ACTIVITY REPORT 2014
ACTIVITY REPORT 2015

ACTIVITY REPORT 2014
ACTIVITY REPORT 2015

Review Investigations, Control of Special Intelligence Methods and Recommendations

Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee

intersentia

Cambridge – Antwerp – Portland

The Dutch and French language versions of this report are the official versions. In case of conflict between the Dutch and French language versions and the English language version, the meaning of the first ones shall prevail.

Activity Report 2014. Activity Report 2015. Review Investigations, Control of Special Intelligence Methods and Recommendations
Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee
Rue de Louvain 48, 1000 Brussels – Belgium
+ 32 (0)2 286 29 11
info@comiteri.be
www.comiteri.be

Cambridge – Antwerp – Portland
www.intersentia.com

ISBN 978-1-78068-439-0
D/2017/7849/45
NUR 823

CONTENTS

LIST OF ABBREVIATIONS

ATG	Mixed Anti-Terrorism Group
BCC	Belgian Criminal Code
BCCP	Belgian Code of Criminal Procedure
BICS	Belgacom International Carrier Services
BNG/ANG	Belgian National General Database
BOJ	Belgian Official Journal
BSS	British Security Service (MI5)
CCB	Centre for Cybersecurity Belgium (Centrum voor Cybersecurity België – Centre pour la cybersécurité Belgique)
CGI	Department for International Police Cooperation
CIA	Central Intelligence Agency
CIP	Central Information Point
COC	Control Agency for Management of Police Information (Controle Orgaan voor het Beheer van de Politionele Informatie – Organe de Contrôle de la Gestion de l'Information Policière)
CUTA	Coordination Unit for Threat Assessment
Data Protection Act	Act of 8 December 1992 on privacy protection in relation to the processing of personal data (Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens – Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel)
ECHR	European Court of Human Rights
EU	European Union
FTF	Foreign Terrorist Fighters
GCCR	Governmental Coordination and Crisis Centre
GCHQ	Government Communications Headquarters
GIA	Armed Islamic Group
GISS	General Intelligence and Security Service of the Armed Forces (Algemene Dienst inlichting en veiligheid van de Krijgsmacht – Service général du renseignement et de la sécurité des Forces armées)
HUMINT	Human Intelligence

ICT	Information and Communication Technology
IMINT	Image Intelligence
Intelligence Services Act	Act of 30 November 1998 governing the intelligence and security services (Wet houdende regeling van de inlichtingen- en veiligheidsdienst – Loi organique des services de renseignement et de sécurité)
IO	Immigration Office
IS	Islamic State
ISIL	Islamic State in Iraq and the Levant
ISIS	Islamic State in Iraq and Syria
JIB	Joint Information Box
NBB	National Bank of Belgium
NSA	US National Security Agency
NSC	National Security Council
NTF	National Task Force
OSINT	Open Source Intelligence
Parl. doc	Parliamentary Document
RD	Royal Decree
Review Act	Act of 18 July 1991 governing the review of police and intelligence services and of the Coordination Unit for Threat Assessment (Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse – Loi organique du contrôle des services de police et de renseignement et de l'organe de coordination pour l'analyse de la menace)
SEP	Scientific and Economic Potential
SIGINT	Signals Intelligence
SIM	Special Intelligence Methods
SIM Act	Act of 4 February 2010 governing the intelligence collection methods used by the intelligence and security services (Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten – Loi relative aux méthodes de recueil de données par les services de renseignement et de sécurité)
SIM Commission	Administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services
SIS	British Secret Intelligence Service (MI6)

SOCMINT	Social Media Intelligence
Standing Committee I	Standing Intelligence Agencies Review Committee (Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – Comité permanent de contrôle des services de renseignement et de sécurité)
Standing Committee P	Standing Police Monitoring Committee (Vast Comité van Toezicht op de politiediensten – Comité permanent de contrôle des services de police)
State Security	State Security (Veiligheid van de Staat – Sûreté de l'État)
Threat Assessment Act	Act of 10 July 2006 on Threat Assessment (Wet betreffende de analyse van de dreiging – Loi relative à l'analyse de la menace)
TSA	US Transportation Security Agency
UN	United Nations
VPN	Virtual Private Network

INTRODUCTION

The Belgian Standing Intelligence Agencies Review Committee (hereafter Standing Committee I) is a permanent and independent review body. It was set up by the Review Act of 18 July 1991 and has been operational since May 1993.[1]

The Standing Committee I is responsible for reviewing the activities and functioning of the two Belgian intelligence services: the civil intelligence service, State Security, and his military counterpart, the General Intelligence and Security Service. In addition, it supervises, together with the Standing Committee P, the functioning of the Coordination Unit for Threat Assessments[2] and his various supporting services.

The review relates to the legitimacy (supervision of observance of the applicable laws and regulations), effectiveness (supervision of the efficiency of the intelligence services), and coordination (the mutual harmonisation of the work of the services concerned). With regard to the supporting services of the Coordination Unit for Threat Assessments, the review only relates to their obligation to pass on information on terrorism and extremism.

The Standing Committee I performs its review role through investigations carried out on its own initiative or on the request of the Parliament or the competent minister or authority. Additionally, the Standing Committee I can act on request of a citizen and of any person holding a civil service position, as well as any member of the armed forces, who has been directly concerned by the intervention of one of the intelligence services.

Since 1 September 2010, the Standing Committee I has been acting also as a judicial body in the control of the special intelligence methods used by the intelligence and security services. The so-called SIM Act of 4 February 2010 has provided the two Belgian intelligence services with an extensive additional arsenal of special (specific or exceptional) powers. However, they come under the judicial control of the Standing Committee I.

The Standing Committee I and its Investigation Service have many powers. For example, the reviewed and controlled services must send, on their own initiative, all documents governing the conduct of the members of the service, and the Committee can request any other text or document. The fact that many

1 The Standing Committee I celebrated its 20th anniversary in 2013 (Van Laethem, W. and Vanderborght, J., *Inzicht in toezicht – Regards sur le contrôle*, Antwerpen, Intersentia, 2012, xxx + 265 p.).

2 Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight Against Terrorism – Fusion Centres throughout Europe*, 2010, 220 p.

documents of the intelligence services are classified in accordance with the Classification Act of 11 December 1998, does not detract from this. Indeed, all employees of the Committee hold a security clearance of the "top secret" level. The Committee can also question anybody. The members of the reviewed services can be summoned if necessary and required to testify under oath. Furthermore, the supervisory body can make all useful findings and seize all objects and documents in any location. Finally, the Committee can demand the assistance of experts and interpreters, and the assistance of the police.

The Standing Committee I is a collective body and is composed of three members, including a chairman. The incumbent members are appointed or renewed by the Chamber of Representatives.[3] The Standing Committee I is assisted by a secretary and his administrative staff, and by an Investigation Service.

Pursuant to Article 35 of the Review Act of 18 July 1991, the Standing Committee I annually draws up a general activity report. These activity reports are drawn up in Belgium's national languages Dutch and French and can be found on the website of the Committee (see www.comiteri.be). With increased globalisation in mind, the Standing Committee I wishes to meet the expectations of a broader public. The sections of the activity reports 2014 and 2015 that are most relevant to the international intelligence community (the review investigations, the control of special intelligence methods, the recommendations and the table of contents of the complete activity reports), have therefore been translated into English. This book is the fifth to be published in English by the Standing Committee I, after the *Activity Report 2006-2007*, the *Activity Report 2008-2009*, the *Activity Report 2010-2011* and the *Activity Report 2012-2013* (see www.comiteri.be).

Guy Rapaille, Chairman
Gérald Vande Walle, Counsellor
Pieter-Alexander De Brock, Counsellor
Wouter De Ridder, Secretary

1 December 2016

3 A committee responsible for monitoring the Standing Committee P and the Standing Committee I has been created and is composed of 13 MPs.

ACTIVITY REPORT 2014

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2014

Appendices

PREFACE – ACTIVITY REPORT 2014

A shooting at the head office of the French satirical weekly magazine 'Charlie Hebdo' in early January 2015 claimed the lives of twelve victims. A hostage situation, which developed almost simultaneously in a Jewish supermarket in the east of Paris, resulted in a further five deaths. Just a few days later, there was a large coordinated anti-terror operation in Belgium with house raids in various places. Two fighters returning from Syria were killed and a third was wounded during a gunfight in Verviers. These three men had been under surveillance by the intelligence services for some time.

Reactions were not long in coming. The Inner Cabinet compiled a list of twelve measures in the fight against terrorism and radicalism. The use of the army for surveillance operations was probably the most striking measure.

A number of these measures have a direct impact on the operations of the Belgian intelligence and security services: the Foreign Fighters Circular of September 2014 will be adapted, the Radicalism Action Plan (which dates back to 2005) must be updated, a National Security Council is being established, and the special protection assignments that are currently performed by State Security will be transferred to the Federal Police.

The Standing Committee I did not wait for the events in Paris and Verviers to unfold. It already conducted a number of investigations in 2014 that are relevant to these government decisions and that can certainly be useful in the implementation of the proposed measures.

At the start of 2014, for example, an investigation into State Security and its statutory close protection assignments was completed, the results of which may prove their worth in the debate on transferring these assignments from State Security to the Federal Police.

The current investigation into the monitoring of extremist elements in the army was also expanded last year with information about the Syria issue. An investigation into how the Coordination Unit for Threat Assessment (CUTA) manages, assesses and disseminates the information contained in the Joint Information Box (JIB), in accordance with the implementation of the Radicalism Action Plan, was also finalised.

The Standing Committee I opened a further investigation in 2014 into cooperation between State Security and the prison administration. More specifically, the Standing Committee I wishes to verify whether the enhanced exchange of information, as decided on in a protocol, is actually happening.

And, lastly, the issue of foreign fighters and their contingent in Syria could obviously not be overlooked. The Standing Committee I started an investigation into the information position of the General Intelligence and Security Service (GISS) and State Security relating to the recruitment, mission, stay and return of young people who are leaving or who have left to Syria or Iraq.

The Standing Committee I is convinced that these investigations will lead to substantiated recommendations to support the further implementation of the measures required in the fight against radicalism and terrorism, while ensuring the protection of fundamental human rights.

As regards the protection of human rights, the Standing Committee I also worked closely in 2014 with the Committee on Civil Liberties, Justice and Home Affairs (LIBE) of the European Parliament, including with a view to finalising a Resolution in response to the Snowden revelations.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2015

CHAPTER II
REVIEW INVESTIGATIONS 2014

Nine investigations were completed in 2014, as was the case in 2013. Two investigations were held at the request of the Monitoring Committee, five were started after a complaint or report, and two were initiated on its own initiative. One investigation was conducted jointly with the Standing Police Monitoring Committee.[4] The nine final reports (II.1 to II.9) will be discussed in brief below.

This will be followed by a summary and brief description of the investigations that are still ongoing (II.10). The five investigations opened in 2014 are also referred to in this latter section. Three of these five new investigations were started following a complaint, while two were started at the Committee's own initiative.

The Committee received a total of 31 complaints or reports in 2014. After verifying some objective information, the Committee rejected 28 of these complaints or reports because they were manifestly unfounded (Article 34 of the Review Act) or because the Committee did not have jurisdiction for the matter in question. In the latter cases, the complainants were referred, wherever possible, to the competent authority. In some cases, the police or judicial authorities were also notified because of a potential risk. As stated, three complaints from 2014 resulted in an investigation being opened.

II.1. THE SNOWDEN REVELATIONS AND THE INFORMATION POSITION OF THE BELGIAN INTELLIGENCE SERVICES

II.1.1. INTRODUCTION

On 6 June 2013, *The Guardian*[5] and *The Washington Post*[6] first published information from tens of thousands of (classified) documents that had been

4 Summaries of joint investigations included in this Activity Report have been drawn up solely under the auspices of the Standing Committee I, not both Committees.

5 G. GREENWALD and E. MACASKILL, *The Guardian*, 6 June 2013 (NSA Taps in to Internet Giant's Systems to Mine User Data, Secret *files* Reveals).

6 B. GELLMAN and L. POITRAS, *The Washington Post*, 6 June 2013 (US Intelligence Mining Data from Nine US Internet Companies in Broad Secret Program).

leaked by Edward Snowden, who held various positions in or for American intelligence services. New revelations have followed another since.

The reports gave an insight into secret programmes of mainly the US National Security Agency (NSA) and the UK General Communications Headquarters (GCHQ). Among other things, they revealed the existence of the PRISM programme used by the NSA to obtain telecommunication (meta)data and brought to light that both American and British services had set up intelligence operations in relation to a number of international institutions and alliances (UN, EU and G20) in which 'friendly countries' were also targeted.

These revelations resulted in many parliamentary, judicial and intelligence investigations throughout the world, including Belgium. On 1 July 2013, the Monitoring Committee of the Senate requested the Standing Committee I for "*[…] an update of the existing information on data mining practices. […] Secondly, the Monitoring Committee wishes the Standing Committee I to investigate the consequences for the protection of the country's economic and scientific potential, and for the legal assignments of our intelligence services. Lastly, the Monitoring Committee wishes the Standing Committee I to investigate how such practices are assessed in relation to the national and international rules that protect the privacy of citizens.*" (free translation).

Thereupon the Standing Committee I opened three investigations[7] that are obviously closely connected with each other. This also applies to a fourth investigation[8] that was initiated following a complaint from the Chairman of the Flemish Bar at the Brussels Bar.

The first investigation reported on here provides an answer to the following questions:

- what capacity do major powers such as the United States and the United Kingdom possess for the large-scale interception and exploitation of data of people, organisations, companies or institutions based in Belgium (or that have any link to Belgium) and which data is involved (both quantitatively and qualitatively)?
- to what extent were the Belgian intelligence services aware of the capacity of these major powers (or to what extent should have they been aware thereof in view of their legal assignments)? Was intelligence collected in this regard or

7 In addition to this investigation, another was opened into the national and international rules applicable in Belgium to the protection of privacy in relation to massive data capturing (see Chapter II.2) and into the possible implications of data mining on the protection of the country's scientific and economic potential (see Chapter II.10.7).

8 Investigation following a complaint by the Chairman of a Bar into the use of information originating from massive data capturing in Belgian criminal cases. See Chapter II.3 in this regard: 'Use in criminal cases of information originating from massive data capturing by foreign services'.

was this not deemed appropriate? Do our services provide adequate protection in this regard?
– what is the significance/value of the concept of 'friendly state' in the context of intelligence services and to what extent does that concept determine the attitude of our own intelligence services?

In the first phase of the investigation, the Standing Committee I wished to obtain the most accurate picture possible, on the basis of open sources, of the massive data capturing by specific States and how these States engage in political espionage at 'friendly services'.[9]

Information that was already available within the Committee was analysed and processed at the same time. National and international media reports were also meticulously registered. Lastly, parliamentary questions and answers, national and foreign academic analyses, online discussion platforms, etc. were consulted.

Various interviews took place as well. For example, contact was made in mid-October 2013 between the Standing Committee I and Laura Poitras (one of the journalists who received documents from Edward Snowden) and Jacob Appelbaum (research journalist and software developer). This meeting produced some interesting insights. An attempt was also made to interview the NSA delegation that was visiting Belgium as part of the ad hoc EU-US Working Group on Data Protection. The delegation advised that it did not have a mandate to talk to the Standing Committee I.

In the second phase, the intelligence services were asked to answer a number of targeted questions and send the Committee a number of documents relating to the relevant theme. Extensive briefings[10] have since been organised and additional documents requested. Lastly, State Security management and staff of GISS were sounded out on adopted and future policies.

The fact that both services were appointed as an expert in the judicial inquiry into the hacking of the Belgacom/BICS network did not form an obstacle in this investigation: the services were able to share all information that was deemed useful and necessary for the investigation with the Committee.[11]

---

9 This part of the investigation was outsourced to *drs.* Mathias Vermeulen, Research Fellow at the European University Institute (EUI) in Florence and the Centre for Law, Science and Technology Studies at VU Brussel, who was appointed as an expert. His work resulted in the study '*De Snowden-revelaties, massale data-captatie en politieke spionage*' (the Snowden revelations, massive data capturing and political espionage (free translation)), which was included in its entirety as Appendix D to the *Activity Report 2013* (p. 132–184) of the Standing Committee I.

10 The Committee had no less than four briefings with GISS, whose personnel proving to be very open and professional.

11 The investigation resulted in an lengthy report for the competent ministers. Certain sections of the report were classified as 'TOP SECRET Act 11/12/1998' with regard to GISS and as 'SECRET Act 11/12/1998' with regard to State Security. The report was submitted for advice to the services involved. Their comments were studied and amendments were made to the

II.1.2. THE SNOWDEN REVELATIONS IN CONTEXT

Ever since the first leaked NSA slides, there has been a continuous stream of new and extremely sensitive information pointing to massive data capturing and political and economic espionage of and on friendly countries. It quickly became clear that the problem was not limited to PRISM, TEMPORA or spying on the G20 as initially thought.[12]

The Standing Committee I emphasised that it did not find any substantiated indications that would show the Snowden slides are not authentic. On the contrary, the Committee was led to conclude from the investigations that the revelations, particularly the existence of massive data capturing and economic and political espionage by friendly services, were truthful 'in broad terms'.[13] The fact that there was no certainty regarding the interpretation given to the slides – partly because of the fragmented nature of the revelations[14] – does not alter this finding. However, this does not mean that caution in interpretation is not required. It was initially assumed, for instance, that the NSA had eavesdropped on millions of conversations in Norway and the Netherlands. It ultimately transpired that this related to telecommunications that the Norwegian and Dutch intelligence services had intercepted themselves abroad in the context of military operations. However, data had unreservedly been shared with the NSA.

The Snowden revelations will be placed in a broader context below.

II.1.2.1. Not only the NSA and GCHQ

The investigation focused solely on massive data capturing by the US National Security Agency (NSA) and the UK General Communications Headquarters (GCHQ). Other services in these countries may have been involved in massive data capturing. And obviously, the United States and the United Kingdom are not the only major powers operating in this way.

The activities of the French, German and Swedish intelligence services, for example, were also discussed in the margin of the Snowden revelations. Not to mention, of course, the capacities that can be developed by countries such as Russia and China. But perhaps just as important in this context are the *Signals*

---

text. Based on the classified report, a 'Restricted' report was drawn up for the principal. This public report contains the most important information from the 'Restricted' report.

12 One example of this is the Boundless Informant Head Map of March 2013, published in G. GREENWALD and E. MACASKILL, *The Guardian*, 11 June 2013 (Boundless Informant: the NSA's secret tool to track global surveillance data).

13 The fact that neither the American nor the British authorities have disputed the authenticity of the leaked documents to date must also be taken into account. At most, the interpretation given to them in some open sources has been contested.

