechtskader. Omdat de *Safe Harbor*-beginselen zijn vastgesteld om voor de Verenigde Staten een 'passend beschermingsniveau' te waarborgen dat borg staat voor een bescherming van persoonsgegevens op een niveau dat in de buurt komt van het beschermingsniveau binnen de EER, moeten we beschouwen dat de Verenigde Staten de geest van het akkoord in hun voordeel hebben omgebogen. Het *Safe Harbor*-systeem werd geenszins gecreëerd om de doorgifte mogelijk te maken van gegevens die vervolgens massaal aan de Amerikaanse veiligheidsautoriteiten kunnen worden bezorgd, terwijl de Europese veiligheidsautoriteiten niet op dezelfde wijze kunnen handelen.

Volgens de Europese Commissie kan de grootschalige onderschepping van persoonsgegevens door het NSA niet worden geacht te zijn gedekt door de beperking van de gegevensbescherming zoals bedoeld in het *Safe Harbor*-akkoord, met het oog op de nationale veiligheid. Als gevolg van de grootschaligheid en het feit dat er geen voorafgaande toestemming is verleend om gegevens op te slaan, kan dit proces immers niet worden beschouwd als noodzakelijk en in verhouding staand tot de belangen van de nationale veiligheid. Omdat er sprake is van een inbreuk op een fundamenteel mensenrecht, moet deze op restrictieve wijze worden beoordeeld, zoals bedoeld en beperkt door de wet.

Voorts stelt de Europese Commissie ook haar nieuwe onderzoek voor naar de bestaande akkoorden over passagiersgegevens (PNR) (MEMO/13/1054) en naar het programma voor het traceren van terrorismefinanciering (TFTP), die de uitwisseling van gegevens voor repressieve doeleinden in deze sectoren regelen.

---

rechtstreeks, hetzij door uitwisseling van informatie met andere vreemde mogendheden), zoals gewijzigd in 2008 door de FISA Amendments Act.

573 Newsroom van de Europese Commissie: http://europa.eu/rapid/press-release_MEMO-13-1059_nl.htm.

In deze mededeling geeft de Commissie meer bepaald blijk van haar wil om uiterlijk in het voorjaar van 2014 een hervorming van de gegevensbescherming in de EU goed te keuren om ervoor te zorgen dat persoonsgegevens effectief en volledig worden beschermd.

Met betrekking tot de trans-Atlantische relaties heeft de Commissie bovendien *13 aanbevelingen gedaan om de werking van de veiligehavenregeling te verbeteren*, nadat uit een op dezelfde dag bekendgemaakte analyse is gebleken dat de werking van de regeling op verscheidene punten tekortschiet. Het geheel van regels zou dus moeten worden herzien en verbeterd.

Op het vlak van de politiële en justitiële samenwerking in strafzaken zou de Commissie druk willen uitoefenen op de Amerikaanse regering opdat zij zich ertoe zou verbinden, als algemeen beginsel, gebruik te maken van een rechtskader zoals de sectorale overeenkomsten en de overeenkomsten inzake wederzijdse rechtshulp die tussen de EU en de Verenigde Staten zijn gesloten (bv. de overeenkomst over PNR en het programma voor het traceren van terrorismefinanciering) telkens wanneer de doorgifte van gegevens vereist is voor rechthandhavingsdoeleinden. Rechtstreekse verzoeken aan de ondernemingen mogen alleen mogelijk zijn in welbepaalde, uitzonderlijke en door de rechter toetsbare situaties.

Meer algemeen heeft de Europese Commissie verklaard te wensen dat de door de Amerikaanse president aangekondigde evaluatie van de activiteiten van de nationale veiligheidsautoriteiten voorziet in de bescherming van EU-burgers die hun verblijfplaats buiten de USA hebben. Die laatsten zouden dezelfde waarborgen moeten genieten als Amerikaanse burgers.