14 *The Guardian* has purportedly published only one per cent of all the documents it received from Snowden (X, *De Standaard*, 3 December 2013 (*Amper 1 procent van informatie Snowden gepubliceerd* – Barely 1% of Snowden information published)).

Intelligence (SIGINT) alliances that exist between certain countries. The best known of these is FIVE EYES, which in addition to the United States and the United Kingdom, includes Canada, Australia and New Zealand. These countries have worked very closely together for decades and captured data communication is assumed to be exchanged almost without restriction. The press has also reported on NINE EYES and FOURTEEN EYES, for example, which open sources allege include Belgium among their members.[15]

Lastly, massive data capturing and exploitation are not the exclusive domain of the government. Major private players sometimes have similar capacities, even though the purpose of their activities usually differs. The Committee has evidently not studied this issue as it lies outside its jurisdiction.

II.1.2.2. Not only PRISM and TEMPORA

The first revelations related mainly to PRISM (as regards the Americans) and TEMPORA (as regards the British). Both intelligence programmes were revealed as a very important source of information, but were certainly not the only ones. The Committee has distinguished among five forms or techniques of massive data capturing or 'unfocused interception' of telecommunications and other forms of communication somewhat schematically (infra).

II.1.2.2.1. Unfocused and massive

The Committee's review investigation was limited to intelligence programmes or techniques that essentially amount to 'unfocused' capturing (also known as fishing expeditions), by which a gigantic fine-mesh net is proverbially cast out and it is only determined afterwards, manually or with the use of automated processes, what is potentially relevant and useful.[16] Accordingly, this does *not* involve eavesdropping on the telephone communications of one individual or institution (even though that too may include significant amounts of sensitive data). A purer form of 'unfocused' capturing, for example, is intercepting and storing *all* information that passes through an international internet cable and then digitally performing searches (data mining). Another example is capturing all mobile telephone signals in a certain region.

However, not all techniques described by the Snowden files are necessarily indicative of 'massive' capturing. For example, when capturing data from fibre optic cables, selectors are normally used, such as a mobile telephone number, an IP address or a specific word (e.g. 'attack'). While it is true that all data passing

15 E. MACASKILL and J. BALL, *The Observer*, 2 November 2013 (Portrait of the NSA: no detail too small in quest for total surveillance).

16 The Committee wishes to point out that capturing and storing (meta)data is still an infringement of privacy within the meaning of Article 8 ECHR, even if the data is not examined or used.

through the cable is screened, only information that meets one or more selection criteria is effectively plucked from it and stored. In this case, the assessment of whether capturing is 'focused' or 'unfocused' depends largely on the quantity and description of the selectors. If the selectors are mainly limited to specific mobile phone numbers or IP addresses, the collection of intelligence appears to be more 'focused' (obviously assuming that a massive amount of numbers and addresses has not been supplied). On the other hand, if very wide selection criteria are applied – such as the use of specific words, a domain name (e.g. '@comiteri.be'), specific search terms in online search engines or specific applications (e.g. VPN techniques or TOR) – the unfocused nature of the collection of intelligence is clear. Although there was no absolute certainty about this at the time of the investigation, indications of massive and indeed unfocused capturing were very clear.

The Committee concluded that the 'massive' nature of data capturing can firstly be inferred from the fact that the capture is 'unfocused'. However, in relation to this investigation, the term 'massive' is equally used in the sense that even if capturing is 'focused', it is done in so many ways and at so many points that the overall information that is captured is 'massive'.

II.1.2.2.2. Five techniques

The following five 'techniques' can both supplement (e.g. because an e-mail via an intercepted cable perhaps cannot be read fully, it may be useful to retrieve the full message from the provider) and overlap each other (e.g. a mobile telephone conversion can be taken directly from the ether or from a cable):

1. upstream collection or wire-tapping of internet or telephone communication that passes through (international) fibre optic cables, for example by placing equipment at crucial points that are run by large telecom operators or by intercepting the cable itself directly, with or without the knowledge of the operator of the cable;[17]
2. downstream collection by which data is captured or requested – under pressure or otherwise – from telecom operators;[18]
3. the interception of wireless communication (traditional radio signals or mobile telephone signals sent via transmission masts and satellites);[19]

---

17 According to Snowden's slides, TEMPORA is the code name of the British programme for this form of capturing.

18 The best known example of this is the PRISM programme, in which nine large US technology companies were found to be willing and/or were forced to supply user data in a structured manner. These companies are Microsoft, Google, Yahoo!, Facebook, PalTalk, YouTube, Skype, AOL and Apple.

19 FORNSAT is purportedly the code name of one of the programmes intended to capture satellite communication. However, the interception of communication from dozens of US diplomatic and consular posts around the world (known as the F6 SITES) could also fall into this category.

4. hacking of IT systems of operators, for example, to divert useful information unnoticed;[20]
5. the cooperation and exchange of data with partner services (whether or not within the context of an alliance such as FIVE EYES).[21]

It is obviously pointless to capture a massive amount of data if it cannot be stored and exploited. In view of the enormous quantity of data that the various programmes collectively generate, not only is a gigantic amount of hardware needed for storage but also high-performance software allowing to find the proverbial needle in the haystack. The XKEYSCORE programme enables NSA analysts to process upstream information, among other tasks. Part of the analysis is undoubtedly automated, with algorithms searching for predetermined 'patterns' and 'anomalies' in the data. Another option for processing the massive amounts of data is to forward it for further analysis to partner countries or services.

II.1.2.3. Not only metadata and not only terrorism

The various programmes do not only capture metadata (such as the sender and recipient's address, connection identification, time and duration, technical device used, size of a file, etc.), but also the content of messages, whether these have been sent by mobile or landline telephone, internal VOIP mail, chats, online forum messages, clouding, e-mail attachments, Skype, etc.

The US government has long contended that only messages related to terrorism, serious forms of criminality and proliferation were intercepted. However, open sources have also convincingly demonstrated that the interests and scope of competence of the NSA, for example, as supplier of the entire US intelligence community, are far wider: economic and political information also appears to be a target.

II.1.2.4. What about personal data of Belgians and data on Belgians and Belgium?

The Standing Committee I was mainly interested in any interception of data relating to or originating from people, organisations, companies or institutions based in Belgium (or that have any link to Belgium). Relatively little in this

---

20 This is what happened at BICS, a subsidiary of Belgacom, which is responsible for telecommunication roaming in large parts of the world. The British are alleged to have succeeded via the SOCIALIST Operation, and with cooperation from the NSA, in installing technically advanced malware and in all probability diverting a massive amount of data.

21 As open sources suggest, there is also the possibility that service A does what service B may not do under its national legislation and vice versa, and that these services exchange data, which in fact amounts to a circumvention of statutory provisions (X, De Morgen, 22 November 2013, *Britse burgers massaal bespioneerd* – massive spying on British nationals).

regard has been published. Nonetheless, the Committee emphasised that it would be naive to conclude from this that Belgium has not been targeted, particularly in view of the presence of important international organisations on Belgian soil. Moreover, there was a lot of information in the revelations which indicates that large-scale interception of 'Belgian data' is possible, either directly (e.g. Belgacom/BICS) or indirectly (Belgian nationals using Google, Hotmail, Facebook, etc.).

II.1.2.5. What makes the revelations significant?

The fact that certain major powers have been in possession of advanced resources and programmes for such massive data capture for some time is general knowledge. For instance, reference can be made in this regard to the revelations concerning the ECHELON network and the SWIFT case.

However, the Snowden revelations pointed out three new elements.

Firstly, electronic espionage is taking place on such a comprehensive and massive scale from hundreds of SIGADS (data collection points) all over the world, with the most advanced hardware and software and an unprecedented use of human and financial resources. Very few means of communication or messages appear to be able to escape such interception. The fact that this happened from within an intelligence context is not so surprising. For example, internet technology, including all forms of communication that occur via the internet, offers a dream source of detailed data that was previously inaccessible. At the same time, the exponential growth of digitisation of daily life has opened many new dimensions for the intelligence world.

The second new element is that it is becoming increasingly clear that the major powers also engage in economic and political espionage on 'friendly countries' and do massive data capturing there.

The last new element is that there is almost certainly information – in the form of internal, official government documents (including leaked slides) – which demonstrates this capturing and its extent.

II.1.3. LEGAL ANALYSIS OF THE POWERS OF STATE SECURITY, GISS AND CUTA

II.1.3.1. Powers of State Security to monitor data capturing and political and economic espionage by foreign services

In an initial reaction, State Security stated that its powers to monitor massive data capturing by foreign intelligence services are evident from Articles 7 and 8 of the Intelligence Services Act. The service later explicitly called into question

its competency with regard to massive infringements of privacy. The Committee had already clearly stated in earlier investigations (e.g. ECHELON[22] and SWIFT[23]) that State Security is responsible for monitoring such espionage practices. The Committee therefore repeated both with regard to 'threats to be monitored' (espionage[24]) and 'interests to be protected' (scientific and economic potential, internal security in the form of 'human rights and fundamental freedoms'[25] and external security in the form of 'sovereignty of the State'[26]), that the Intelligence Services Act provides clear grounds for monitoring massive data capturing by foreign intelligence services, even in respect of what are referred to as friendly countries or friendly services. The Committee also emphasised that this case does not involve 'potential' threats, but 'actual' threats.

In 2008, State Security stated: "*our services have been monitoring the US Echelon system for some time. However, if an activity were to arise from the application of this new Protect America Act that would constitute an infringement of one of the interests to be protected by law, State Security will, within its legal mandate, also share its intelligence with the authorities and competent bodies concerned in accordance with the objectives of their assignments*" (free translation).

The Committee lastly drew attention to the fact that Article 8 ECHR, which offers protection against unlawful infringements of privacy, entails a positive obligation for the Member States of the Council of Europe. One of the ways to fulfil that positive obligation would be to encourage national intelligence services to detect and report on massive infringements. The Committee also referred in this regard to the recommendation arising from the draft report of the LIBE Committee of the European Parliament: '*Calls on the Member States immediately to fulfil their positive obligation under the European Convention on Human Rights to protect their citizens from surveillance contrary to its requirements, including when the aim thereof is to safeguard national security, undertaken by third states or by their own intelligence services, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law.*'[27] In that sense, intelligence services, among others, can be seen as an instrument in

22 STANDING COMMITTEE I, *Activity Report 1999*, 24–51. It is noteworthy that State Security had previously stressed to the Committee that monitoring the ECHELON system was within the scope of its competence.

23 STANDING COMMITTEE I, *Activity Report 2006*, 38–39.

24 'Espionage' does not relate only to the covert search for government information, but also includes those practices aiming to obtain confidential data of private individuals or businesses (STANDING COMMITTEE I, *Activity Report 2006*, 34–43 and STANDING COMMITTEE I, *Activity Report 2012*, 20–32).

25 First and foremost, privacy is obviously being targeted here.

26 Unlimited and unauthorised interception within the territory of a foreign State constitutes an infringement of sovereignty, even if those operations are in accordance with the law of the State that is performing them.

27 This recommendation was repeated almost verbatim in the definitive report (European Parliament, LIBE Committee Inquiry, *Electronic mass surveillance of EU citizens. Protecting*

the hands of the government to fulfil its positive obligation under the European Treaty.

II.1.3.2. Powers of GISS to monitor data capturing and political and economic espionage

In 1999, the Committee found that *'GISS is not actively investigating the 'Echelon' system and […] relies for that purpose firstly on the fact that such an investigation is not within its scope of competence as described in the new Act of 30 November 1998 on the intelligence and security services […]'*[28] (free translation). This view was repeated in 2006 in the context of the SWIFT case.[29] GISS has also maintained that it is not competent in the context of this investigation. The Committee could only concur partly with this view. Firstly, it cannot be ruled out that the espionage activities of the NSA or other friendly services also extend to Belgian defence policy. Under Article 11 of the Intelligence Services Act, GISS is supposed to perform intelligence work when an attempt is made '*to obtain unauthorised access*' (free translation) to information on the defence policy. The Committee therefore concluded that although GISS is not competent to deal with massive data capturing per se, it is competent to deal with espionage in relation to defence policy. The Committee emphasised, however, that there were no specific indications of this latter aspect in the Snowden revelations about Belgium.

Furthermore, since 2010, GISS has been competent to protect the SEP in relation to companies or institutions that are included on a specific list. A proposed list was drawn up by the Ministers of Justice and Defence at the end of 2012. Although the Ministerial Committee has not formally approved this list, GISS has considered itself competent to protect the SEP of these companies since 2013. The service therefore could no longer simply state that it was not competent with regard to the monitoring of massive data capturing since the companies included in the list may also be threatened by such practices.

GISS was also given the assignment in 2010 to "*neutralise attacks in the context of cyber-attacks on military computer and communications systems or systems controlled by the Minister of Defence and to identify the perpetrators, without prejudice to the right to immediately respond with its own cyber-attack in accordance with the legal provisions on armed conflicts*" (Article 11 §1, 2 of the Intelligence Services Act) (free translation). The Committee has already pointed to the restricted scope of application of this provision: if the attacks are targeted against other FPS or critical national infrastructure (e.g. communication

fundamental rights in a digital age. Proceedings, Outcome and Background Documents, 2013–2014, 29–30).

28 STANDING COMMITTEE I, *Activiteitenverslag 1999*, 45.

29 STANDING COMMITTEE I, *Activity Report 2006*, 38.

networks), the response may only be defensive, with no authority to neutralise the hostile system.[30]

II.1.3.3. Powers of CUTA

The core task of the Coordination Unit for Threat Assessment is to draw up ad hoc or strategic threat assessments, either on request or at its own initiative (Article 8 of the Threat Assessment Act). The powers of CUTA in this regard are limited to 'terrorism and extremism'. CUTA therefore has no specific task in relation to the current problem.

CUTA has been assigned an additional task pursuant to the Act of 1 July 2011 on the security and protection of critical infrastructures: it must perform threat assessments on specific 'critical infrastructures' in certain cases. This concept includes 'public electronic communication'. The Act is mainly aimed at 'risks of disruption or destruction of its infrastructure'. CUTA stated that it has not performed such assessments at its own initiative or on request.

II.1.3.4. Powers of the Belgian intelligence services to capture communication

Two arrangements relating to the interception of communication apply to the Belgian intelligence services: the SIM Act, which has permitted the use of specific and exceptional intelligence methods by both State Security and GISS since 2010, and the INT arrangement (Article 259*bis* §5 of the Belgian Criminal Code in conjunction with Article 44*bis* of the Intelligence Services Act), which grants specific interception powers to GISS.

In principle, neither of these arrangements constitutes a ban on the upstream or downstream collection of data, the interception of wireless communications, or the hacking of IT systems. Among other things, this is because the Belgian arrangement for the use of methods does not distinguish between wired and wireless communication, as is the case in the Netherlands and Sweden, for example. Legislation moreover specifically states for SIM methods that computer systems may be penetrated '*whether or not using technical resources, false signals, false keys or false capacities*' (Article 18/16 of the Intelligence Services Act) (free translation). For other methods as well, the intelligence service may try to obtain information in different ways: directly or via the operator. Furthermore, the means of communication (landline, mobile telephone, satellite telephone, etc.), the nature of the communication (written message, spoken word, sound and image) and the nationality of those communicating are not relevant for the purpose of the SIM Act or the INT arrangement.

---

30 STANDING COMMITTEE I, *Activity Report 2011*, 113.

Although neither arrangement contains explicit prohibitory provisions, a number of restrictions must still be kept in mind.

Firstly, acquiring communication data from an operator based in Belgium, without its knowledge (as happened with the hacking of the Belgacom subsidiary BICS) is not permitted. Article 18/17 §3 of the Intelligence Services Act states that "*if intervention is required on an electronic communications network, the operator of the network or the provider of an electronic communications service may be ordered by a written demand from the head of service and consequent upon such an order shall be required to provide technical cooperation*" (free translation).

Furthermore, as communications that may be intercepted under the INT arrangement seem to be limited to what is understood as 'communication or disclosures of information between people' (verbal or written, coded or otherwise), monitoring the surfing behaviour of an individual, for example, is not permitted.

More important is the fact that the SIM Act and the INT arrangement restrict the territorial application of interception options. This restriction can be summarised as follows[31]:

- a SIM method may not be used from abroad;
- a SIM method may not be used if the communication is located abroad[32];
- a SIM method may be used from within Belgian territory for the part of the communication that occurs in Belgium;
- based on the INT arrangement, there may be no monitoring of communication that originates from Belgium[33];

---

31 The description of the territorial scope of application was very sketchy in both statutory arrangements.
In the SIM Act, the provision concerned (particularly '*within the territory of the Kingdom*' (free translation) – Article 18/1 of the Intelligence Services Act) relates to the *place from where* or *where* (this is unclear) the method can be applied. The Committee believes that this arrangement must be interpreted, as a precaution, to mean that the SIM method may only be used when the signal of the communication to be captured is within Belgian territory. GISS interpreted the SIM arrangement to mean that SIM methods may be used abroad, if this is done as part of an assignment that is performed in Belgium. The Committee could not concur with this reasoning.
The criterion in the INT arrangement is the '*place from where the communication originates*', regardless of its destination or where or from where it is intercepted. The point of departure of communication therefore determines the jurisdiction of GISS (*Parl. Doc.* Chamber of Representatives 2002–03, 50K2059/001, 9 *et seq.*).

32 This means, for instance, that the communication of an individual phoning Belgium from abroad may be intercepted when the signal is within Belgian territory.

33 Due to worldwide roaming and the technological evolution, it is not obvious from a technical perspective for GISS to meet these requirements. This is the case, for instance, with a telephone call that originates in Belgium but is intercepted abroad. It is often not possible for GISS to determine the point of departure.

- based on the INT arrangement, there may be monitoring of communication from within Belgium if the communication originates abroad;
- based on the INT arrangement, monitoring in a foreign country is permitted according to Belgian law if this communication originates abroad, *"both in relation to armed conflicts and humanitarian missions. In the latter case it is up to Belgium to show that such equipment is legitimate, given the assignments that are entrusted to its military troops under the international mandate that forms the basis for its presence on foreign soil"*[34] (free translation).

A final restriction relates to the fact that only 'focused' captures are permitted, in principle.

The use of a SIM method, for example, is mainly 'focused' on an individual or a group. It must moreover be demonstrated that there is a genuine connection with one of the threats listed in the legislation. Practice also shows that SIM methods are not used in an unfocused manner: in 2012, for example, only 700 authorisations to obtain communication or localisation data were granted to State Security and GISS combined. Obviously just one method can generate a lot of data (such as all incoming and outgoing telephone communications for a number of months) but, as stated, the restriction lies mainly in the fact that the method focuses on an individual or a group.

It was also not the legislature's intention in relation to GISS's ability to intercept communications originating abroad for these to be 'exploratory' interceptions. Restrictions such as '*the ban on exploratory or general interceptions*' (free translation), the fact that there must be '*serious indications* [in advance] *that relate to the threat as defined in Article 11, §2, of the Act of 30 November 1998 or in the hypotheses envisaged in Article 44*' (free translation)[35], the fact that '*the possibility of monitoring is only ancillary in nature*' and must be '*properly motivated before it is used and […] a balance [must] be found between the protection of privacy and the significant risks to security and any undermining of the functioning of the democratic institutions*'[36] (free translation) are all clearly set out in the preparatory works that gave rise to the legislative amendment of 2003. In addition, Article 44*bis* Intelligence Services Act requires that the so-called Interception Plan of GISS lists the organisations or institutions whose communications will be subject to interception during the coming year. This list must also specify the envisaged period of each interception and it must be clear

---

34 This was the interpretation given by the authorised official who explained the government bill on interceptions to the Council of State (*Parl. Doc.* Chamber of Representatives 2002–03, 50K2059/001, 9 *et seq.*) The Standing Committee I noted that not every intervention falls under an international mandate and not every interception relates to a decision to deploy troops.

35 *Parl. Doc.* Chamber of Representatives, DOC 50, 2059/001, 6.

36 *Parl. Doc.* Chamber of Representatives, DOC 50 2059/003, 4 – Hearing of the then Chairman of the Standing Committee I.

from the reasons given that the interception is based on one of the legitimate grounds as described in Article 44*bis* of the Intelligence Services Act.

The INT arrangement was amended in 2010. Based on a recommendation of the Standing Committee I, '*searches*' were also made possible in addition to the '*interception, tapping, inspection or recording*' of telecommunications. The intention was to legitimise an existing, unlawful situation that was required for operational purposes: before GISS knows the frequencies on which a target in the Interception Plan broadcasts, it needs to go through the bandwidth. 'Searches' are therefore necessary. Searching for frequencies or signals on which targets in the Interception Plan broadcast is accordingly legitimate. However, searching for potential threats that do not appear in the Interception Plan by picking up all frequencies or signals without any prior and specific basis is not legally permitted.

II.1.3.5. Powers of the Belgian intelligence services to obtain data from partner services

Article 20 of the Intelligence Services Act provides that the Belgian intelligence services are responsible for collaborating with their foreign counterparts. In the first instance, this obviously means that they must be able to receive information and intelligence from foreign partners. However, does this also mean that such data may be used if they know or suspect that it has been obtained illegally or unlawfully? Or if a foreign service forwards data about a Belgian national that it obtained legally to its Belgian partner, which would not have been able to obtain that data without authorisation?

The specific question as part of the investigation was whether data obtained through an infringement of privacy may be used in an intelligence context. The Act of 30 November 1998 provides only for the destruction of data if this has been obtained without due regard of the SIM rules. The Ministerial Committee for Intelligence and Security[37], which must further implement cooperation with foreign services, has also not organised anything in this regard. The Standing Committee I referred in this regard to a recommendation included in a Resolution of the European Parliament: '*Calls on the Member States, including when represented by their intelligence agencies, to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including the protection of human rights under the TEU, the ECHR and the EU Charter of Fundamental Rights*'[38]

---

37 The Ministerial Committee was replaced by the National Security Council, see RD of 28 January 2015 on the establishment of the National Security Council, *BOJ* 30 January 2015.

38 Resolution of the European Parliament of 12 March 2014 on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs

This recommendation is in line with the position that State Security had adopted in the context of the ECHELON case: "*State Security formally states that it has not received any such unlawfully obtained intelligence. If it were offered any, it would refuse it*"[39] (free translation). This assumes, of course, that the receiving service would make the minimum effort to determine how the intelligence in question had been obtained. However, practice shows that 'supplying intelligence services' usually keep their sources (and thus the origin of intelligence) secret and that the 'receiving services' accept this. This type of understanding is part of the international intelligence culture, just like the third-party service rule, the *quid pro quo* principle and the requirements of confidentiality. Although this does not mean that the Committee outrightly supports these principles, they cannot be abruptly and unilaterally breached.

II.1.3.6. Powers of the Belgian intelligence services to collect political or economic intelligence abroad

It is the task of State Security to counter threats, not by acting itself but by developing a solid information position and informing the competent authorities in good time of imminent or actual threats. Moreover, State Security is obviously interested in 'political' intelligence of private or public persons or institutions that form (or may form) a threat to the interests within the scope of competence of the service, even if these are foreign persons or institutions. The service is clearly not looking only for publicly accessible information in this regard. It has a statutory mandate for its actions. Contrary to most foreign services, State Security acts exclusively from within Belgian territory for this purpose. However, from a legal perspective, there is no prohibition on actually collecting intelligence abroad. There is an important exception to this rule: SIM methods may only be used in Belgium (see III. 1.3.4). Another difference between State Security and certain foreign services is that State Security does not actively search, for instance, for economic intelligence on foreign companies in order to favour Belgian companies. This does not form part of its statutory mandate. State Security must collect intelligence in order to protect the economic potential of the country against espionage or interference by third parties, for example, and not spy itself to search for information that would be advantageous to Belgian companies.

GISS likewise does not have jurisdiction to engage in the collection of economic intelligence. The analysis differs from State Security with regard to 'political espionage' in the sense that the military intelligence service is active

(2013/2188(INI)). The Chairman of the Standing Committee I, Guy Rapaille, was heard together with Senator and member of the former Monitoring Committee of the Senate, Armand De Decker, by the LIBE Committee, which prepared this resolution.

39 Oral question to the Minister of Justice dated 16 February 1998, CRIV49KC0504, Q. No.740.

abroad, mainly in support of military operations. It is evident that political intelligence may be collected as a result of such operations.

II.1.3.7. Cooperation with foreign services

Reference has already been made above to Article 20 of the Intelligence Services Act, which stipulates that the intelligence services are responsible for collaborating with their foreign counterparts. The third section of this provision instructs the Ministerial Committee for Intelligence and Security to determine '*the conditions for the cooperation referred to in §1 of this Article*' (free translation). However, the Ministerial Committee has not yet issued any directive to this effect. State Security has drawn up a detailed (and classified) instruction on bilateral cooperation with correspondents. The Standing Committee I has already stated that it regards this directive as valuable, but has also pointed out that certain options chosen by State Security need to be supported by the political decision-makers, i.e. the members of the Ministerial Committee.[40] One of the main aspects of that cooperation (which intelligence may be communicated to foreign services?) was only briefly covered.

At the time of the investigation, GISS was still working on a similar memorandum with 'verifiable criteria' for the purpose of cooperation with foreign intelligence services (in the broad sense). This was scheduled for completion in 2014. In the context of this investigation, the Committee highlighted the importance of such a directive for GISS because – after approval by the Ministerial Committee – it can offer a democratically legitimised framework for alliances that the military intelligence service has already entered into.

II.1.4. STATE SECURITY, MASSIVE DATA CAPTURING AND POLITICAL AND ECONOMIC ESPIONAGE

II.1.4.1. Did State Security cooperate in the NSA programmes?

State Security was and is in no way involved in the massive data capturing by the NSA and GCHQ. More specifically, State Security had no access to the PRISM or XKEYSCORE software of the NSA, for example, and was also not involved in the spying on Belgacom/BICS. State Security moreover only has exceptional direct contact with the NSA. Over the last few years, the Standing Committee I has noted only one meeting, which was for the purpose of a specific problem. State

40 The Standing Committee I recommended that State Security send its directive to the Ministerial Committee for approval (STANDING COMMITTEE I, *Activity Report 2012*, 75, *Activiteitenverslag 2013*, 4 and *Activity Report 2013*, 167. This has not been done to date.

Security has so little contact with the NSA because, as a civil intelligence service, it mostly corresponds with the FBI and the CIA in regard to the United States.

II.1.4.2. Did State Security engage in massive data capturing?

There is no evidence to suggest that State Security engaged in massive data capturing either alone or in cooperation with other partners. The SIM Act moreover does not permit massive data capturing; SIM methods also cannot be used abroad. Lastly, it must be noted that State Security – in contrast to GISS – does not have any interception powers abroad.

II.1.4.3. Collection of political and economic intelligence by State Security?

As already explained above (see II.1.3.1), State Security collects intelligence of a '*political, ideological, religious or philosophical nature*' relating to Belgian or foreign individuals and groups that form (or may form) a threat to the internal and external security of the country. The Committee has not been able to determine within the context of this investigation that the service does not operate within the legal framework. The Committee also has no indication that State Security actively searches for economic intelligence on foreign companies in order to share this with Belgian companies, for instance.

II.1.4.4. The information position of State Security before and after the Snowden revelations

Given its jurisdiction in this area, was, could or should State Security have been aware of how the NSA and GCHQ operated before the Snowden revelations and what did State Security do after the revelations: was the problem monitored, what analyses were drawn up, which authorities were involved, etc.? From the answer to these two questions, the Committee has been forced to conclude that State Security adopted a very passive attitude towards the revelations.

II.1.4.4.1. State Security's attitude before the revelations

When the ECHELON case made the headlines in 1998, State Security seemed to be unaware of the existence of this software used by the United States to intercept European telephone, fax and e-mail communications. State Security attributed this to a lack of personnel and material resources and the fact that the protection of the SEP had only recently been entrusted to it.

One year after the first ECHELON report, the Committee wished to check whether State Security had tried to obtain further information about this worldwide interception network. The answer was no. Reference was made,

among other things, to the fact that the Ministerial Committee had not yet defined 'the scientific and economic potential of the country'.

Before press reports in 2006, State Security was also not aware that American services could view financial transaction data that was exchanged via SWIFT on a massive scale. The service used the same arguments in this case. The Standing Committee I could not concur with this.[41] Moreover, even after the incident became known, State Security did not show any sense of initiative.[42]

In August 2007, the Committee asked State Security about the possible consequences of the Protect America Act, which gave the American intelligence services extended powers to intercept all types of communication. The service answered that ECHELON had been monitored for some time and that it would communicate its information to the competent authorities if activities arose from the application of the Protect American Act that constituted an infringement of one of the interests to be protected (also see II.1.3.1).

At the end of 2008, State Security informed the Committee that it had not yet drafted any reports on ECHELON, but would monitor the ECHELON system or any other intercepting communication system. However, since no threat to internal or external security or the SEP had yet been established, State Security stated that monitoring such systems was not a priority.

Also in 2008, State Security warned the members of the government against using a BlackBerry because communication via this device, which was very popular at the time, was not secure. Indeed, all European BlackBerry data traffic passed through the United Kingdom, which could request encryption keys to protect national security or the economic welfare of the country on the basis of the RIPA Act. State Security added that comparable legislation in the United States had facilitated access to the SWIFT database by the American authorities. The underlying reasoning for this warning proved applicable to many forms of data capturing that were revealed by Snowden: Belgian or European communications often pass through foreign countries where local authorities can force persons or companies to reveal this data. The Committee regarded the warning as a good example of active interest, but found that this did not result in the service issuing a general warning concerning other forms of telecommunication as well at the time.

The Committee had to conclude that although State Security was aware of the fact that certain major powers – including friendly ones – had enormous interception capabilities before the revelations in 2013, it had no idea that these were being used on such a massive scale worldwide and that political and economic Europe was also regarded as a target in that regard. The Committee found that State Security had little insight into the nature and scope of the actions by friendly major powers, despite all the previous cases and the

41 STANDING COMMITTEE I, *Activity Report 2006*, 42–43.
42 STANDING COMMITTEE I, *Activity Report 2006*, 42–43.

information that was available in open sources. The Committee noted that State Security had not carried out any overall analysis for the government prior to the revelations, or drawn up a memorandum with regard to massive data capturing. However, the general public and companies were made aware of the possible or real threat of economic espionage, in particular, including by friendly countries, by means of seminars, a brochure and the media.

Since the ECHELON case, no instructions have been given by the hierarchy at any time to monitor such phenomena. There was accordingly no reference to be found to 'massive data capturing' or 'economic and political espionage by friendly services' in State Security's annual action plans. The topic was also never raised as regards the United States and the United Kingdom in an informal consultation platform of Western intelligence services before the revelations.

II.1.4.4.2. State Security's attitude after the revelations

State Security took three initiatives after the revelations. Firstly, representatives of the American correspondents of State Security, the CIA and the FBI, were confronted with the press reports. However, State Security never received an official response and did not insist on it further. Secondly – just as in the ECHELON case – general responses were formulated to a number of ministerial and parliamentary questions. Lastly, State Security acted as a result of the hacking of Belgacom/BICS, both as an expert in a judicial inquiry and within its intelligence assignment.

Nonetheless, the Committee was forced to conclude that State Security took very little action, even after the revelations. There was no active searching of open sources, no analyses were drawn up and there was no reporting. No instructions were given by management to monitor this case and to determine, for instance, whether and to what extent Belgian interests could be under threat. Belgium also did not place the problem on the agenda in the aforementioned consultation platform. No official questions were directed to GISS even though this service, as the natural discussion partner of the NSA, may have had access to more information. The Committee deduced from this that the service did not appreciate the problem or adequately see the connection with its statutory assignments.

II.1.4.4.3. Analysis of State Security's operations and attitude before and after the revelations

As stated, State Security raised a number of issues after both the ECHELON and SWIFT cases that were intended to explain why the service was not or could not have been aware of the espionage. The Committee noted that major progress has been made at each of those levels: the protection of the SEP and fundamental freedoms have been included in the Act, the Ministerial Committee issued a

directive on the SEP, staffing has increased over the last decade and the service is not allowed to use special intelligence methods. Even so, State Security hardly monitored the phenomenon of massive data capturing and the question again arises how the service could identify such operations of foreign intelligence services and/or whether this is possible within the current legal framework given the available resources.

The Committee held the view that it was possible for State Security to monitor the massive data capturing, including by friendly countries, in general and not necessarily in detail, and to brief and make the authorities aware at regular intervals about new practices, technical capabilities and potential threats. The information position that allows such awareness could be developed on the basis of open sources, information originating from GISS and other foreign partners, and within the limits of the current available resources and legally permitted methods.

The Committee also held the view that monitoring massive data capturing was not only necessary to inform the authorities thereof and take countermeasures, if needed, but also for State Security to modernise its own intelligence collection techniques.

The Standing Committee I felt the need to cite a number of other explanations as to why State Security did not take action before or after the revelations.

Firstly, the United States and the United Kingdom are what is known as 'friendly countries'. The service therefore saw no reason to change its priorities in relation to counter-espionage. The Committee thus found that the concept of 'friendly State' had a far-reaching impact on State Security's attitude. State Security seemed increasingly more receptive to the concept of 'strategic partners' rather than 'friendly services'.

However, State Security took no initiative to include this issue in the action plan to be approved by the competent minister. The Standing Committee I felt that there is also a role for the competent political authorities to play in this (i.e. the Minister of Justice and/or the Ministerial Committee for Intelligence and Security) when State Security proposes its annual priorities. The 2014 Action Plan once again took a classic 'threat assessment' as its point of departure for espionage.

Related to this, of course, is the fact that State Security feels that the American and British services provide a lot of useful intelligence and does not want to jeopardise these information flows.

There is generally less knowledge of signals intelligence and its technical capabilities at State Security.

Lastly, State Security did not regard the potentially massive infringement of privacy of the Belgian general public and companies as a threat that needs monitoring.

II.1.5. GISS, MASSIVE DATA CAPTURING AND POLITICAL AND ECONOMIC ESPIONAGE

II.1.5.1. Did GISS cooperate in the NSA programmes?

As was the case with State Security, the Standing Committee I was able to conclude that GISS did not cooperate in upstream collection, downstream collection or the hacking of IT systems. In other words, GISS did not participate in programmes such as PRISM, XKEYSCORE or TEMPORA and the service did not cooperate in the hacking of the Belgacom/BICS network.[43] Employees of GISS also never had any direct access to and received no training on these programmes or operations.

The answer is not so clear-cut with regard to the other two data-capturing techniques (interception of wireless communication and cooperation with foreign counterparts). After all, GISS cooperates to some extent in international programmes that the NSA also participates in, albeit to a very limited extent in light of the Snowden files. The cooperation is in fact limited to participating in interceptions in very specific and exceptional cases and to passing on intercepted SIGINT to the NSA as a partner service in a bilateral or multilateral context. The cooperation falls under the obligation as set out in Article 20 of the Intelligence Services Act (cooperation with foreign services – *supra*) and essentially envisages the fight against terrorism and the protection of Belgian and allied forces.

International cooperation in relation to SIGINT generally occurs within various forums that are formalised to some extent, e.g. by means of a Memorandum of Understanding (MOU), entered into by various SIGINT services, often without explicit and formal political cover. The Standing Committee I further investigated two multilateral SIGINT alliances of which GISS is a member: one that has existed for a number of decades and was originally set up in the context of the Cold War, and a second that was established as a result of a specific military operation, with a view to dividing the SIGINT duties there. The Committee made the following findings, among others, in relation to these two alliances:

- the objectives of an alliance are sometimes described broadly and therefore permit activities, in theory, in relation to Belgium that could fall outside the scope of legal competence of GISS.
- the membership of certain alliances is subject to the *do ut des* principle in the sense that certain efforts/investments/intelligence are expected from the partner. It is obvious that there can never be a balance between 'give' and 'take' in an alliance between a smaller service and a larger service. Yet the added value of the presence of a smaller service within an alliance lies not

[43] The service also confirmed this explicitly with regard to the Prime Minister.

(or not only) in the intelligence that it can provide, or when its own analysis capacity is limited, or costs can be shared. It is moreover plausible to think that it is also advantageous for certain countries to create broader international support for their activities through a network.

- over the years – and this is completely understandable – enormous trust has built up among the countries that cooperate closely in relation to SIGINT, which has resulted in significant loyalty and solidarity. This could explain why the NSA was immediately supported when it explained publicly that three attacks had been prevented in Belgium on the basis of its intelligence.[44] This subsequently proved to be information that had contributed positively towards a better information position in a specific Belgian terrorist case.
- although the principle of no spying on partner countries applies within alliances, the NSA and GCHQ seem not to have abided by this particular rule of conduct.
- in quantitative terms, international cooperation is very important for the Belgian SIGINT department. Most of the intelligence that this department forwards to internal or external customers in the form of reports comes from foreign partners.
- despite the fact that this form of cooperation is regarded as very important, there is no formal assessment of the overall value of the information that is supplied from the alliances.
- in 2013, GISS forwarded only a very limited number of reports in the context of one of these alliances, half of which contained information about Belgians. Most of that information was terror-related. However, this was different in the case of the other network because, as stated, the GISS's interception device forwards the metadata of all transmitted communications so all partners can consult it.
- the interceptions made by GISS as part of the international military operation were legal: they were included in the Interception Plan, they formed part of the GISS's assignment to protect Belgian and allied forces operating within an international mandate, and they were – through the use of a limited number of criteria – 'focused'. The deployment of SIGINT personnel by the Government was also approved in the broader context of sending troops. The Ministerial Committee for Intelligence and Security had not set out any directives, however, for cooperation or for forwarding intelligence to third-party services.[45]
- within a specific framework, the metadata of *all* communication of a certain region was stored and shared among the partner countries. GISS had no idea

---

44 K. CLERIX, *MO Magazine*, 6 August 2013 (*Militaire inlichtingendienst getroffen door ernstig cyberincident* – Military intelligence service affected by serious cyber incident).