– *Globale hervorming van de regels inzake gegevensbescherming*

Zoals aangekondigd in januari 2012[574] werkt de Commissie aan een globale hervorming van de gegevensbescherming. De hervorming wil de beginselen van de gegevensbeschermingsrichtlijn van 1995 actualiseren en moderniseren om de privacyrechten te waarborgen in de toekomst. Deze hervorming omvat twee wetgevingsvoorstellen: een *verordening* tot vaststelling van het algemene EU-kader voor gegevensbescherming en een *richtlijn* inzake de bescherming van persoonsgegevens die worden verwerkt voor het voorkomen, opsporen, onderzoeken of vervolgen van strafbare feiten en aanverwante gerechtelijke activiteiten.

De hervorming beoogt meer bepaald de volgende voornaamste wijzigingen[575]:

– "*Eén stel regels inzake gegevensbescherming, geldend in de gehele EU*. Overbodige administratieve formaliteiten, zoals sommige verplichte meldingen door bedrijven, worden afgeschaft. Dit moet hen circa 2,3 miljard euro aan kosten per jaar besparen.
– Elk bedrijf is momenteel verplicht om alle maatregelen inzake gegevensbescherming aan de toezichthouders te melden, wat overbodige administratieve lasten meebrengt en bedrijven jaarlijks 130 miljoen euro kost. In plaats daarvan verplicht de verordening de verwerkers van persoonsgegevens meer verantwoording en rekenschap af te leggen.
– Zo moeten bedrijven en organisaties ernstige gegevenslekken zo snel mogelijk (zo mogelijk binnen 24 uur) aan de nationale toezichthouder melden.
– Organisaties krijgen te maken met slechts één nationale gegevensbeschermingsautoriteit, in de EU-lidstaat waar zij hun belangrijkste vestiging hebben. Insgelijks is de nationale gegevensbeschermingsautoriteit het aanspreekpunt voor burgers, ook als hun gegevens worden verwerkt door een bedrijf dat buiten de EU is gevestigd. Wanneer voor de verwerking van gegevens toestemming vereist is, moet deze uitdrukkelijk worden gegeven, en niet worden verondersteld stilzwijgend te zijn gegeven.

574 Persbericht: http://europa.eu/rapid/press-release_IP-12-46_nl.htm.
575 Persbericht: http://europa.eu/rapid/press-release_IP-12-46_nl.htm.

- Mensen zullen gemakkelijker toegang krijgen tot hun eigen gegevens en hun persoonsgegevens gemakkelijker van de ene dienstverstrekker naar de andere kunnen overdragen (recht op gegevensoverdraagbaarheid), wat de onderlinge concurrentie zal vergroten.
- Een 'recht om te worden vergeten' moet mensen in staat stellen om privacyrisico's op internet beter te beheren, d.w.z. hun gegevens te wissen als er geen gegronde redenen zijn om ze te bewaren.
- De EU-regels zijn van toepassing wanneer persoonsgegevens *buiten de EU worden verwerkt* door bedrijven die op de markt van de EU actief zijn en hun diensten aan EU-burgers aanbieden.
- Onafhankelijke nationale gegevensbeschermingsautoriteiten zullen meer bevoegdheden krijgen om de EU-regels op hun grondgebied te doen eerbiedigen, onder meer om boetes op te leggen aan bedrijven die die regels overtreden. Die boetes kunnen oplopen tot 1 miljoen euro of tot 2% van de totale jaarlijkse omzet van een bedrijf.
- In een nieuwe *richtlijn zullen grondbeginselen en algemene regels worden vastgesteld voor de bescherming van persoonsgegevens in het kader van de politiële en justitiële samenwerking in strafzaken*. De voorschriften zullen zowel op binnenlandse als grensoverschrijdende gegevensoverdrachten van toepassing zijn."

B. SOEVEREINITEIT VAN BELGIË

Het traceerprogramma waarvan sprake in deze studie steunt duidelijk op een internationale structuur waaraan zeker de Verenigde Staten (NSA) en het Verenigd Koninkrijk (*GCHQ)* deelnemen, maar wellicht nog andere Lidstaten van de Raad van Europa en de Europese Unie. Die laatste werden wellicht 'ingehaald' door de structuur waaraan ze hebben meegewerkt en zijn zelf het slachtoffer geworden van de grootschalige controleoperaties.