45 The necessity of such directives is clear from the fact that partner countries could, for example, use the forwarded data for purposes other than what it was collected for.

about the volume of the stored data. All the partner countries had access to this data and could perform searches in it. GISS also made use of this possibility. This usage was, however, less clear-cut from a legal perspective. Depending on the search method (e.g. data mining to detect new threats), GISS was possibly operating in a legal vacuum. The Committee believes that the interception rules need to be developed further in this case.
- the Committee stressed that it had no indication that GISS would use alliances to obtain information that it cannot legally collect itself. However, GISS did not verify the lawfulness (according to Belgian or foreign law) of the collection of intelligence by foreign partners. The main reason for this is that it is almost impossible. In addition, the people who receive the raw intelligence (and this is, in fact, the only intelligence that could give an indication of whether it has been obtained lawfully) are not well-versed in legal matters.
- strict secrecy, which is strictly monitored, exists within the alliances. This duty of confidentiality does not only apply within GISS (through intensive fragmentation), but also outside it. The importance of this aspect will be explained further below.

The duty of confidentiality imposed on the SIGINT alliances is very strict. At a formal level, all intelligence relating to SIGINT is protected by the requirement to have a specific clearance, over and above the normal Belgian 'TOP SECRET' security clearance. This is not a requirement that is based on Belgian legislation but rather an obligation that originates from NATO regulations. Obtaining this clearance is not subject to additional screening; the candidates – who must already hold TOP SECRET clearance – are given a briefing during which the sensitivity of working with SIGINT is emphasised. GISS ensures that the number of people with this clearance is kept to a minimum.

Although the Committee understands that signals intelligence is a very sensitive area in which the need-to-know principle must be applied strictly and certain fragmentation is warranted, it does not see any fundamental differences with certain other domains of intelligence work that are equally sensitive. Examples include image intelligence (IMINT) or the use of SIM methods. Whatever the case, such confidentiality cannot be extended to the political level (i.e. the Minister of Defence and/or the Ministerial Committee for Intelligence and Security). At the time of the investigation, only the Minister of Defence had specific SIGINT clearance. The Standing Committee I wondered whether the previous and current Ministers of Defence were 'adequately' informed – in other words, if they were able to assume their political responsibility towards Parliament – regarding politically relevant elements of GISS's SIGINT cooperation, and thus whether or not the culture of strict secrecy characterising

SIGINT led to insufficient transparency. Obviously, the question of whether a certain element is 'politically relevant' is an evolutionary fact (given changes in political sensitivity, a fluctuating geopolitical situation, new technological developments, etc.).[46]

The Committee did emphasise that the confidentiality was not prompted by any form of deliberate retention.

On other occasions, GISS has stated that its duty to adequately (or even fully) inform the authorities is fulfilled by notifying the Standing Committee I about SIGINT details. However, it is evident that the review body cannot ensure political cover.

The Committee also referred in this regard to the Ministerial Committee's lack of a directive under Article 20 of the Intelligence Services Act. Such a directive would at least set out a broad outline for GISS's cooperation at SIGINT level, as well as rules for exchanging SIGINT with various partners. This will be dealt with more extensively in the recommendations.

II.1.5.2. Did GISS engage in massive data capturing?

The Standing Committee I found that data capturing by GISS itself could not be described as 'massive' at the time of the investigation, because of legal, technical and staff constraints. However, the Committee did have a number of reservations in this regard.

As already stated (*infra*), the interception device that was used in the aforementioned military operation formed an exception to this in a certain sense.

Secondly, the scope of the 2014 Interception Plan was so broad that very few restrictions were placed on the GISS's interception options in theory. Partly in view of the technological developments and the presence of GISS in certain SIGINT alliances, the Committee, pursuant to its powers under Article 44*bis* of the Intelligence Services Act, formulated its comments in this regard. If GISS uses the new technological options, it must take into account the restrictions placed by the INT arrangement (see II.1.3.2).

II.1.5.3. Collection of political and economic intelligence by GISS?

GISS only gathers foreign intelligence in the political or economic sphere to the extent that this is relevant to its assignments, for example the protection of Belgian and foreign troops.

---

46 However, some form of control would be possible through the approval of the budgets that are needed for certain procurements.

II.1.5.4. The information position of GISS before and after the Snowden revelations

As stated, the scope of competence of GISS includes espionage in relation to defence policy. No specific indications of this were found in the Snowden revelations about Belgium. In addition, the service has been competent since 2013 to monitor data capturing, insofar as this may form a threat to the SEP of a number of named companies and institutions. The Committee is further of the opinion that it is the duty of an intelligence service to know the capabilities and procedures of other services, not only to inform the competent authorities and to be able to take countermeasures, but also to modernise its own collection techniques. This goes for both friendly services and other services.

The Committee was therefore of the opinion that GISS also had to be asked whether it was or could have been aware of the operations of the NSA and GCHQ before the revelations. The actions taken by GISS after the revelations were also investigated.

II.1.5.4.1. The GISS's attitude before the revelations

Before the ECHELON case made the headlines in 1998, GISS was aware of the alliance that existed among the so-called FIVE EYES. However, since these countries did not form a military threat, GISS decided – correctly at that time, according to the Committee – that it did not have to make any special intelligence efforts.

One year after its first ECHELON report, the Committee wished to see whether GISS had taken any further steps. The service did point out at the time that the increasing digitisation of society posed enormous threats in relation to communications security.

In 2006, GISS was unaware that the US services had access to SWIFT data. However, the Standing Committee I decided this was normal, given the GISS's scope of competence.[47]

Following the signature of the Protect America Act in 2007, which gave the US intelligence services extended powers to intercept all types of communication, the Committee also questioned GISS. One division stated, among other things, that it was not unreasonable to think that the NSA was carrying out interceptions on Belgian soil, in relation to national or foreign authorities and private institutions. It also referred to the possible consequences of the additional interception options provided under the Protect America Act. Another division did not share this view, however. This division did not perceive any threat as it had a good working relationship with the US services and counted on mutual loyalty.

---

47 STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 39.

As far as the GISS's information position before the Snowden revelations is concerned, the Committee distinguished between the insight of the service into the theoretical and actual SIGINT capacities of the NSA and GCHQ on the one hand, and its insight into the scale and SIGINT target strategy of these services on the other hand.

The theoretical technological capacities of the NSA did not surprise the GISS's SIGINT department, which was and is well aware of technological developments. This department moreover had insight into the type and origins of intelligence that can effectively be traced through such methods. The SIGINT department had no knowledge of specific programmes and their code names, however. The SIGINT department did not carry out any studies or draft reports in this regard. In addition to the above-mentioned secrecy, the fact that these capacities were not particularly surprising to technologically skilled people in the SIGINT sector, and thus did not give rise to a specific initiative, undoubtedly played a role here.

As far as the scale of data capturing, the target strategy, and the integrity of the numerous technical options are concerned, the Committee was able to conclude that GISS did not have much factual data on which to build in this regard.

Lastly, it must be mentioned in relation to the nature of the monitored persons, that GISS was only able to make an overall inference from the SIGINT provided by the NSA that this related to people suspected of involvement in or links to international terrorism. There were no indications that ordinary citizens, policymakers or companies were the focus of the NSA's attention.

II.1.5.4.2. The GISS's attitude after the revelations

GISS firstly contacted various representatives of the different intelligence services, including the NSA and GCHQ, to express Belgium's dissatisfaction. During a meeting with European counterpart services, an initiative was also taken to boost confidence among the services, with those present able to voluntarily undertake not to perform any clandestine SIGINT operations in relation to other EU countries. Lastly, GISS pointed within one of its networks to the potential operational and political consequences of the underlying facts of the Snowden revelations.[48]

GISS organised briefings on the case for various authorities. Answers were also prepared for the many parliamentary questions.

GISS further provided technical cooperation in the judicial inquiry that followed the hacking of the BICS network. GISS is also involved in the analysis of the malware.

---

48 The political consequences refer, among other things, to tighter supervision of the intelligence services, such as in the Netherlands and Germany.

Lastly, GISS announced a dual reaction/attitude: one at national level and one at international level.

At national level, more attention would have to be paid to cyber security, both within and outside GISS, and to cyber intelligence. The Snowden revelations have exposed weaknesses in the security system. These must addressed through technical measures, briefings, screening, etc. In other words, a full risk management strategy must be developed in relation to possible leaks.

At international level, trust in the intelligence services involved must be reinstated. GISS pointed out that reverting to 'isolationism' would not be the right response. International cooperation must be maintained. Yet, they should be aware that it is no longer clear who can be considered to be friendly services. As is also the case for State Security, a directive on cooperation with foreign services should be drawn up as well.

The Committee had to conclude that apart from compiling a file in preparation for an international meeting, GISS did not carry out any structured search of open sources, did not prepare any all-sources analysis, and did not make adequate use of its own intelligence.

One meeting was held with State Security in relation to the revelations.

II.1.5.5. Analysis of the GISS's operations and attitude before and after the revelations

The fact that GISS initially took little intelligence-related initiatives both before and after the revelations can mainly be explained by the fact that the underlying threats, such as those reported on at the time of the investigation, fell outside its scope of competence. On the other hand, the Committee holds the view that every intelligence service must have a documented insight into the capabilities of its counterpart services, either to support its own collection or to be able to take countermeasures, if needed (e.g. if it becomes clear that Belgian defence policy is the target of espionage). In that sense, a certain form of monitoring would have been appropriate.

The GISS's attitude was obviously also explained by the fact that friendly nations were involved. As part of the investigation into the protection of communication systems against possible foreign interceptions and cyber attacks, for instance, the Committee was able to conclude that the actions of the US intelligence services did not appear in the Intelligence Steering Plan.[49] After all, GISS relied on the loyalty of the partner services within NATO, since the application of the Patriot Act is targeted against the enemies of the United States.[50, 51] The Committee was able to

[49] See STANDING COMMITTEE I, *Activity Report 2011*, 111, on the ECHELON case.

[50] This attitude was also observed in the German intelligence services, for example.

[51] In an earlier investigation, the Committee even had to note that any espionage by friendly services was not seen as an immediate threat that would require its priority attention (see STANDING COMMITTEE I, *Activiteitenverslag 2000*, 57).

conclude that an increasing number of players these days feel there are many partners in the intelligence world, but no friends.

A third element that could help explain a lack of action from GISS is undoubtedly the fact that the US intelligence service was one of its most important sources of information. This can result in certain intelligence activities not being seen as a problem or being seen as less of a problem.

The Committee did emphasise that GISS has made efforts to put this on the agenda at international SIGINT forums since the end of 2013.

II.2. PROTECTION OF PRIVACY AND MASSIVE DATA CAPTURING

In the wake of the Snowden revelations, the former Monitoring Committee of the Senate asked the Committee to provide an overview of the rules applicable in Belgium to the protection of privacy for resources that permit the large-scale interception and exploitation of the data of people, organisations, companies or institutions based in Belgium. The investigation should also have provided insight into the legal instruments that allow the State, citizens or companies to take action against any infringements of fundamental and other rights.

The Committee relied on the expertise of Prof. Annemie Schaus (ULB) for this investigation. From the comprehensive advisory report, which was included in its entirety in the last annual report[52], the Committee recalled the following, among other things [53]:

- the massive and random nature of the interception, monitoring, use and storage of personal data are contrary to the ECHR on all levels.
- respect for privacy is also a duty of the providers of social network services that fall under the territorial scope of the ECHR.
- convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which is binding on all Member States of the Council of Europe, is one of the best legal instruments to protect individuals against the risks inherent to electronic monitoring.

---

52 A. SCHAUS, *'Opinion on the rules applicable in Belgium to the protection of privacy in relation to resources that permit the large-scale interception and exploitation of data of people, organisations, companies or institutions based in Belgium (or that have any link to Belgium)* (free translation)', STANDING COMMITTEE I, *Activiteitenverslag* 2013, 185–210.

53 The Committee already formulated some of these conclusions as a result of its investigation into the ECHELON network (STANDING COMMITTEE I, *Activiteitenverslag* 2000, 27–60) and the SWIFT case (STANDING COMMITTEE I, *Activity Report 2006*, 38–43). At the time of the ECHELON case, the Belgian Parliament also arrived at the conclusion that the system constituted an infringement of Article 8 ECHR because it did not comply with the principles of legality, legitimacy and necessity *Parl.Doc.* Senate 2001–02, no. 2–754/1 and *Parl. Doc.* Chamber of Representatives 2001–02, no. 50 1660/001).

- directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, applies rationae loci to the providers of social network services, even if they are headquartered outside the European Economic Area (EEA).[54] This Directive prohibits the transfer of personal data outside States that are not EEA members if these States cannot guarantee at least the same degree of protection.
- the EU-US Safe Harbour agreement on data protection was clearly breached, because companies with a Safe Harbour certification have allowed the use of personal data as part of the large-scale data collection by the National Security Agency (NSA).
- personal data that is processed for the purpose of police and judicial cooperation in criminal cases does not fall under the scope of Directive 95/46/EC or the Safe Harbour principles. The exchange of such data between the European Union and the United States is governed by ad-hoc agreements, such as the agreement on mutual legal assistance, the agreement on the use and transfer of passenger name records (PNR), and the agreement on the processing and transfer of financial messaging data with a view to preventing and combating terrorism and terrorist financing (TFTP).
- the large-scale monitoring of electronic communication without the consent of the State in whose territory that monitoring has occurred infringes the sovereignty of that State, even if the interception occurs from an installation within the territory of a third-party State. The fact that these interception operations comply with the law of the State that performs them does not alter this. The same applies to clandestine interception operations from embassies of third-party States within the territory of the host country.
- the State, citizens and companies have various means to combat infringements of fundamental rights before the International Court of Justice, the European Court of Human Rights, the Belgian courts, etc.
- the use of certain methods (such as phone tapping or hacking) by a foreign intelligence service within Belgian territory constitutes a criminal offence.

At the instigation of its Committee on Civil Liberties, Justice and Home Affairs (LIBE), the European Parliament formulated various identical conclusions in its Resolution '*on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs*'[55]:

---

54 See in this regard: Group 29, WP 163 'Opinion 5/2009 on online social networking' of 12 June 2009.

55 Resolution 2013/2188 (INI) of the European Parliament (12 March 2014), P7_TA(2014)0230.

- the surveillance programme PRISM which was revealed constitutes a serious interference with the fundamental rights of citizens.[56] It is stressed that privacy is not a luxury right, but that is the foundation stone of a free and democratic society.
- the Member States must refrain from accepting data from third states that has been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies that are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments.
- the Member States are called upon to immediately fulfil their positive obligation under the ECHR to protect their citizens from surveillance contrary to the provisions of the Convention, including when the aim thereof is to safeguard national security, and to ensure that the rule of law is not weakened as a result of extraterritorial application of a third country's law.
- Member States must install meaningful oversight of intelligence activities by parliamentarians or expert bodies with legal powers to investigate.

II.3. USE IN CRIMINAL CASES OF INTELLIGENCE ORIGINATING FROM MASSIVE DATA CAPTURING BY FOREIGN SERVICES

In July 2013, the Chairman of the Flemish Bar at the Brussels Bar lodged a complaint with regard to '*State-organised and unrestricted internet espionage that had been used massively for years*' (free translation). The Chairman was referring to the data capturing activities of the American and British intelligence services via Signals Intelligence (SIGINT), which had been brought to light by Edward Snowden. He contended that these activities, to the extent they could also affect Belgians, were contrary, inter alia, to Article 8 ECHR, the provisions of Convention no. 108 on data privacy[57], and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union. The President also argued that State Security[58] had not complied with the 'positive legal obligation' that rests on the government to safeguard the fundamental rights and freedoms of citizens[59] and

---

56 The European Court of Human Rights will also have to rule on the massive data capturing. It was approached in October 2013 by various associations that filed a complaint relating to the revealed practices. Judgment has not been handed down in this case to date.

57 Council of Europe, Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, ratified in Belgium by means of the Act of 17 June 1991.

58 Although the complainant referred only to State Security, the Standing Committee I held that GISS should also be included in the investigation.

59 In this regard, see ECHR, no. 38478/05 of 5 March 2009, Jankovic *v.* Croatia, and ECHR, no. 32881/04 of 28 April 2009, K.H. *v.* Slovakia.

that the use before the courts of data that has been obtained by massive data capturing "*is at odds with the obligation to safeguard rights and fundamental freedoms*" (free translation).[60]

The investigation of the Standing Committee I focused mainly on this last issue since the other aspects of the claim had already been dealt with in two earlier investigations.[61]

II.3.1. LEGAL FRAMEWORK FOR THE TRANSFER OF INTELLIGENCE TO JUDICIAL AUTHORITIES

There are several provisions that govern the transfer of information from the intelligence services to the judiciary:

- article 29 BCCP stipulates that an official – and thus also a member of State Security or GISS – who receives notice of an offence or crime during the performance of his duties, must report this to the judicial authorities;
- when such information is obtained via specific or exceptional methods, the provisions under Article 19, 1° of the Intelligence Services Act apply, which entails that the transfer takes place on the basis of an unclassified official report drawn up by the SIM Commission;
- article 19 of the Intelligence Services Act states that State Security and GISS may share the intelligence in their possession with the judicial authorities only when this is relevant in the context of their assignments;
- lastly, the intelligence services and the judicial authorities usually rely on Article 20 §2 of the Intelligence Services Act (which provides for technical assistance by State Security and GISS) as the basis for the reciprocal flow of information. However, the Standing Committee I has already stressed on several occasions that this provision must be interpreted restrictively and thus not form the basis for passing on intelligence.[62]

These rules were detailed further in circulars COL 9/2005 and COL 9/2012 of the Board of Procurators General.

---

60 It is important to stress that the Chairman, who had referred to a possible 'infiltration' of the suspected espionage activities to Belgian criminal case files, could not produce any files in which this could have been the case. A survey within his Bar also failed to produce any specific case files that could have been usefully investigated by the Committee.