Laten we niet vergeten dat het UKUSA-akkoord betreffende inlichtingen inzake telecommunicatie, dat in 1947 werd gesloten door vijf Angelsaksische landen (Verenigde Staten, Verenigd Koninkrijk, Canada, Nieuw-Zeeland en Australië), het basisakkoord is voor de controle van communicatie in de ruime betekenis en al aan de basis stond van de ruggengraat van het controlesysteem Echelon, dat in de jaren 2000 voor schokgolven zorgde in Europa. De uitstekende studie van Dimitri Yernault over dit afluistersysteem is nog steeds brandend actueel en zou hier bijna volledig kunnen worden overgenomen.[576]

Een fundamentele vraag rond de grootschalige controle van elektronische communicatie zonder instemming van de Staat op wiens grondgebied de controle plaats heeft, zelfs vanaf een installatie op het grondgebied van een derde Staat, bestaat erin te weten of ze de soevereiniteit van die Staat schendt. Het antwoord is positief indien de Staat er niet mee heeft ingestemd, zelfs indien de afluisteroperaties conform zijn aan het recht van de Staat die ze uitvoert (rechtstreeks of via handelsondernemingen die er vrijwillig of gedwongen aan deelnemen): dit type afluisteroperaties schendt de soevereiniteit van de Staat op wiens grondgebied de communicaties worden onderschept.

---

576 Dimitri Yernault, De la fiction à la réalité: le programme d'espionnage électronique global "Echelon" et la responsabilité internationale des Etats au regard de la convention européenne des droits de l'homme, *RBDI,* 2000, p. 137 e.v.

Het onderscheppen van communicatie is namelijk per definitie een daad van dwang – clandestien of toegestaan door de wetgeving van de derde Staat – die wordt uitgeoefend op het grondgebied van een andere Staat en zijn soevereiniteit schendt.[577]

De Staat op wiens grondgebied de dwang wordt uitgeoefend, moet zijn voorafgaande toestemming geven.[578] Gebeurt dat niet, dan schenden de afluisteroperaties, de controle, de clandestiene onderschepping en *a fortiori* de operaties door *malware*systemen de soevereiniteit van die Staat. Aldus kan die dwang een diplomatieke reactie rechtvaardigen.

Hetzelfde geldt voor de clandestiene afluisteroperaties vanuit ambassades van derde Staten op het grondgebied van de Staat waar de afluister- en controleoperaties plaatsvinden. Ook die kunnen de goede diplomatieke relaties in gevaar brengen.

Ze vormen immers een inbreuk op het Verdrag van Wenen inzake diplomatiek verkeer van 18 april 1961, meer bepaald op artikel 3d, dat voor de diplomatieke zending [alleen] het volgende mogelijk maakt:

d) het met alle wettige middelen nagaan van de toestanden en ontwikkelingen in de ontvangende Staat en het uitbrengen van verslag daarvan aan de regering van de zendstaat;

Krachtens artikel 41.1 hebben diplomatieke zendingen de plicht "de wetten en regelingen van de ontvangende Staat te eerbiedigen. Ze hebben ook de plicht zich niet in te laten met de binnenlandse aangelegenheden van die Staat." Voor het overige mogen de gebouwen van de zending, overeenkomstig artikel 41.3, niet worden gebruikt op een wijze die onverenigbaar is met de functie van de zending, die, zoals we net hebben gezien, alleen inlichtingen mag inwinnen met behulp van wettige middelen (voornoemd artikel 3d).

Tot slot bepaalt artikel 27.1: "1. Door de ontvangende Staat wordt aan de zending toegestaan voor alle officiële doeleinden onbelemmerd verbindingen te onderhouden; deze verbindingen worden door de ontvangende Staat beschermd. Ten einde zich met de regering en met andere zendingen en consulaire posten – waar deze zich ook mogen bevinden – van de zendstaat in verbinding te stellen, mag de zending alle daarvoor in aanmerking komende middelen gebruiken, diplomatieke koeriers en codeberichten daarbij inbegrepen. De zending mag evenwel geen radiozender installeren en gebruiken zonder toestemming van de ontvangende Staat."

Het spreekt voor zich dat dit type clandestiene en ongecontroleerde onderschepping van communicatie op zich het recht op privacy schendt zoals het wordt beschermd door de voornoemde bepalingen en tot gevolg heeft dat de Staat internationaal aansprakelijk wordt, ongeacht of die Staat al dan niet lid is van de Raad van Europa of de Europese Unie. Is dat het geval, dan gaat de internationale aansprakelijkheid voor schending van de soevereiniteit van de Staat gepaard met de schending van de internationale verdragen die van toepassing zijn op het recht op eerbiediging van het privéleven.

C. OVERZICHT VAN DE ACTIEMIDDELEN TER BESCHIKKING VAN DE STAAT, BURGERS EN BEDRIJVEN

Natuurlijk is het onmogelijk, tenzij er precieze bewezen feiten aanhangig worden gemaakt die in specifieke gevallen worden aangeklaagd, om alle mogelijke rechtsmiddelen te bestu-

577 PHIJ, *Lotus case,* 7 september 1927, *Recueil,* Série A, nr. 9, p. 18.

578 Zie de werkzaamheden van het Institut de droit international, *Annuaire de droit international,* vol. 68-I, 1999; zie ook Dimitri Yernault, *op. cit.,* p. 180.

deren in een zaak met een dergelijke reikwijdte zoals die welke E. Snowden heeft aangeklaagd en waarin alle verantwoordelijken nog niet zijn aangewezen. Een van de te voeren acties zou erin kunnen bestaan te vragen dat er een parlementair onderzoek wordt gehouden om de feiten en de elementen van verantwoordelijkheid van de betrokkenen nauwkeurig vast te stellen. De Staat op wiens grondgebied structurele inbreuken op de mensenrechten worden begaan, is algemeen verplicht die te 'voorkomen' of te bestraffen.[579] Die Staat kan dus niet onverschillig blijven. In dit geval lijkt het duidelijk dat de grootschalige controle van persoonsgegevens door het NSA en/of andere spelers op het Belgisch grondgebied van structurele aard is.

In deze fase kunnen we hier alleen maar enkele pistes naar voren schuiven.

1. Internationaal Gerechtshof

De Staat kan het internationaal geschil, dit wil zeggen de internationale aansprakelijkheid van de vreemde Staat die de illegale afluisterpraktijken heeft begaan of die heeft toegestaan dat dergelijke afluisterpraktijken hebben plaatsgevonden, bijvoorbeeld door zijn grondgebied ter beschikking te stellen voor het onderscheppen en illegaal afluisteren, voor het Internationaal Gerechtshof brengen indien de zeer restrictieve voorwaarden betreffende de bevoegdheid van dit Hof vervuld zijn. De vraag betreffende de naleving van het Verdrag van Wenen inzake diplomatiek verkeer en consulaire betrekkingen kan bij hetzelfde Hof aanhangig worden gemaakt.

2. Europees Hof voor de Rechten van de Mens[580]

Indien de Staat die aansprakelijk is voor de controle of eraan heeft meegewerkt lid is van de Raad van Europa, dan is een transnationaal beroep voor het Europees Hof voor de Rechten van de Mens een rechtsmiddel om de schendingen te doen ophouden en schadevergoeding te verkrijgen. Een dergelijk beroep werd ernstig overwogen in de zogenaamde zaak 'Echelon'.[581] Indien in deze zaak het bewijs zou worden geleverd van interventies van de geheime diensten van het Verenigd Koninkrijk of andere Staten die het EVRM hebben ondertekend, dan zou het om een exemplarische actie gaan.

3. Belgische gerechten: hacking en strafbare feiten

– Belgische bedrijven die het slachtoffer zijn van illegale onderschepping van gegevens in hun bezit kunnen – naargelang de feiten – klacht indienen tegen de vreemde Staat voor de gerechten van de betrokken Staat, maar ook voor de Belgische gerechten indien bewezen is dat de feiten een verband hebben met België (onderschepping in België). Zo kan de malware die het informaticasysteem van Belgacom lijkt te hebben besmet, het voorwerp zijn van een rechtsvordering in België. Een nauwkeuriger uiteenzetting van de feiten is echter noodzakelijk om een juridische studie aan deze mogelijkheid te wijden.