61 See Chapter II.1. 'The Snowden revelations and the information position of the Belgian intelligence services' and Chapter II.2. 'Protection of privacy and massive data capturing'.

62 See STANDING COMMITTEE I, *Activiteitenverslag 2004*, 137 and STANDING COMMITTEE I, *Activity Report 2006*, 50–51.

II.3.2. LEGAL FRAMEWORK FOR THE USE OF INTELLIGENCE IN CRIMINAL CASES

As COL 9/2012 states, since there are no restrictions on the furnishing of evidence in criminal cases, all necessary documents may be included in the investigation file provided that they are not classified. Intelligence from State Security or GISS does not have any special probative value.

However, the following question was crucial to this review investigation: what happens if intelligence passed on by the Belgian intelligence services to the judicial authorities has been obtained by means of a data collection system that is unlawful under Belgian law? The Committee referred in this regard to the opinion that its expert[63] had formulated in an earlier investigation:

> *"The Belgian criminal procedural law […] has a rule that excludes evidence which has been unlawfully obtained. However, this exclusion is not absolute. A new Article 32 has been added to the Belgian Code of Criminal Procedure by the Act of 24 October 2013, which reads:*
>
> *"Article 32. A decision will be made to declare unlawfully obtained evidence invalid if:*
> – *complying with the relevant formal requirements is prescribed subject to otherwise being declared invalid; or*
> – *the committed irregularity has impaired the reliability of the evidence; or*
> – *the use of the evidence is contrary to the right to a fair trial."*
>
> *This provision follows from the 'Antigoon' judgment of the Supreme Court on 14 October 2003. This case law had already given rise to the Act of 9 December 2004 on reciprocal international legal assistance in criminal cases and to the amendment of Article 90ter of the Belgian Code of Criminal Procedure, Article 13 of which stipulates:*
>
> *"Article 13. For the purpose of criminal proceedings being conducted in Belgium, use may not be made of evidence:*
> 1. *that has been collected irregularly abroad if the irregularity:*
>   – *according to the law of the State in which the evidence has been collected follows from the contravention of a formal requirement that is prescribed subject to otherwise being declared invalid;*
>   – *impairs the reliability of the evidence;*
> 2. *whose use constitutes an infringement of the right to a fair trial."*
>
> *This regulation of evidence thus implies that any unlawfulness or irregularity does not automatically lead to that evidence being disregarded"* (free translation).

63 See '*Opinion on the rules applicable in Belgium to the protection of privacy in relation to resources that permit the large-scale interception and exploitation of data of people, organisations, companies or institutions based in Belgium (or that have any link to Belgium)* (free translation)', in STANDING COMMITTEE I, *Activiteitenverslag* 2013, 209–210.

It follows from this – hypothetically – that intelligence which is legal in the country of origin under the stated conditions (not irregular in the country of origin and no impairment of the right to a fair trial) may indeed be added to and used in Belgian criminal proceedings, even its collection would have been unlawful under Belgian law.

II.3.3. PROCESSING AND FORWARDING OF FOREIGN SIGINT BY STATE SECURITY AND GISS

II.3.3.1. General

State Security does not keep in regular contact with the foreign services that set up massive data capturing programmes via SIGINT according to the Snowden revelations. The international partners of State Security are the American FBI and CIA and the British Security Service (MI5) and Secret Intelligence Service (MI6), which are not SIGINT agencies themselves (in contrast to the NSA and GCHQ). The original SIGINT source (e.g. the NSA or GCHQ) has already been removed several steps before this intelligence reaches State Security via these partners and State Security passes this on to the public prosecutor's offices. State Security also does not simply forward the data received from abroad to other Belgian services. In principle, the information is assessed and supplemented or qualified if necessary.

As far as GISS is concerned – which does have direct contact with the NSA and GCHQ – an earlier investigation has shown that the data which these foreign services possibly collect on a massive scale is not shared proportionately with GISS. Although the exchange of intelligence between the services is very limited, this does not rule out the possibility that some of this data could have originated from the controversial programmes. GISS does not verify the lawfulness or otherwise – according to Belgian or foreign law – of the collection of intelligence by foreign partners. This is also almost impossible because it is seldom indicated how the information has been collected. Nonetheless, the Committee stated (just as in the first investigation 'The Snowden revelations and the information position of the Belgian intelligence services') that the receiving service should make the minimum effort to determine how the intelligence in question has been obtained. However, practice shows that 'supplying intelligence services' usually keep their sources (and thus the origin of intelligence) secret and that the 'receiving services' accept this. This type of understanding is part of the international intelligence culture, just like the third-party service rule, the *quid pro quo* principle and the requirements of confidentiality. However, this does not mean that the Committee outrightly supports these principles. The Committee confirms that these principles cannot be abruptly and unilaterally breached.

The Committee also refers in this regard to a judgment of a Dutch court that had to examine whether and to what extent an intelligence service (Dutch in this case) may accept and use data from foreign partners if it is not certain how this data was collected, for which the hypothesis exists (or at least is not refuted) that it may have been collected via methods that the national service cannot or may not apply.[64] The Court held the following, inter alia: "*Given the basic principle of Article 59, 1° of the Dutch Intelligence and Security Services Act 2002 and the wide discretion of the Member States in testing against Article 8 ECHR, the State argues on adequate grounds that it cannot be expected to jeopardise urgently needed cooperation with foreign services, such as those of the USA, simply because of a lack of knowledge about their procedures and the chance that Dutch services will receive intelligence that has been collected in a manner that is not permitted in the Netherlands. The compelling interest of national security is what is decisive here*" (free translation).

II.3.3.2. Specific

As stated, the Chairman's consultation with the members of his Bar did not produce any specific case files that could point to any intelligence that has been included in criminal case files and originated from (foreign) massive data capturing programmes. Even the investigation of the Standing Committee I – which related, in principle, to the period 2011–2013 – produced very little in the way of specific data.

II.3.3.2.1. As regards State Security

The information originating from State Security related only to the period from November 2012 (until June 2014) because the database of this service could only establish a link from then between the outgoing memoranda and the incoming messages that formed their basis.

During that period, State Security received around 4,000 intelligence reports from the FBI, CIA, BSS and SIS. However, of the approximate 550 memoranda that State Security sent in the same period to the public prosecutor's offices, a direct link could be established between the original foreign intelligence and those memoranda in only 14 cases. Additionally, there was information that originated from SIGINT in only two memoranda (which both related to the same case). Even so, the service providing the information was not an intelligence service. Moreover, it was impossible for State Security to determine precisely which SIGINT resources have been used, although nothing pointed to any massive unfocused capturing. The SIGINT information was summarised

64 The Hague District Court of 23 July 2014, cause list number C/09/455237 / HA ZA 13.1325. An appeal has been lodged against this judgment.

very briefly in the memoranda sent to the public prosecutor's offices, without reference to the original source. The memoranda also included intelligence produced by State Security itself. These memoranda did not include any information on the relationship between a client and his lawyer.

In general, this investigation indicated that State Security shared SIGINT information from American and British sources with the judicial authorities only to a very limited extent.

II.3.3.2.2. As regards GISS

GISS also passed on intelligence originating from SIGINT operations of the American or British services to the public prosecutor's offices in only two cases. GISS sent a classified and unclassified report in both cases.

In one of the cases, it transpired that the information originated from SIGINT operations of one of the envisaged foreign intelligence services. These were not 'unfocused' operations as they focused on a specific target. The information in the other case originated from the internet.

II.3.4. CONCLUSION

The volume of intelligence and information originating from abroad that the Belgian intelligence services passed on to the judicial authorities in the investigated period was very limited.

The Standing Committee I moreover found no indications that this involved intelligence originating from (American or British) massive data capturing programmes (SIGINT data). The information also did not relate to the relationship between lawyers and their clients.

In the context of this investigation the Standing Committee I therefore found that no inferences could be drawn suggesting that information originating from abroad had prejudiced the rights of Belgian legal subjects in that manner.

II.4. STATE SECURITY AND ITS CLOSE PROTECTION ASSIGNMENTS

II.4.1. TIME FRAME

The Standing Committee I learnt in the context of an earlier review investigation[65] that there were possible problems with the availability of

[65] STANDING COMMITTEE I, *Activity Report 2012*, 40–42. (II.5. Joint investigation into CUTA's threat assessments relating to foreign VIP visits to Belgium). The close protection

'protection officers' at State Security for carrying out close protection assignments. A number of assignments were allegedly not carried out. The Committee thereupon decided to open an investigation focusing on the following questions: does State Security carry out all the close protection assignments that are entrusted to it, what problems does it face in this regard, and what are the causes of these problems?

In mid-July 2013 – when the investigation was in full swing – the Federal Government decided to transfer this assignment of State Security to the Federal Police.[66] This decision did not come as a total surprise: at the end of March 2013, State Security submitted a (draft) 'Strategic plan 2013–2016' to the Minister of Justice, which mentioned transferring the close protection assignments to another service. This was in line with State Security's strategic course in which the intelligence assignment takes priority: reintegrating the inspectors that are currently in the Close Protection Service would allow to reinforce the intelligence assignment.

Although discussions on the transfer did commence, the Council of Ministers at the time ultimately decided in February 2014 not to decide on the issue during the current legislature.

This was done by the new Parliamentary majority in the Federal Coalition Agreement of October 2014: "*The government will take the necessary initiatives so the Federal Police can fully take over the close protection assignments (including staff and accompanying resources) from State Security. This will be a budgetary-neutral initiative*"[67] (free translation).

Once the transfer is complete, a number of findings from this investigation will undoubtedly become less relevant. However, this does not apply to all of the Committee's conclusions. After all, a number of problems will continue to exist unabated, even if the Federal Police and not State Security is responsible for close protection.

II.4.2. LEGAL FRAMEWORK

The protection of persons is a duty of the (administrative) police and has long been performed by State Security, which was expressly given this assignment in 1998. Article 7, 3° of the Intelligence Services Act stipulates that "*the execution of*

assignment of State Security had already attracted the attention of the Standing Committee I before. In this regard, see inter alia STANDING COMMITTEE I, *Activiteitenverslag 1996*, 70–86 and 231; *Activiteitenverslag 2003*, 164–168 and *Activity Report 2011*, 134 *et seq.*

66 According to press reports of 7 October 2013 (*Belga, De Morgen, het Nieuwsblad*), the spokesperson for the Minister of the Interior announced that the transfer would take place on 1 April 2014.

67 The transfer had not been completed by the time this activity report was finalised.

assignments for the protection of persons that are entrusted to it by the Minister of the Interior" (free translation) is one of the duties of State Security.

Article 5 of the Intelligence Services Act further stipulates: "*State Security carries out the duties assigned to it under the authority of the Minister of Justice. The Minister of the Interior can nevertheless make demands on State Security in connection with the execution of assignments provided for in Article 7, if these concern […] the protection of persons. In such a case the Minister of the Interior, without becoming involved in the organisation of the service, specifies the subject of the request and can make recommendations and give precise indications concerning the resources to be employed and the financial resources to be allocated. Should it prove impossible to act on such recommendations and evidence because their execution would imperil the execution of other assignments, the Minister of the Interior shall be informed thereof at the earliest opportunity. This does not discharge State Security from the obligation to execute the request*" (free translation).

The assignment is detailed further in Article 8, 5° of the Intelligence Services Act "*protection of persons: ensuring the protection of the lives and the physical integrity of the following persons, designated by the Minister of the Interior: a) foreign heads of State; b) foreign heads of government; c) the family members of foreign heads of State or government; d) members of Belgian and foreign governments; e) certain important people who are the subject of threats resulting from the activities referred to in Article 8, 1°*" (free translation).

Protection officers "*are the only agents of the State Security field services who are competent to carry out close protection assignments, to the exclusion of any other assignment*" (Article 22 of the Intelligence Services Act) (free translation). To this end, they have the general powers that all State Security agents possess[68] and can use almost all normal intelligence methods. The protection officers also have purely policing powers (e.g. the right to enter abandoned buildings, conduct security searches, identity checks, etc.).

In addition to the provisions from the Intelligence Services Act, a number of other rules are important. For example, on 8 February 2000, a protocol agreement on '*Police measures relating to the visits of certain foreign personalities*' (free translation) was entered into between the Ministers of the Interior, Foreign Affairs and Justice, laying down protection measures that are always provided in a number of pre-determined cases. The close protection assignment within this protocol agreement applies only to heads of State, heads of government and ministers of Foreign Affairs. The agreement provides for close protection of the personalities involved by protection officers of State Security. This protocol was evaluated in September 2003 and the capacity of State Security for the various protection assignments was determined.

---

68 Cf. Article 24 of the Intelligence Services Act, with reference to Articles 12–14 and 16–18 of the Intelligence Services Act.

In early March 2004, the Board of Procurators General issued Circular no. 6/2004 on the protection of personalities, government officials and private individuals under threat.[69] Among other things, this circular further details the provisions of Article 23 of the Intelligence Services Act. The provision governs the exchange of information with the judicial authorities in relation to the protection of persons.

Reference can also be made to Government Instruction MO 100.A of 10 June 1974. Although this instruction is outdated, the spirit of it remains important, specifically in relation to cooperation and the division of roles among the services.

Lastly, State Security drafted a number of internal regulations, most recently in February 2013.

II.4.3. PROCESS DESCRIPTION OF THE PROTECTION ASSIGNMENTS

The protection assignments are subdivided into 'permanent' and 'ad hoc' (or also 'official') assignments. Permanent assignments relate to the protection of foreign diplomats who are accredited in Belgium and receive protection during their stay in the country (in principle, constantly). Ad hoc assignments relate to the protection of VIPs during their official visits to Belgium.

In relation to the ad hoc assignments, State Security is the last link in a process in which the need for protection of a visiting VIP is assessed and then implemented.

The FPS Foreign Affairs is firstly advised, via diplomatic channels, of the visit of a person who needs protection. A request for protection is prepared. The Government Crisis Centre then opens a file in order to assess whether the person needs protection and, if so, which protection.[70] To this end, it asks CUTA and the Federal Police, each in relation to their scope of competence, to investigate the threats to which this person is exposed. Information is also provided by the judicial authorities, among others.[71, 72] CUTA[73] (and the Federal Police when

---

69 This replaced Circular COL 1/2001 *'governing the procedures to be taken into account when communicating information concerning close protection – Implementation of Article 23 of the Act of 30 November 1998'* (free translation) of 5 February 2001.

70 A State Security liaison officer is also attached to the Crisis Centre.

71 Cf. COL 6/2004 of 1 March 2004 issued by the Board of Prosecutors General on the protection of personalities, government officials and private individuals under threat.

72 If necessary (e.g. if certain elements are unclear) the Crisis Centre organises a coordination meeting with the authorities involved in the case.

73 The assessment of the threat during a visit by a foreign VIP to Belgium falls under the scope of CUTA's legal assignments. After all, one of its tasks is "*to perform a joint assessment on an ad hoc basis that must enable one to judge whether threats, as referred to in Article 3, exist and what measures are necessary in such a case*" (free translation) (Article 8, 2° of the Threat

there are specific elements of a criminal threat) shares its findings with the Crisis Centre, which in turn decides which measures are needed.[74] If necessary, State Security is given an intervention assignment, which it then carries out. Certain tasks may also be assigned to the local police or other authorities (e.g. airport police).

II.4.4. THE STATE SECURITY'S CLOSE PROTECTION SERVICE

The Close Protection Service forms part of State Security's External Services and falls under the control of the Director of Operations.

The service is headed – in principle – by a head of section, assisted by one or more deputies. Since October 2011, it was in fact headed by a deputy head of section (commissioner), who has been assisted since September 2012 by a divisional inspector. The secretariat of the service was provided by a group of six protection assistants (i.e. not administrative staff and also not recruited for this purpose), who took turns to man the secretariat.

Protection itself is the task of protection officers and assistants. Protection officers are at the grade of inspector (level B). Their task consists in managing any type of protection assignment or holding the position of 'key man'.[75] Protection assistants are level C personnel.[76] They are tasked with performing the protection assignments entrusted to State Security.

The status of personnel performing close protection assignments is governed by the Royal Decree of 13 December 2006 on the status of the officials of the field services of State Security.

The workforce of the Close Protection Service has grown sharply over the years, almost tripling since 2000. The main change in the composition of the workforce occurred in 2009, with a sharp rise in staff levels due to the recruitment of protection assistants.[77] The workforce was at its largest in 2010, the year of the Belgian European Presidency. Since then, inspectors (around one-

---

Assessment Act). For more detailed information see: STANDING COMMITTEE I, *Activity Report 2012*, 40–42 (II.5 Joint investigation into CUTA's threat assessments relating to foreign VIP visits to Belgium).

74 The protection assignments are divided into categories depending on the 'threat level' as described in the Threat Assessment Act of 10 July 2006 and the Threat Assessment Decree of 28 November 2006. Four threat levels are described in Article 11 of the Threat Assessment Decree: level 1 or 'low', level 2 or 'average', level 3 or 'serious' and level 4 or 'very serious'.

75 The key man is the person who sits in the front passenger seat of the VIP vehicle.

76 The required diploma for level C is higher secondary education, while that of level B is short-cycle higher education. Subject to succeeding in a comparative selection for promotion to a higher level, a protection assistant may be promoted to level B.

77 This position, which made up around two-thirds of the workforce in 2012, did not previously exist.

third of the workforce) have been transferred from the Close Protection Service to reinforce State Security's intelligence sections.

II.4.5. FINDINGS

II.4.5.1. Performance or non-performance of the assignments

As stated, State Security carries out two types of protection assignments: 'permanent' and 'ad hoc' or 'official'.

The number of ad hoc assignments fluctuated over the years. The Committee found that a number of these assignments were not carried out. According to State Security, this applied to about one in every four assignments in the period 2010–2012. This number decreased, however. In 2012, depending on the source, the number of 'refusals' was between 4% (State Security) and 11% (Crisis Centre).[78] An important finding is that these assignments account for a rather limited part of the Close Protection Service's workload in practice: only one-fifth of the number of hours worked was spent on 'official assignments'.

Permanent assignments are always carried out.[79] These permanent assignments have a significant impact on the operations of the Service. The Standing Committee I recommended reassessing these permanent assignments to see whether they could be carried out differently, so as to use fewer resources (infra).

II.4.5.2. Protection Assistants versus Protection Officers

The workforce of the service is made up of Protection Assistants (level C) and Protection Officers at the level of inspector (level B). The Protection Assistants constitute more than two-thirds of the workforce. However, the demarcation of tasks between Protection Assistants and Protection Officers is less stringent than the job descriptions formally suggest (e.g. with reference to assuming or not assuming responsibility). The Committee stressed the need to ensure that this distinction does not lead to tension.