---

579 Zie meer bepaald Dimitri Yernault, op. cit., p. 214.

580 Dit beroep lijkt efficiënter dan een beroep voor het Mensenrechtencomité, maar deze mogelijkheid mag niet worden uitgesloten.

581 Zie Dimitri Yernault, *op. cit.,* p. 154 e.v.

- In de mate waarin specifieke bepalingen betreffende de bescherming van persoonsgegevens daarin voorzien, kunnen ze natuurlijk van toepassing zijn op private personen zodra die verantwoordelijk zijn voor de verwerking van persoonsgegevens in de betekenis van de hierboven bestudeerde bepalingen. Dit is meer bepaald het geval met de richtlijnen die ook bestemd zijn voor de aanbieders van netwerken, telecommunicatiediensten enzovoort; dit moet natuurlijk verder worden uitgeklaard in elk afzonderlijk geval. Voor Facebook bijvoorbeeld werd er een grondige studie gevoerd.[582] Dit zou moeten gebeuren voor elke potentiële verantwoordelijke wiens rol zou kunnen worden bepaald in de zaak die ons bezighoudt.
- Volgens de vaststelling van de feiten, indien bewezen was dat private bedrijven buiten medeweten van de Staat hebben meegewerkt aan de uitvoering van de onderscheppingspraktijken (bv. op de optische kabel in Oostende of door vrijwillig persoonsgegevens door te geven aan een vreemde Staat (NSA of ander)), dan kunnen de Staat of particulieren of bedrijven die het slachtoffer zijn van deze hacking een strafrechtelijke klacht indienen krachtens de wet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens, meer bepaald op grond van artikelen 550*bis* en 314*bis* van het Strafwetboek en van de artikelen 124 en 145 van de wet van 13 juni 2005 betreffende de elektronische communicatie. Hacking wordt immers strafrechtelijk bestraft.[583]

Titel IXbis van het Belgisch Strafwetboek heeft als titel "Misdrijven tegen de vertrouwelijkheid, integriteit en beschikbaarheid van informaticasystemen en van de gegevens die door middel daarvan worden opgeslagen, verwerkt of overgedragen". Artikelen 550*bis* en 550*ter* bestraffen diverse gedragingen met straffen die gaan van 3 maanden tot 5 jaar opsluiting. De Belgische strafwet verbiedt het feit "zich toegang te verschaffen tot een informaticasysteem" of "zich daarin te handhaven" (artikel 550*bis*, § 1, 1ste lid), maar ook "om enig gebruik te maken van een informaticasysteem van een derde" (artikel 550*bis*,§ 3, 2°) of "enige schade aan dit systeem te veroorzaken" (artikel 550*bis*, § 1, 3°). De wet bestraft "hij die opdracht geeft of aanzet tot het plegen van een van de misdrijven bedoeld in §§ 1 tot 5" (artikel 550*bis*, § 6) en "hij die, terwijl hij weet dat gegevens bekomen zijn door het plegen van een van de misdrijven bedoeld in §§ 1 tot 3, deze gegevens onder zich houdt, aan een andere persoon onthult of verspreidt, of er enig gebruik van maakt" met gevangenisstraf van zes maanden tot drie jaar en/of met geldboete van 26 tot 100.000 euro (artikel 550*bis,* § 7).

Titel V van het Belgisch Strafwetboek ("Misdaden en wanbedrijven tegen de openbare orde door bijzondere personen gepleegd") bevat een hoofdstuk VII*bis* met als titel "Misdrijven betreffende het geheim van privé-communicatie en -telecommunicatie". Artikel 314*bis,* § 1 bestraft met gevangenisstraf van zes maanden tot één jaar en/of honderd tot tienduizend euro hij die "privé-communicatie", "waaraan hij niet deelneemt", "tijdens de overbrenging ervan", […], "er kennis van neemt", "opneemt", "zonder de toestemming van alle deelnemers aan die communicatie of telecommunicatie" of die daartoe "enig toestel opstelt of doet opstellen". Artikel 314*bis,* § 2 bestraft met gevangenisstraf van zes maanden

582 Jean-Philippe Moiny, Facebook au regard des règles européennes concernant la protection des données, *Rev. Eur.de droit de la consommation,* p. 235.

583 De Belgische wetgeving strekt in dit verband tot voorbeeld.

tot twee jaar en/of met geldboete van vijfhonderd tot twintigduizend euro hij die "een op die manier verkregen inlichting" "onthult, verspreidt of er wetens enig gebruik van maakt".

Personen en bedrijven die het slachtoffer van deze misdrijven zijn geweest, kunnen in België een strafrechtelijke klacht indienen bij de procureur des Konings of zich burgerlijke partij stellen. De vraag naar de territoriale bevoegdheid om een dergelijke klacht te kunnen indienen wordt opgelost in functie van de feiten van de zaak. Ofwel werd het misdrijf in België gepleegd (bv. onwettige toegang tot een informaticasysteem in België), ofwel hebben de gevolgen van de misdaad zich voorgedaan in België (indien jurisprudentie van het Hof van Cassatie ter gelegenheid van een zaak met betrekking tot een cheque die in Teheran werd uitgegeven en op een Belgische bank werd getrokken, op cybercrime wordt toegepast[584]).

Dit gezegd zijnde, in het Belgisch recht kunnen deze feiten van hacking wettelijk zijn indien ze, overeenkomstig de bepalingen van het Wetboek van Strafvordering betreffende de opslag van informaticagegevens, worden begaan met behulp van het procedé van de zoeking in een informaticasysteem en de uitbreiding van die zoeking, bevolen door de onderzoeksrechter bij gemotiveerde beschikking, "naar een informaticasysteem dat zich op een andere plaats bevindt" (artikel 88*ter* van het Wetboek van Strafvordering) en door het bevel dat dezelfde magistraat geeft aan een persoon die "bijzondere kennis" heeft om toegang te verkrijgen tot gegevens die zijn opgeslagen "in een verstaanbare vorm" (artikel *88quater* van het Wetboek van Strafvordering). Deze onderzoeksmaatregel kan ook onder strenge voorwaarden plaatsvinden als "uitzonderlijke methode voor het verzamelen van gegevens" door de Veiligheid van de Staat of de Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht (artikel 18/16, §§ 1 tot 5 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst).

Hacking of het gebruik van gegevens die in België zijn verzameld of gebruikt, zonder wettelijke toelating, blijft een strafbaar feit. Het Belgisch Wetboek van Strafvordering bevat in artikel 29 voor elke ambtenaar die kennis krijgt van een misdrijf de verplichting om die te melden aan de procureur des Konings. Het gaat om een algemene verplichting die betrekking heeft op eender welk misdrijf.[585]

4. Gebruik van de informatie verkregen door een onwettig controlesysteem

De vraag stelt zich of een politie- of inlichtingendienst die dit soort informatie ontvangt, die informatie mag gebruiken in het kader van zijn opdrachten. *De wet betreffende de bijzondere methoden voor het verzamelen van gegevens bepaalt dat indien een uitzonderlijke maatregel* voor het verzamelen van gegevens, zoals hacking, op onwettige wijze heeft plaatsgevonden, de commissie die belast is met het toezicht op de specifieke en uitzonderlijke methoden voor het verzamelen van gegevens van de inlichtingen- en veiligheidsdiensten die gegevens bewaart en de inlichtingen- en veiligheidsdiensten verbiedt die gegevens te exploiteren (artikel 18/10, § 6, lid 4 van de wet van 30 november 1998 houdende regeling van de inlichtingen- en veiligheidsdienst). Op te merken valt dat geen enkele bepaling de gevolgen reglementeert