II.4.5.3. Overtime issue

'Compensatory leave' (i.e. leave granted when the hours worked, calculated over a four-month period, exceed the normal average length of a working week) and

78 The difference between the two relates to the points of reference used and the manner in which Articles 7 and 8 of the Intelligence Services Act are interpreted by both institutions.

79 It turns out that the persons to be protected were not always 'risk-aware' themselves, which sometimes caused problems for the performance of these assignments.

'compensatory rest' (granted, for example, when the maximum number of working hours in a day is exceeded) were a source of concern. The number of hours of compensatory leave and rest not taken is remarkably high. The Committee was able to establish that this increased by more than 44,000 hours between January 2010 and the end of December 2012. There has been a slight reduction since then: around 3,300 hours have been taken during the first three months of 2013, but the remaining total is still very high.

The decision to transfer inspectors from the Close Protection Service (supra) has had a particularly adverse effect on the number of overtime hours. The increase in personnel, and more specifically the hiring of Protection Assistants, clearly had no effect on the overtime issue. The impact of measures to bring this overtime issue under control (such as the sustained rationalisation of the teams, outsourcing to third parties, etc.) has proved to be (very) limited. Other measures (such as paying overtime or redefining or even cutting back on – particularly permanent – assignments) were considered but never materialised.

II.4.5.4. Formal escort assignments

'Formal escorting' – i.e. monitoring that State Security believes does not involve any associated threat, but where the VIP's status still requires official monitoring to be provided – is currently carried out with limited resources, linked to a private driver and limousine. The Standing Committee I was unable to conclude that the use of private drivers and limousines was favourable from a budgetary perspective, in fact the contrary applied. On the other hand, the Committee believed that there was a loss of quality at functional level and that the deployment of limited resources constituted a risk, both to the persons being protected and the State Security members themselves. The Standing Committee I therefore felt that an in-depth evaluation of this working method is warranted.

II.4.5.5. Removing inspectors from their intelligence assignments

Inspectors were previously removed from the Close Protection Service to reinforce intelligence sections. However, the reverse also happened: if there was too much work in the Close Protection Service, members of the intelligence sections (Field Services) of State Security were brought in to assist.[80] The Committee was able to establish that this practice has since decreased significantly: it happened only once in 2012. The Close Protection Service has not had to rely on members of the intelligence sections since 2013.

[80] This practice had its drawbacks: the performance of State Security's intelligence assignments was weakened as a result and members of the intelligence sections who normally have to act in complete discretion (contact with sources, shadowing, etc.) were put into the spotlight.

II.4.5.6. Defining threat levels

It is beyond the scope of the review investigation to express an opinion on how the various stakeholders (State Security, CUTA and the Crisis Centre) determine or interpret the threat levels.[81] However, it could be established that the specific application of the threat levels did not produce a consistent picture in the field. There was only a very loose connection between the resources deployed in the field and the formal threat levels set by CUTA.

II.4.5.7. Disinvestment in materials

Lastly, the Standing Committee I established a number of other – mainly material – problems in the performance of close protection assignments. The Standing Committee I recommends systematically remedying these issues and to involve people with adequate field knowledge who can thus come forward with practical solutions.

II.5. COMPLAINT OF THE CHURCH OF SCIENTOLOGY AGAINST STATE SECURITY

In March 2013, the non-profit association *Scientologykerk van België vzw/Église de scientologie de Belgique asbl* lodged a complaint with the Standing Committee I.[82] The complainant referred in this regard to newspaper reports in *La Dernière Heure*, *Het Laatste Nieuws* and *De Morgen* that were based on two leaked memoranda of State Security. One memorandum was entitled "*Church of Scientology – infiltration of the Congolese community (or of Congolese origin) in Belgium; presence in the Democratic Republic of Congo*" (free translation) and the other was entitled "*Phenomenon analysis of non-State-directed interference activities*" (free translation).[83] It was clear from the reports that State Security believed the Church of Scientology wanted to gain a foothold in the Democratic Republic of Congo and was looking for middlemen for that purpose in the Belgian-Congolese community. However, the religious movement also wanted to

---

81 In this regard, see: STANDING COMMITTEE I, *Activity Report 2012*, 40–42 (II.5 Joint investigation into CUTA's threat assessments relating to foreign VIP visits to Belgium).

82 The investigation that was opened on 14 April 2013 and whose final report was approved on 21 May 2014 was suspended for a long period because a similar investigation was running at the request of the Senate.

83 For more information about these two memoranda, see: STANDING COMMITTEE I, *Activity Report 2013*, 106–112 (II.2 Confidential memoranda on the Church of Scientology in the press).

lend support to the East-Congolese rebel group 'March 23 movement' (M23). The Church of Scientology asked the Committee three specific questions:

- *"to investigate whether the basis of this information is real and the manner in which the information has been disseminated to the public;*
- *to verify how this report was drawn up and how it was distributed;*
- *to determine whether that defamation impairs the fundamental rights conferred by the Constitution on the association that has lodged the complaints, more specifically the presumption of innocence" (free translation).*

Some of those questions were already answered in the investigation '*Confidential memoranda on the Church of Scientology in the press*' (free translation). In that report, the Committee reported extensively on the production and distribution of the classified memoranda. Those elements will therefore only be repeated briefly in this report.

II.5.1. MONITORING OF THE CHURCH OF SCIENTOLOGY BY STATE SECURITY

The Standing Committee I is aware that the monitoring of a religious movement by an intelligence service can give rise to certain concerns with respect to freedom of religion and association.

As a result of the review investigation, the Standing Committee I was of the option that when monitoring the Church of Scientology's activities in Belgium, State Security was acting within its statutory powers, pursuant to articles 7 and 8 of the Intelligence Services Act of 30 November 1998. Among the activities that threatens or could threaten the fundamental interests of the State, article 8 of the Intelligence Services Acts includes inter alia interference, harmful sectarian organisations and criminal organisations. The "*safety and the physical and moral protection of persons*" as well as the *"safety and protection of goods*" are interests included in article 8 under the notions of "*internal security of the State*" and of *"maintenance of democratic and constitutional order"* (free translation), like the safety and maintenance of the State, the rule of law and the democratic institutions.

In an earlier investigation on the monitoring of harmful sectarian organisations by State Security[84], the Standing Committee I had already concluded that:

- the criteria used to determine harmfulness in view of analysing the schemes of a religious movement and describing it as 'sectarian' and 'harmful' were

[84] See a summary of this review investigation in STANDING COMMITTEE I, *Activity report 2010*, 19.

relevant and referred to the fundamental principles set out in the Constitution, laws and international conventions on the protection of human rights;
– the selected priorities were also relevant to the severity of some threats noticed in Belgium;
– the identified threats concerned not only the exercise of individual freedom, health and physical integrity, but also the interference in the functioning of public authorities and the economy.

With regard to the Church of Scientology specifically, State Security put forward that the further aim of the sect is the conquest and totalitarian transformation of the world, and has thus concluded to the inadequacy of this aim with the democratic principles of our society.

Until 2007, State Security considered that the main threat posed by the Church of Scientology was a risk for the physical and/or psychological integrity of individuals that could lead to put their lives in danger. In 2008, State Security redefined the terms of its work on the Church of Scientology, considering that it should henceforth focus on the interference in the public authorities by the sect.

The Standing Committee I read the State Security's global analysis of the multiple approaches of interference by the Church of Scientology in the public authorities. However, the Committee determined that State Security's own observations had never identified '*illegal*' means used to approach political policymakers. On the other hand, State Security has a number of indications which give rise to suspicion that '*fraudulent or clandestine means*' were used to this end.

The Standing Committee has therefore concluded that State Security legally monitored the activities of the *Scientologykerk van België vzw/Église de scientologie de Belgique asbl*, without infringing the rights conferred to the plaintiff by the Constitution and the law.

II.5.2. UNDERLYING INTELLIGENCE OF THE LEAKED MEMORANDA

The information from the two memoranda was gathered on the basis of different intelligence methods (including an analysis of open sources and testimony from former followers) by various departments within State Security. The Standing Committee I did not find any irregularities in this regard.

The information that was provided to the authorities was evaluated and analysed according to the rules.

The reports that the Committee examined were concise and contained mostly facts. The necessary reservations were made when certain data could not be confirmed.

The analysis related mainly to the ideology, practical organisation, activities and presence of the Church of Scientology.

II.5.3. DISSEMINATION OF THE TWO MEMORANDA AND THE PRESUMPTION OF INNOCENCE

The complainant was of the view that the press leaks were timed to coincide with the hearing of the criminal case against the Church of Scientology in the Council chamber. They argued that the intention was to cause damage to the organisation or at least cast it in a negative light. The complainant further pointed to the fact that State Security was appointed as a technical expert in the criminal case.

The Committee returned to its findings from the earlier investigation in relation to this aspect of the complaint.[85] It therefore concluded that its investigation into the dissemination and leaking of the memoranda had not revealed any decisive information that could be used as a basis on which to hold State Security liable.

II.6. INFORMATION POSITION OF THE INTELLIGENCE SERVICES AND CUTA IN RELATION TO A TRAINEE PILOT

Among other things, reference was made in a review investigation of the Standing Committee P into '*information flows at airports*'[86] to a person who had been able to attend pilot training at a Belgian airport, despite indications of radicalisation in his past. Since this example could point to inadequate exchange of information among the relevant public authorities, it was decided in June 2013 to initiate a joint investigation '*on the information position and monitoring by the support services of CUTA – including into the assessment of the threat by CUTA – regarding a private individual X who was admitted to attend an aeroplane pilot course in Belgium*' (free translation).[87, 88]

---

85 STANDING COMMITTEE I, *Activity Report 2013*, 106–112.

86 www.comitep.be/AdditionalReports/2012–06–12_NL_informatiestromen_luchthavens.pdf ('Operational information flows at airports') (free translation).

87 The results of the investigation in relation to the section on 'police' are stated only briefly in this report. For more detailed information, the Standing Committee I refers to the publications of the Standing Committee P.

88 As a result of the discussion of this investigation in the Monitoring Committee of the Chamber of Representatives, it was decided in 2015 to explore one aspect in more detail in a new investigation '*into the determination – by CUTA – of the level of the threat posed by and to an individual, and into the consequences that such a threat level has in relation to the division of duties, measures, information flow, practical implications for a citizen and monitoring*' (free translation).

The trainee pilot concerned, a foreigner who had arrived in Belgium in the early 1990s, first came under State Security's radar at the time of his application for naturalisation at the end of the 1990s.[89] The service was in possession of information indicating that he was a member of a specific organisation and had received aeronautical training. The man confirmed this information during a discussion with State Security agents. He also explained that his refusal to participate in certain 'actions' of that organisation, which were aimed at another State, had led to him seeking refuge in Belgium. He maintained that membership of the organisation had been his only chance to access education. State Security found these explanations to be plausible.

In the same year, the individual concerned applied for a job as a maintenance technician at Brussels Airport. The State Security post at the airport was asked to investigate further. However, that investigation did not lead to any concrete results.

The man only attracted the attention of the security services again in March 2006, when according to the Brussels Airport aviation police, he acted aggressively – under the influence of a radical imam – and was possibly radicalised. State Security was advised. They met with the man a second time but this also produced nothing of note. It did turn out, however, that he was visiting a mosque which was known to State Security.

State Security received information again in November 2007, this time from the Ostend-Wevelgem airport police: the man was taking flying lessons with a view to obtaining a private pilot's licence. He seemed to be in a great hurry to get his licence and paid his lessons in cash, which could have been problematic in view of the police information from March 2006. However, State Security still had no specific information pointing to a tendency towards radicalisation.[90]

Nonetheless, the security services (police, State Security, GISS and CUTA) started regularly exchanging information from that time. GISS received information about the individual for the first time. However, the service did not initiate an investigation, despite having stated that it was paying special attention to trainee pilots after the 9/11 terrorist attacks.

At the request of the Ostend-Wevelgem airport police, a coordination meeting about the individual was held in December 2007. This meeting was attended by various police forces and the two intelligence services. State Security and GISS could not add any new information.

After the meeting, the DJP/Terro was of the opinion that there was no reason to refuse the individual's security pass, which gave him access to Wevelgem

89 State Security did not keep a copy of the opinion that it issued in 1998 as part of the naturalisation procedure. For more information in this regard, also see: STANDING COMMITTEE I, *Activity Report 2012*, 11–20 (II.1 State Security's role in relation to the procedures for obtaining Belgian nationality).

90 State Security did not investigate the funds used to finance the flying lessons. In view of the lack of evidence on radicalisation, such an investigation was deemed to be disproportionate.

Airport. It was however decided to issue an alert about the individual on the basis of the Schengen Agreement and to request a threat assessment from CUTA.

CUTA's assessment was completed in mid-December 2007.[91] It set the threat at level 2.[92, 93] When asked, CUTA explained to the Committees that it had never received any concrete information to give rise to a suspicion that the individual would carry out terrorist activity. The only worrying elements were his past history at a specific organisation, his flying lessons and a (temporary) change in behaviour. Threat level 3, which represents '*a possible and likely threat*', was therefore not justified in this case. Even so, CUTA did advise all services to remain vigilant, to permanently monitor the individual's situation and to pay attention to any changes in his behaviour that could point to radicalisation. In case of a level 2 threat, CUTA does not actively monitor the case file itself but leaves this up to the competent services, without specifically designating a 'pilot service'. CUTA only actively monitors itself from a level 3 threat assessment. Nonetheless, the Committees had to conclude that it was not clear to the different support services involved, who had to assume responsibility for coordination or precisely what the requested monitoring entailed. It was also not always possible for a support service that was not involved in the threat assessment from the outset to know whether or not CUTA had asked for permanent monitoring.

At the start of 2008, there were a number of additional meetings with the security services and information was regularly exchanged. In April 2008, State Security even drafted an internal summary memorandum about the threat that the individual could pose. The service once again concluded that it had no negative information.

New police information in mid-November 2008 indicated that the individual had acted strangely at the airport after returning from holiday. A new coordination meeting was convened. Shortly afterwards, State Security decided to speak to the man for a third time. His employer was also questioned this time. Once again, there proved to be no elements pointing to radicalisation.

State Security received a few more memoranda from the police between 2009 and 2011. In June 2010, State Security drafted another report stating that the individual had obtained his private pilot licence and wanted to train as a commercial pilot.[94] However, he was no longer systematically monitored by State Security.

---

91 Although both the Immigration Office (IO) and the FPS Mobility, i.e. two support services of CUTA, were requested to provide additional information, CUTA did not receive any further information that could point to an enhanced threat level.

92 "*Level 2 or AVERAGE is attributed if it is clear that the threat against the person, the group or the event that is the subject of the assessment is not very plausible*" (Art. 11, §6, 2 of the Threat Assessment Decree) (free translation).

93 CUTA noted that there were no elements that pointed to the individual having a radicalising effect on others. In that sense, he did not fall under the Radicalism Action Plan.

94 The individual has not possessed a valid licence since May 2012 and thus may no longer fly aeroplanes.

II.7. INVESTIGATION INTO THE INFORMATION PROVIDED BY STATE SECURITY AS PART OF A NATURALISATION DOSSIER

A Public Prosecutor opposed the granting of Belgian nationality to a private individual, referring to information from State Security regarding "*important facts inherent to the person*" (free translation). However, the individual concerned believed there had been a misunderstanding. At the end of July 2013, the man filed a complaint with the Standing Committee I.[95] The Committee opened a review investigation, which was completed in February 2014.

II.7.1. COMPLAINT

The complainant was of the opinion that he was the victim of an infringement of his individual rights by State Security. After all, it transpired from the opinion of the Public Prosecutor that he was known to State Security because of his active involvement in a movement that appears on the European list of terrorist organisations, as well as his '*suspected involvement*' (free translation) in activities such as extortion, bribery of officials, money laundering and financing of terrorism with counterfeit money.

The complainant argued that the above reasons were completely unfounded and described them as '*very offensive, degrading and defamatory*' (free translation). He maintained that none of the facts communicated by State Security to the Public Prosecutor were substantiated by concrete information. The complainant also referred to his clean criminal record.

II.7.2. FINDINGS

After investigating, the Committee concluded that there was indeed a problem in this case with the assessment, processing and communication of information by State Security to the judicial authorities.

The complainant was first noted by State Security in 2009. At that time, State Security received intelligence that indicated he was a militant of a certain terrorist organisation. The intelligence also mentioned his involvement in

95 The complainant also approached the Data Protection Commission, in May 2013, in order to gain access to the personal data processed by State Security. In accordance with Article 13, 3° of the Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data (Privacy Act), the Commission informed the complainant that the necessary verifications had been carried out. The individual also requested that the case be brought before the Court of First Instance. This resulted in his dossier being submitted to the Chamber of Representatives as a naturalisation application.

various forms of trafficking with illicit groups and money laundering. However, this information came from a single source. Further investigation was thus carried out.

Pursuant to Article 29 BCCP, State Security briefed the Public Prosecutor and Federal Prosecutor on all rather vague and unconfirmed information at the start of 2010. Since State Security was not entrusted with any expertise assignment, it inferred from this that no judicial inquiry had been opened as a result of this briefing.

When the complainant submitted his application for Belgian nationality in December 2012, State Security sent the same information (which had not been updated) to the Public Prosecutor's Office without reservation. Based on this, the Public Prosecutor issued a negative opinion on the nationality application.

By failing to update the information on the complainant, State Security acted lightly, and had adversely affected the complainant's chances of acquiring Belgian nationality.

As a result of the complaint that the aggrieved party lodged with the Standing Committee I, State Security adjusted its position and the information was updated. Taking this newly collected intelligence into consideration, State Security believed that the complainant must be regarded as '*not known as unfavourable by State Security*' (free translation). State Security undertook to notify the competent Public Prosecutor thereof.

II.8. COMPLAINT ABOUT HOW STATE SECURITY MONITORS THE MANAGER OF A BELGIAN EXPORT COMPANY

The manager of a company lodged a complaint with the Committee in mid-2013.[96] Since 2010, certain members of State Security had apparently approached him regularly with questions about customer lists, suppliers and their banking details. This company is a broker, acting as a middleman or intermediary in the sale or export of products.[97] This case involved what are known as '*dual-use products*', in other words "*items, including software and technology, which can be used for both civil and military purposes, including all goods which can be used for both non-explosive uses and assisting in any way in the manufacture of nuclear weapons or other nuclear explosive devices*" (free translation).[98]

---

96 The investigation was opened on 3 October 2013 and the final report was sent to the Monitoring Committee on 12 September 2014.

97 A broker can assume various roles, making it difficult to gain a clear-cut understanding of its operations. The broker sometimes also acts as an intermediary between two legal entities that are established abroad, so the traded products are never transported via Belgium.

98 Council Regulation (EC) No 1334/2000 of 22 June 2000 setting up a Community regime for the control of exports of dual-use items and technology.

The complainant said that contact with State Security became increasingly strained, and that he even felt intimidated and threatened. He also feared that information he had to provide would end up with third parties and wondered whether there was an obligation to cooperate with the intelligence service.

II.8.1. ACCOUNT OF THE FACTS

When the Customs and Excise Administration (C&E) carried out a routine inspection in 2010, it encountered an attempt by the above company to export embargoed goods. A substantial amount was paid as an out-of-court settlement and the company escaped prosecution.

However, State Security was informed of the case by the Strategic Goods Control Unit (SGCU), which oversees the activities of such companies in Flanders and maintains regular contact with the intelligence service. Thereupon, State Security opened a case file. Subsequent contact with the two authorities concerned (C&E and SGCU) revealed that other 'incidents'[99] had occurred in the past. The company was possibly not adhering to the applicable rules. Foreign correspondents also referred to suspicious conduct and contact between the company and foreign business partners.

State Security also made direct contact with the company and visited its premises a total of twelve times between 2010 and 2013 to request information.

II.8.2. FINDINGS

II.8.2.1. Powers of State Security

The activities of the above company could be linked to proliferation, one of State Security's key assignments (Article 8 of the Intelligence Services Act). In accordance with the action plan in force at the time, this threat also warranted 'active priority monitoring'.[100] In view of the indications provided by third-party

[99] Both administrations had repeated contact with the company, which seemingly had problems with document management and regulations. Several consultations were arranged with the SGCU to assist the company with regard to legislation, sanctions, the need to supply technical information, etc. The Customs and Excise Administration in turn made appointments with the company to conduct a full customs audit, but the company did not keep these appointments.

[100] United Nations reports moreover show that the proliferation of CBRN weapons must be regarded as one of the most significant threats. The fight against proliferation is fundamental in both national and international security policy. State Security has an important role in this regard. The Standing Committee I has previously discussed State Security's proliferation-related activity: STANDING COMMITTEE I, *Activity Report 2008*, 43-57; *Activity Report 2011*, 129–132, and; *Activity Report 2013*, 127–130.

services, State Security would have been in serious breach of its duties if it had not acted.

The company's complaint – namely that State Security was unlawfully monitoring it – is thus unfounded: State Security's actions were not random but were based on important indications and the service remained within its scope of competence. There is moreover no indication that State Security's assessment of the case was hasty or indiscriminate.

II.8.2.2. Direct contact with the complainant

State Security opted rather quickly to make direct contact with the company involved. It assumed that the established irregularities were not intended to intentionally contravene the export restrictions, but were rather the acts of a small company that was trying to survive financially and was possibly unaware of the scope of its actions. State Security thus correctly chose an ordinary intelligence collection method, namely approaching the party involved directly.

The questions that State Security asked in relation to customers and banking details were justifiable and fell within its scope of competence. In view of the circumstances of the case, this constitutes an adequate and proportional intelligence method.[101] Such information may be collected from any private person or organisation (Article 16 of the Intelligence Services Act). However, the party involved is bound by any professional secrecy that it is subject to and the statutory requirements on the protection of privacy. Both regulations impose restrictions on the disclosure of information to third parties.

The complaint relating to the intimidating attitude of a member of State Security could not be assessed on the basis of State Security documents and, when expressly questioned about this, the members of State Security denied that they had acted in an intimidating manner. The Committee found that it was no longer possible to determine the true state of affairs in retrospect, but stressed that intimidation is obviously not permissible.

The Committee lastly emphasised that a citizen is entitled not to cooperate in an intelligence investigation.

II.8.2.3. Complexity of the fight against proliferation

The Standing Committee I established in the margins of the investigation that proliferation is a very complex and unclear issue, both for the companies dealing with it and the services that have a role to play in this regard.

---

[101] In theory, it would also be possible to use exceptional SIM methods to obtain banking details or communication with customers since the case related to the fight against proliferation. However, the use of exceptional methods was not necessary in this case.

An adequate monitoring and sanctions scheme moreover is still lacking. Although State Security obviously does not have to monitor or sanction, this does mean that the problems in terms of competence between the Federal State and the Regions[102] in this regard, are not conducive to the operations of the services involved, and thus also not for State Security, which must be able to obtain useful information from these services.

In the conclusions of the review investigation into '*the role of the intelligence services within the framework of the fight against the proliferation of non-conventional and very advanced weapons*' (free translation) of 2008, the Standing Committee I already pointed out that the detection of transactions involving proliferation and the catch-all clause[103] are difficult for various reasons. These include the multiplicity of transactions to 'proliferation countries', the issue of dual-use goods, the lack of reliable and transparent data that is provided by the companies, and the complexity of the coding of goods by customs services .[104]

By means of this investigation, the Standing Committee I was able to establish that the above problems have not yet been resolved, which complicates State Security's activities in this regard.

II.9. WAS A PRIVATE INDIVIDUAL MONITORED BY THE INTELLIGENCE SERVICES?

A complaint was submitted to the Standing Committee I at the end of November 2013. The complainant, who has been domiciled in Belgium since 1994 and is a Belgian national, was convinced that he was under surveillance and was being shadowed by 'the intelligence services'. He saw several possible reasons for this, including being a member of a certain religious, Islamic movement. The complainant was under the impression that his telephone calls and e-mail traffic were being intercepted. This was apparently happening both in Belgium and his country of origin.

---

102 It is clear from a parliamentary question addressed to the Minister-President of the Flemish government about structural cooperation among the SGCU, State Security and C&E that this has not yet been finalised. A cooperation agreement was concluded in 2007 between the Federal State and the three Regions on import, export and transit, as well as dual-use products and technologies and the granting of permits in this regard. However, this agreement only related to the FPS Foreign Affairs and the Regions, and not to the FPS Economy, State Security and C&E: Flemish Parliament: Question no. 1159 of Mr ROEGIERS of 1 April 2014.

103 Which goods are military and must thus be monitored has been determined at international level and recorded in production lists. However, various countries also have a clause in their legislation that allows products which are not on the list for security reasons to still be placed under permits, e.g. because they are used for military purposes. This is the 'catch all' clause.

104 STANDING COMMITTEE I, *Activity Report 2008*, 42–57, in particular p. 55–57.

The Committee opened a review investigation into this at the start of February 2014: was the individual concerned actually known to State Security and GISS? If so, since when and in what context? Were special intelligence methods being used? What intelligence had been gathered about him? Etc. The Committee obviously did not have jurisdiction to investigate any role of foreign intelligence services.

The review investigation was completed in mid-May 2014. It showed that the Belgian intelligence services had not carried out any unlawful acts with regard to the complainant.

II.10. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2014 AND INVESTIGATIONS INITIATED IN 2014

This section contains a list and brief description of all investigations opened in 2014 and those investigations that were continued during the operating year 2014 but could not yet be completed.

II.10.1. MONITORING EXTREMIST ELEMENTS IN THE ARMY

As a result of briefings given by GISS, the Standing Committee I took note of the problem of military staff moving within extremist circles and military staff who are members or sympathisers of motorcycle gangs. During the same period, the media reported on the temporary presence of a militant jihadist in the Battalion of Ardennes hunters, who apparently drafted combat manuals with the experience gained there.

The Committee decided to open a review investigation into '*the detection and monitoring by GISS of extremist elements among the personnel of Defence and the Armed Forces*' (free translation). The investigation aims to examine whether GISS is tackling this problem efficiently and whether the service is also respecting citizens' rights in this regard.

The regulations on the verification or the so-called vetting of candidate members of Defence were amended during the course of the investigation. It was decided to expand the investigation to include this issue so the focus would be on two processes: the screening process during the recruitment phase and the detection process and monitoring of radical or extremist elements that had already been recruited.

During 2014, additional information was requested, inter alia, from the Appeal Body for security clearances, certificates and advice and other

investigative actions were carried out. It was also decided to supplement the provisional results of the investigation with information about the Syrian issue.[105]

II.10.2. HOW THE SPECIAL FUNDS ARE MANAGED, USED AND AUDITED

In 2011–2012, two criminal investigations were started into the possible misuse of funds intended for the payment of informants. The Investigation Service I was engaged in both investigations in view of its judicial mandate.[106] As the information in the Standing Committee I's possession pointed to possible structural problems, it was decided at the beginning of September 2012 to open a themed investigation into '*the manner of managing, spending and auditing funds intended for the payment of State Security and GISS informants*' (free translation).

However, in view of the current criminal investigations, the review investigation was immediately suspended. It was decided that the investigation could resume again at the end of March 2014. The report will be finalised in 2015.

II.10.3. INVESTIGATION INTO THE JOINT INFORMATION BOX

According to the initiators, the creation of what is known as a Joint Information Box (JIB) – approved by the Ministerial Committee for Intelligence and Security – formed the spearhead of the Radicalism Action Plan. This is a work file that was managed within CUTA, inter alia for the purpose of structurally collecting intelligence on entities that are monitored as part of the Radicalism Action Plan.

It was decided in a joint meeting of the Standing Committees P and I in mid-November 2012 to open an investigation into how '*CUTA manages, assesses and distributes the information contained in the Joint Information Box (JIB), in accordance with the implementation of the Radicalism Action Plan*' (free translation).

In 2014, both the Investigation Services P and I carried out various investigative acts. The report was finalised in April 2015 and sent to the

105 In March 2015, the Minister of Defence announced to the Defence Commission that two radicalised former soldiers were fighting in Syria.

106 STANDING COMMITTEE I, *Activiteitenverslag 2013*, 99–100 (Chapter VI. Criminal investigations and judicial inquiries).

Chairman of the Monitoring Committee and the Ministers of Justice and the Interior.

II.10.4. INTELLIGENCE AGENTS AND SOCIAL MEDIA

At the end of 2012, the media reported on the profiles of intelligence service employees on social networking sites such as Facebook and LinkedIn. What was then the Monitoring Committee of the Senate requested the Standing Committee I to open an investigation into '*the extent of the phenomenon by which employees of State Security, as well as possibly GISS and CUTA, disclose their capacity as agents of those institutions on the internet via social media*' (free translation). The Committee also had to investigate the potential risks of such disclosure and the extent to which countermeasures could and should be adopted.

In December 2012 the Standing Committee I commenced its investigation into the employees of GISS and State Security. Various investigative acts were carried out. The final report was completed in the first half of 2015.

II.10.5. PERSONNEL OF CUTA AND SOCIAL MEDIA

A joint investigation with the Standing Committee P was also opened in 2013 concerning CUTA employees and their presence on social networking sites. After all, in accordance with Article 56, 6° of the Review Act, external supervision of the operations of CUTA is conducted by both Committees jointly.

The final report was approved in March 2015 at the joint meeting of the Standing Committees I and P and sent to the Monitoring Committee of the Chamber of Representatives.

II.10.6. INTERNATIONAL CONTACTS OF CUTA

One of the assignments of the Coordination Unit for Threat Assessment is to maintain contact with 'similar foreign or international services' (Article 8, 3° of the Threat Assessment Act). In their joint meeting in early May 2013, the Standing Committees I and P decided to investigate how CUTA carries out that assignment.[107] All the parties involved were extensively questioned and additional investigative acts were carried out in 2014.

[107] 'Joint investigation into how CUTA maintains international relationships with similar foreign or international services pursuant to Article 8, 3° of the Threat Assessment Act of 10 July 2006' (free translation).

II.10.7. PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL AND THE SNOWDEN REVELATIONS

The revelations of Edward Snowden gave an insight into top secret programmes, mainly of the US National Security Agency (NSA). These revelations resulted in many parliamentary, judicial and intelligence investigations throughout the world, including in Belgium. The Standing Committee I opened four investigations, which are obviously closely connected with each other.

Three of the four investigations were completed in 2014 (see II.1, II.2 and II.3). The last review investigation[108], which has not yet been finalised, deals with the possible implications of these foreign programmes on the protection of the scientific and economic potential of the country. The aim of this investigation is to check whether the Belgian intelligence services:

- have paid attention to this phenomenon;
- have detected any real or potential threats to the Belgian scientific and economic potential;
- have notified the competent authorities and proposed protection measures; and
- have sufficient and adequate resources to monitor this problem.

The report will be completed in the course of 2015.

II.10.8. WRONGFULLY MONITORED BY THE INTELLIGENCE SERVICES?

At the end of February 2014, a person of North African origin lodged a complaint with the Standing Committee I. The individual, who has lived with his family in Belgium since May 2012, complained that he was being monitored in an 'oppressive way' by the intelligence services. The complainant alleged that he had no idea why he would attract attention. He had never had any problems in his country of origin or in the Asian country where he had worked for several years. He had no criminal record or links to terrorism or radicalism. He moreover stated that he was the target of monitoring operations, a feeling that was strengthened by the unusual treatment he received twice at Brussels Airport.

---

108 'Investigation into the attention that Belgian intelligence services pay (or do not pay) to potential threats to the Belgian scientific and economic potential originating from large-scale electronic surveillance programs on communication and IT systems used by foreign countries and/or intelligence services'.

In July 2014, the Committee decided to open an investigation in order to determine whether the complainant had actually attracted the attention of State Security or GISS and, if so, with what results.

Various investigative acts were carried out and the final report was sent to the Chairman of the Monitoring Committee and the Ministers of Justice and Defence in February 2015.

II.10.9. STATE SECURITY AND THE APPLICATION OF THE WORK RULES

In mid-2014, the Committee decided to open an investigation into '*how State Security interprets and implements the work rules, in particular the rules on sick leave*'(free translation). The reason was a complaint by a protection assistant at State Security's close protection services. The individual concerned, who was suspended and alleges to have suffered financial damage (leave of absence without pay) and administrative damage (delay in career), also identified other problems: the management of overtime, the vague legal framework in relation to the work rules, the rules on sick leave, preventive medicine, etc.

In February 2015, the Committee's final report was sent to the Minister of Justice and the Chairman of the Monitoring Committee.

II.10.10. ISSUE OF FOREIGN FIGHTERS AND THEIR CONTINGENT IN SYRIA

Since 2013, the Syrian conflict has been a magnet for foreign fighters from all over the world. Relatively speaking, a large number of those fighters are from Belgium.

The Standing Committee I therefore decided to open an investigation in October 2014 into '*the information position of the two intelligence services (GISS and State Security) regarding the recruitment, mission, stay and return to Belgium of young adults (Belgian and other nationals living in Belgium) who are leaving or who have left to Syria or Iraq and the exchange of intelligence with various authorities*' (free translation). Various topics came up for discussion: what mandate do the Belgian intelligence services have in this regard and how was/is it managed? Do the intelligence services have any insight into the recruitment and departure phase? Do they have an idea of the composition of these fighters in Syria? Are they aware of the activities that these fighters are developing locally? Are developments abroad being translated into possible domestic threats? If so, which threats? What about monitoring and the approach upon their return? How are the relevant services (GISS, State Security, CUTA and the police) cooperating in this regard? How is this being reported on and to whom?

At the start of March 2015, a first interim report was discussed in the Monitoring Committee of the Chamber of Representatives responsible for monitoring the Standing Committees P and I. A second report will be submitted before the 2015 summer recess.

II.10.11. STATE SECURITY AND THE COOPERATION PROTOCOL WITH PENAL INSTITUTIONS

A review investigation was opened on 1 October 2014 into how State Security implements the '*protocol agreement governing cooperation between State Security and the Directorate-General for the Execution of Penalties and Disciplinary Measures*' (free translation). Two prior investigations were the direct reason for this investigation.[109] The aim is to assess whether the agreement is being efficiently implemented, whether State Security is able to extract useful information for its assignments and, in the margins, whether the exchange of information on detainees is in accordance with the protection of the rights of individuals guaranteed by the Constitution and the law.

The investigation will be completed in 2015.

II.10.12. WRONGFUL FORWARDING OF INTELLIGENCE BY GISS

A private individual lodged a complaint with the Standing Committee I at the start of October 2014. The complainant alleged that he had been dismissed for urgent cause on the basis of information that his employer had received from an employee of GISS. The Committee decided to open an investigation at the end of October 2014.

The investigation had to clarify how GISS had handled the case file, whether the service had complied with the applicable legislation and whether intelligence had indeed been passed to a third party. The investigation was completed in June 2015.

---

109 STANDING COMMITTEE I, *Activity Report 2011*, 114–117 (II.3 Information position and actions of the intelligence services with regard to Lors Doukaev) and *Activity Report 2012*, 33–38 (II.3. Possible monitoring of an individual during and after detention in Belgium).

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS 2014

Article 35 §1, 1 of the Review Act stipulates that the Committee must pay specific attention in its annual Activity Report '*to the specific and exceptional intelligence collection methods, as referred to in Article 18, 2° of the Act of the Intelligence and Security Services Act of 30 November 1998 [and] to the application of Chapter IV(2) of the same Act*'[110] (free translation). This chapter therefore deals with the use of special intelligence methods by both intelligence services and the manner in which the Standing Committee I performs its jurisdictional role in this matter. It provides a brief summary of the two half-yearly reports drawn up by the Committee for the Monitoring Committee.[111]

III.1. BACKGROUND: THE 'SIM WORKING GROUP'

A 'SIM Working Group' was established in April 2014 by the two intelligence services, the SIM Commission and the Investigation Service of the Standing Committee I. This working group met four times in 2014 on the following topics: the latest jurisprudence of both the Commission and the Committee; an explanation of legal and operational ad hoc questions (e.g. the terms of the urgency procedure); the presentation and clarification of a specific case; and lastly, the specific details of a certain SIM-related topic (e.g. best practices for motivating the extension of a method in use). These meetings promote good relations and communication between the partners. These informal consultations obviously do not affect the independence of the Standing Committee I's assessment of the legality of the methods.

---

110 For an analysis on the special intelligence methods and on the manner in which they are monitored, please refer to: STANDING COMMITTEE I, *Activity Report 2010*, 51–63 and W. VAN LAETHEM, D. VAN DAELE and B. VANGEEBERGEN (eds.), De Wet op de bijzondere inlichtingenmethoden (Special Intelligence Methods Act), Antwerp, Intersentia, 2010, 299 p.

111 Articles 35 §2 and 66*bis* §2, third paragraph, of the Review Act.

III.2. FIGURES WITH REGARD TO THE SPECIFIC AND EXCEPTIONAL METHODS

Between 1 January and 31 December 2014, a combined total of 1,282 authorisations were granted by the two intelligence services for the use of special intelligence methods: 1,132 by State Security (of which 976 specific and 156 exceptional) and 150 by GISS (of which 114 specific and 36 exceptional).