584 Correctionele rechtbank, Dendermonde, 29 september 2008, *Tijdschrift voor Strafrecht,* 2009/2, 111-114.

585 Alain Winants, De Veiligheid van de Staat en de BIM-Wet, in Wauter Van Laethem, Dirk Van Daele en Bart Vangeebergen(Eds), *De Wet op de bijzondere inlichtingenmethoden,* Intersentia, Antwerpen Oxford, p. 141.

die moeten worden gegeven in het geval waarin deze onwettigheid door een buitenlandse dienst werd begaan. Een mogelijke oplossing kan worden gevonden in de besprekingen die zijn voorafgegaan aan de goedkeuring van de wet van 4 februari 2010 betreffende de bijzondere methoden voor het verzamelen van inlichtingen. De wet van 1998 betreffende de inlichtingendiensten verwijst in artikel 20, § 1 immers naar de samenwerking met buitenlandse diensten. De voorzitter van het Vast Comité I heeft echter aangegeven dat "het Comité geen toezicht kan uitoefenen op de buitenlandse inlichtingendiensten. Het zou aangewezen zijn om de wet op dit punt aan te vullen zodat de wettelijkheid van de operaties van bevriende buitenlandse inlichtingendiensten, die op ons grondgebied worden toegelaten, eveneens kan worden gecontroleerd door de Veiligheid van de Staat."[586] De heer Winants heeft bij deze gelegenheid verklaard: "Indien een buitenlandse inlichtingendienst zijn bevoegdheden te buiten gaat, dan geniet de Veiligheid van de Staat de mogelijkheid om tussen te komen op grond van voornoemd artikel 20 van de wet van 1998)."[587] De heer Hellemans, directeur van de ADIV, verklaarde van zijn kant: "De ADIV gaat uit van het principe dat het stelselmatig door de buitenlandse diensten op de hoogte wordt gebracht wanneer die diensten een doel nastreven in België. De dienst onderhoudt goede contacten met de bevriende landen en maakt gebruik van een systeem voor gegevensuitwisseling. Natuurlijk blijft de dienst aansprakelijk voor de gegevens die op het Belgisch grondgebied worden verzameld."[588]

Uit dit alles blijkt ten eerste dat het aanwenden door een buitenlandse dienst van een uitzonderlijke methode voor het verzamelen van gegevens in België, zoals hacking, niet gereglementeerd is, ten tweede dat deze methode om inlichtingen te verzamelen een strafbaar feit vormt en ten derde dat het voor de Belgische diensten verboden is om op onwettige wijze verkregen inlichtingen te gebruiken, zo niet zouden de Belgische diensten zich eveneens schuldig maken aan het plegen van een misdrijf als ze dit wetens en willens doen.

De problematiek van de samenwerking met buitenlandse diensten en de manier om daarop toezicht uit te oefenen is een van de prioriteiten van het Vast Comité I. Al in het activiteitenverslag van 2008 bracht het Comité verslag uit over verschillende bijdragen in het buitenland teneinde een doeltreffende democratische controle op de inlichtingendiensten te bevorderen en deze initiatieven krijgen de steun van Martin Scheinin, Speciaal Rapporteur van de Verenigde Naties voor bevordering en bescherming van de mensenrechten en de fundamentele vrijheden in de strijd tegen het terrorisme.[589] De uitwisseling van informatie met 'bevriende' diensten is momenteel slechts onderworpen aan ethische beginselen. Deze lacune in de wetten betreffende het toezicht op de inlichtingendiensten werd bekritiseerd en er werd voorgesteld dat nieuwe regelgeving dit juridisch vacuüm zou opvullen.[590]

De kwestie betreffende het gerechtelijk gebruik van dit soort informatie krijgt een andere oplossing. Het Belgisch strafprocesrecht voorziet immers in een regel die onwettig verkregen bewijselementen uitsluit. Deze uitsluiting is echter niet absoluut. De wet van

---

586 *Parl. st.,* Kamer, 52ste zittingsperiode, 2009-2010, DOC 52 / 2128/000, p. 41.

587 *Ibid.*

588 *O.c.,* p. 46.

589 Vast Comité I, Activiteitenverslag 2008, p. 87.

590 Oor een grondige studie hierover, zie o.a. Elizabeth Sepper, Democracy, Human Rights and Intelligence Sharing, *Texas International Law Journal,* Vol. 46: 151, 2010, pp. 153-206; Europees parlement, Comité burgerlijke vrijheden, justitie en binnenlandse zaken, *Working Document 5 on Democratic oversight of Member State intelligence services and of EU intelligence bodies,* 11 november 2013, DT\1009342EN.doc.

24 oktober 2013 heeft in het Wetboek van Strafvordering immers een nieuw artikel 32 ingevoegd, dat als volgt luidt:

> "Art. 32. Tot nietigheid van onregelmatig verkregen bewijselement wordt enkel besloten indien:
> – *de naleving van de betrokken vormvoorwaarden wordt voorgeschreven op straffe van nietigheid, of;*
> – *de begane onregelmatigheid de betrouwbaarheid van het bewijs heeft aangetast, of;*
> – *het gebruik van het bewijs in strijd is met het recht op een eerlijk proces."*

Deze wet geeft gevolg aan de zogenaamde arrest-'Antigone' van 14 oktober 2003 van het Belgisch Hof van Cassatie .[591] Deze rechtspraak had al aanleiding gegeven tot de wet van 9 december 2004 betreffende de wederzijdse internationale rechtshulp in strafzaken en tot wijziging van artikel 90*ter* van het Wetboek van strafvordering, die in artikel 13 bepaalt:

> "Art. 13. In het kader van een in België gevoerde strafrechtspleging mag geen gebruik worden gemaakt van bewijsmateriaal:
> *1° dat in het buitenland op onregelmatige wijze is verzameld indien de onregelmatigheid:*
> – *volgens het recht van de Staat waarin het bewijsmateriaal is verzameld volgt uit de overtreding van een op straffe van nietigheid voorgeschreven vormvereiste;*
> – *de betrouwbaarheid van het bewijsmateriaal aantast;*
> *2° waarvan de aanwending een schending inhoudt van het recht op een eerlijk proces."*

Deze reglementering van het bewijs impliceert dus dat eender welke onwettigheid of onregelmatigheid er niet automatisch toe leidt dat dit bewijselement terzijde wordt geschoven. In een belangrijk boek[592] heeft de voorzitter van de strafkamer van het Belgische Hof van Cassatie echter verklaard dat er, naast de nietigheden waarin een wettekst specifiek voorziet of die welke de betrouwbaarheid van het bewijsmateriaal aantasten of waarvan het gebruik het recht op een eerlijk proces schendt, ook nietigheden bestaan als gevolg van onrechtmatig verkregen bewijs, dit wil zeggen het geval waarin het bewijsmateriaal is aangetast door het plegen van een misdrijf.[593] Ter gelegenheid van een studie naar de rechtspraak in deze materie maakt deze eminente magistraat, met betrekking tot misdrijven gepleegd door onderzoeksorganen, een onderscheid tussen enerzijds de situatie van een misdrijf dat wordt begaan om een bewijs te verkrijgen en anderzijds de situatie van een misdrijf dat al is gepleegd op het ogenblik waarop de vaststelling wordt gemaakt van een door een delinquent gepleegd misdrijf.[594] In het eerste geval, bijvoorbeeld onwettige hacking, is het bewijs niet ontvankelijk. In het tweede geval, bijvoorbeeld de deelname aan de handel in verdovende middelen teneinde de daders aan te houden, "zou het bewijs ontvankelijk zijn wanneer het misdadig voornemen duidelijk voorafgaat aan de interventie van de politie en de verbaliserende overheid slechts onregelmatigheden begaat die extern zijn aan de beslagleggingen, zoekingen, observaties en verhoren" (vrije vertaling).[595]

---

591 AR P.03.0762.N.
592 Jean de CODT, *Des nullités de l'instruction et du jugement,* Brussel, Larcier, 2006, 233 pp.
593 *O.c.,* p. 16.
594 *O.c.,* p. 103-104.
595 *O.c.,* p. 105.