The following table draws a comparison with the figures of previous years. It must also be noted that the Committee has been applying a different counting method for one specific method since January 2013. Previously, the number of 'Inspections of identification data of electronic communications' was only referred to in the footnote and not included separately in the totals. This was previously opted for because the heads of the intelligence services allowed (most of the) 'Inspections of identification data' in the same document as, for example, 'Inspections of call data' or 'Inspections of localisation data'. However, since this relates to different methods, strictly speaking, the Standing Committee I considered that including such 'Inspections of identification data' separately would provide a more accurate picture of the actual number of specific methods used. In other words, if the stated number of special methods since 2013 is higher than for previous years, this is largely due to a different counting method and not because these methods have been used more frequently.

	GISS		State Security		TOTAL
	Specific method	Exceptional method	Specific method	Exceptional method	
2012	67	24	655	102	848
2013	131	23	1102	122	1378
2014	114	36	976	156	1282

Although an increase of around 13% was noted in 2013 (taking the new counting method into account), the total number of special intelligence methods decreased by 7% in 2014. This decrease related to the specific methods for both services; by contrast, there was an increase in the use of exceptional methods.

Three major categories are distinguished for each service below: specific methods, exceptional methods, and the interests and threats justifying the use of these methods.

III.2.1. AUTHORISATIONS WITH REGARD TO GISS

III.2.1.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2012	NUMBER 2013	NUMBER 2014
Entry into and surveillance of or in places accessible to the public, using a technical device	8	14	7
Entry into and searching of places accessible to the public, using a technical device	0	0	0
Inspection of identification data of postal traffic and requesting the cooperation of a postal operator	0	0	0
Inspection of identification data of electronic communications, requesting the cooperation of an operator, or direct access to data files	25 dossiers	66 methods[112]	67
Inspection of call data for electronic communications and requesting the cooperation of an operator	30	15	12
Inspection of localisation data of electronic communications and requesting the cooperation of an operator	4	36	28
TOTAL	**67**[113]	**131**[114]	**114**

Whereas GISS had noted an increase in the number of surveillances and localisations in the previous year, these methods were used less frequently in 2014.

II.2.1.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2012	NUMBER 2013	NUMBER 2014
Entry into and surveillance in places not accessible to the public, with or without a technical device	1	1	1
Entry into and searching of places not accessible to the public, with or without a technical device	0	0	1
Setting up and using a fictitious legal person	0	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	0	0	0

112 A decrease can be noted compared to previous years, as the 66 authorisations relate to 16 dossiers.

113 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

114 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

NATURE OF EXCEPTIONAL METHOD	NUMBER 2012	NUMBER 2013	NUMBER 2014
Collecting data on bank accounts and banking transactions	7	5	5
Penetrating an IT system	2	0	3
Monitoring, intercepting and recording communications	14	17	26
TOTAL	**24**[115]	**23**[116]	**36**

In relation to exceptional methods, one figure stands out: the number of tapping measures has increased from 17 to 26.

III.2.1.3. Interests and threats justifying the use of special methods[117]

GISS may use specific and exceptional methods in respect of three of its assignments, each of which is related to the safeguarding of specific interests:

- the intelligence assignment focused on threats against the inviolability of the national territory, the military defence plans, and the scientific and economic potential in the area of defence (Article 11, 1° of the Intelligence Services Act);
- the military security assignment focused, for example, on preserving the military security of defence personnel, military installations, and military IT and network systems (Article 11, 2° of the Intelligence Services Act);
- the protection of military secrets (Article 11, 3° of the Intelligence Services Act).

NATURE OF INTEREST	NUMBER 2012	NUMBER 2013	NUMBER 2014
Intelligence assignment	63	111	109
Military security	7	15	5
Protection of secrets	21	28	36

NATURE OF THREAT	NUMBER 2012	NUMBER 2013	NUMBER 2014
Espionage	78	94	123
Terrorism (and radicalisation process)	3	6	7
Extremism	3	24	15
Interference	2	1	0
Criminal organisation	1	16	2
Other	5	13	0

115 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

116 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

117 Each authorisation may involve multiple interests and threats.

In relation to GISS, the threat of 'espionage' still requires the most frequent use of SIM methods. The rather limited use of SIM methods in the context of 'terrorism' and 'extremism' is noteworthy (22 in 2014, as compared to still 53 in 2013).

III.2.2. AUTHORISATIONS WITH REGARD TO STATE SECURITY

III.2.2.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2012	NUMBER 2013	NUMBER 2014
Entry into and surveillance of or in places accessible to the public, using a technical device	75	109	86
Entry into and searching of places accessible to the public, using a technical device	1	0	0
Inspection of identification data of postal traffic and requesting the cooperation of a postal operator	2	0	0
Inspection of identification data of electronic communications, requesting the cooperation of an operator or direct access to data files	254 dossiers	613[118] methods	554 methods
Inspection of call data for electronic communications and requesting the cooperation of an operator	147	136	88
Inspection of localisation data of electronic communications and requesting the cooperation of an operator	176	244	248
TOTAL	655[118]	1102[119]	976

The slight reduction in the number of specific methods used by State Security is due to the fact that fewer specific 'Surveillances' (86 as compared to 109), fewer 'Inspections of identification data' (554 as compared to 613) and fewer 'Inspections of call data' (88 as compared to 136) were carried out. Only the number of 'Localisations' remained stable.

118 A decrease can be noted compared to previous years, as the 613 authorisations relate to 243 dossiers.

119 In seventeen cases, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist. In the previous year there were nine cases.

120 In nine cases, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist. In the previous year there were nine cases as well.

III.2.2.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2012	NUMBER 2013	NUMBER 2014
Entry into and surveillance in places not accessible to the public, with or without a technical device	8	6	9
Entry into and searching of places not accessible to the public, with or without a technical device	6	6	21
Setting up and using a fictitious legal person	0	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	12	6	18
Collecting data on bank accounts and banking transactions	16	11	8
Penetrating an IT system	10	12	18
Monitoring, intercepting and recording communications	50	81	86
TOTAL	**102**[121]	**122**[122]	**156**

The increase in the number of exceptional methods used was not fully attributable this year to the 'Tapping measures' (81 as compared to 86), but mainly to the 'Searches' (6 as compared to 21) and the 'Opening of post' (6 as compared to 18).

It should also be noted that the urgency procedure, in which only the Chairman of the SIM Commission is asked for advice, was used in 19 cases (as compared to 11 the previous year).

III.2.2.3. Interests and threats justifying the use of special methods

The following table lists the threats (and potential threats) for which State Security issued authorisations for the use of specific and exceptional methods. Of course, a single method may be directed against multiple threats. State Security may use specific methods in the context of all threats falling within its competence (Article 8 of the Intelligence Services Act). Exceptional methods may not be used in the context of extremism and interference. However, they are allowed in the context of the radicalisation process that precedes terrorism (Article 3, 15° of the Intelligence Services Act). The Act uses the following definitions (free translation):

121 In five cases, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

122 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

1. Espionage: seeking or providing information which is not accessible to the public and the maintenance of secret relationships which could prepare for or facilitate these activities;
2. Terrorism: the use of force against persons or material interests for ideological or political reasons with the aim of achieving its objectives by means of terror, intimidation or threats;

Radicalisation process: a process whereby an individual or a group of individuals is influenced in such a manner that this individual or group of individuals is mentally shaped or prepared to commit terrorist acts;

3. Extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or aims, regardless whether they are of a political, ideological, religious or philosophical nature, which in theory or in practice conflict with the principles of democracy or human rights, with the proper functioning of democratic institutions or with other foundations of the rule of law;
4. Proliferation: trafficking in or transactions with respect to materials, products, goods or know-how which can contribute to the production or the development of non-conventional and very advanced weapon systems. In this context, this refers to the development of nuclear, chemical and biological weapons programmes and the transmission systems associated with them, as well as the persons, structures and countries involved;
5. Harmful sectarian organisations: any group with a philosophical or religious purpose or one which appears to be such and which, in terms of its organisation or practices, carries out harmful illegal activities, causes harm to individuals or society, or violates human dignity;
6. Interference: an attempt to use illegal, fraudulent or clandestine means to influence decision-making processes;
7. Criminal organisations: any structured association of more than two people lasting over time, aiming to carry out criminal acts and offences by mutual agreement, in order to acquire direct or indirect benefits in terms of capability, where use is made of intimidation, threats, violence, trickery or corruption, or where commercial or other structures are used to conceal or facilitate the commission of offenses. This means the forms and structures of criminal organisations which have a substantial relationship to the activities referred to in the above threats, or which could have a destabilising impact at a political or socio-economic level.

NATURE OF THREAT	NUMBER 2012	NUMBER 2013	NUMBER 2014
Espionage	243	359	319
Terrorism (and radicalisation process)	288	580	499
Extremism	177	246	267
Proliferation	28	15	33

NATURE OF THREAT	NUMBER 2012	NUMBER 2013	NUMBER 2014
Harmful sectarian organisations	7	9	0
Interference	10	8	10
Criminal organisations	5	9	8

The above figures reveal no significant changes in relation to 2013: from the perspective of SIM methods, 'Terrorism' and 'Extremism' remain the priority for State Security. However, despite the Syrian issue, a slight decrease has been noted in the number of methods used for these threats (766 as compared to 826 in 2013). This can be explained partly by the fact that in the context of 'Terrorism' and 'Extremism', State Security focuses mainly on the fighters in Syria and less on other forms of extremism.

The competence of State Security is not determined merely by the nature of the threat. The service may take action only in order to safeguard certain interests:

- the internal security of the State and maintenance of democratic and constitutional order:
  a) the security of the institutions of the State and the protection of the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to every constitutional state, as well as human rights and fundamental freedoms;
  b) the safety and physical and moral protection of persons and the safety and protection of goods;
- the external security of the State and international relations: the protection of the inviolability of the national territory, the sovereignty and independence of the State, the interests of the countries with which Belgium is striving towards a common goal, and the international and other relationships which Belgium maintains with other States and international or supranational institutions;
- safeguarding of the key elements of the scientific or economic potential.

Bearing in mind that different interests may be at play for each authorisation, the figures for 2014 are as follows:

NATURE OF INTEREST	**NUMBER 2012**	**NUMBER 2013**	**NUMBER 2014**
Internal security of the State and maintenance of democratic and constitutional order	704	1177	1100
External security of the State and international relations	693	1160	1075
Safeguarding of the key elements of the scientific or economic potential	15	11	10

III.3. ACTIVITIES OF THE STANDING COMMITTEE I AS A JURISDICTIONAL BODY AND A PRE-JUDICIAL CONSULTING BODY

III.3.1. STATISTICS

This section deals with the activities of the Standing Committee I in relation to specific and exceptional intelligence methods. Attention will also be paid to the jurisdictional decisions made in this regard. However, it must firstly be stressed that the Committee subjects *all* authorisations to use special methods to a prima facie investigation, with a view to a referral or otherwise.

Article 43/4 of the Intelligence Services Act states that a referral to the Standing Committee I can be made in five ways:

- at its own initiative;
- at the request of the Data Protection Commission;
- as a result of a complaint from a citizen;
- by operation of law, whenever the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and has prohibited the use of the data;
- by operation of law, if the competent Minister has issued an authorisation based on Article 18, 10°, §3 of the Intelligence Services Act.

In addition, a referral may also be made to the Committee in its capacity as a pre-judicial consulting body (Article 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure). When requested, the Committee gives its opinion on the legitimacy of the use in a criminal case of intelligence acquired by means of specific or exceptional methods. The decision to ask for the Committee's opinion rests with the examining courts or criminal courts. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

METHOD OF REFERRAL	NUMBER 2012	NUMBER 2013	NUMBER 2014
1. At its own initiative	19	16	13[123]
2. Data Protection Commission	0	0	0
3. Complaint	0	0	0
4. Suspension by SIM Commission	17	5	5
5. Authorisation by Minister	2	2	1
6. Pre-judicial consulting body	0	0	0
TOTAL	**38**	**23**	**19**

[123] In two cases, the Committee's decision was only made in January 2015.

Once the referral has been made, the Committee may make various kinds of interim or final decisions. However, in two cases (1 and 2 below) a decision is made before the actual referral to the Committee.

1. Decision to declare the complaint to be null and void due to a procedural defect or the absence of a personal and legitimate interest (Article 43, 4°, first paragraph of the Intelligence Services Act);
2. Decision not to take any action with regard to a complaint that is manifestly unfounded (Article 43, 4°, first paragraph of the Intelligence Services Act);
3. Suspension of the disputed method pending a final decision (Article 43, 4°, last paragraph of the Intelligence Services Act);
4. Request for additional information from the SIM Commission (Article 43, 5°, §1, first to third paragraphs of the Intelligence Services Act);
5. Request for additional information from the relevant intelligence service (Article 43, 5°, §1, third paragraph of the Intelligence Services Act);
6. Investigation assignment for the Investigation Service I (Article 43, 5°, §2 of the Intelligence Services Act). Reference is made here to the large body of additional information that is collected by the Investigation Service I in a more informal manner before the actual referral and information that is collected at the Committee's request after the referral;
7. Hearing of the SIM Commission members (Article 43, 5°, §4, first paragraph of the Intelligence Services Act);
8. Hearing of the head of service or the members of the relevant intelligence service (Article 43, 5°, §4, first paragraph of the Intelligence Services Act);
9. Decision about secrets relating to an ongoing criminal investigation or judicial inquiry to which the members of the intelligence services are privy, after consultation with the competent magistrate (Article 43, 5°, §4, second paragraph of the Intelligence Services Act);
10. Decision of the Chairman of the Standing Committee I, after having heard the head of service, if the member of the intelligence service believes that he must maintain the confidentiality of the secret information to which he is privy because its disclosure would be prejudicial to the protection of sources, the protection of the privacy of third parties, or the performance of the assignments of the intelligence service (Article 43, 5°, §4, third paragraph of the Intelligence Services Act);
11. Discontinuation of a method if it is still in use or has been suspended by the SIM Commission and an order stating that the information obtained through this method may not be used and must be destroyed (Article 43, 6°, §1, first paragraph of the Intelligence Services Act);
12. Partial discontinuation of an authorised method. This refers to a situation in which, for example, the use of a method is limited in time, and not to the situation in which several methods have been approved in a single

authorisation by a head of service and the Committee discontinues only one of them.
13. Total or partial lifting of the suspension and ban imposed by the SIM Commission (Article 43, 6°, §1, first paragraph of the Intelligence Services Act). This means that the method authorised by the head of service was found to be (partially) legal, proportionate and subsidiary by the Committee.
14. No competence of the Standing Committee I;
15. Unfounded nature of the pending case and no discontinuation of the method;
16. Advice given as a pre-judicial consulting body (Articles 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure).

The Standing Committee I must deliver a final decision within one month of the day on which a referral has been made to it in a particular matter (Article 43, 4° of the Intelligence Services Act). This period was respected in all dossiers.

NATURE OF DECISION	2012	FINAL DECISION 2012	2013	FINAL DECISION 2013	2014	FINAL DECISION 2014
1. Invalid complaint	0		0		0	
2. Manifestly unfounded complaint	0		0		0	
3. Suspension of method	1		0		3	
4. Additional information from SIM Commission	0		0		0	
5. Additional information from intelligence service	6		0		1	
6. Investigation assignment of Investigation Service	11		50		54	
7. Hearing of SIM Commission members	0		0		0	
8. Hearing of intelligence service members	0		0		0	
9. Decision regarding investigation secrecy	0		0		0	
10. Sensitive information during hearing	0		0		0	

NATURE OF DECISION	2012	FINAL DECISION 2012	2013	FINAL DECISION 2013	2014	FINAL DECISION 2014
11. Discontinuation of method	4		9		3	
12. Partial discontinuation of method	18		5		10	
13. Lifting or partial lifting of ban imposed by SIM Commission	13	38	2[124]	23	0	17
14. No legal competence	0		0		0	
15. Lawful authorisation / No discontinuation of method / Unfounded	3		7		4	
16. Pre-judicial advice	0		0		0	

The Standing Committee I made 17 decisions in 2014, as compared to 23, 39 and 38 in 2013, 2012 and 2011 respectively. One of the reasons for this decrease is the fact that the SIM Commission suspends fewer methods (15 and 17 in 2011 and 2012 respectively). Furthermore, there is undoubtedly the fact that many legal issues have been once and for all clarified in case law over the last few years and subsequently implemented by the services.

III.3.2. DECISIONS

The 17 final decisions delivered by the Standing Committee I in 2014 are briefly presented below. The summaries have been stripped of all operational information. Only the information that is relevant to the legal issue have been included. In some cases, the Committee has had to refrain from explicitly including certain elements from the legal issue in order to safeguard the mandatory confidentiality.

The decisions have been divided into five categories:

– legal (procedural) requirements prior to the implementation of a method;
– justification for the authorisation;
– proportionality and subsidiarity requirements;

[124] The Standing Committee I in fact held that the suspension by the SIM Commission was devoid of purpose (see dossier 2013/1728).

- legality of the method in terms of the techniques applied, data collected, duration of the measure, and nature of the threat
- the consequences of an unlawful method or an unlawfully implemented method.

Where relevant, some decisions are included under several categories.

III.3.2.1. Legal (procedural) requirements prior to the implementation of a method

III.3.2.1.1. Prior notification to the SIM Commission

A specific method may be used only after notification of the authorisation is given to the SIM Commission. In dossier 2014/3291, the Commission was notified of an authorisation, while the method pursuant to that decision had started the day beforehand. The Commission therefore suspended the part of the method that occurred before the notification. The Committee confirmed the decision.

III.3.2.1.2. Mandatory information in the authorisation

The intelligence service wanted to search a hotel room that was hired by a target (dossier 2014/2898). However, the authorisation did not mention the name of the hotel and obviously also no room number. The intelligence service gave that information to the SIM Commission during the course of the same day, and added that it would inform the SIM Commission immediately if the target changed hotels. The Committee found this working method to be legal. Firstly, the law does not require that the decision '*must specify the name (and location) of a hotel or the number of the room to be inspected […]. However, considering that indications are that a hotel room is involved and not a building that serves as the home or place of residence of a person, it is essential to assess the observance of the principles of proportionality and subsidiarity*' (free translation). The Committee also found that the Chairman of the SIM Commission was immediately advised of the exact location.

III.3.2.1.3. Method relating to a possible journalist

The intelligence service wished to use a specific method for a person in respect of whom it '*could not be ruled out*' (free translation) that he was a journalist (dossier 2014/2723). The Committee decided that '*the absence of specific information relating to the identity of this person meant that it could not be verified whether or not the procedure envisaged in Article 18, 2°, §3 must be applied*' (free translation). The method was therefore unlawful.

III.3.2.2. Justification for the authorisation

III.3.2.2.1. Insufficiently accurate justification

In the above dossier (2014/2723), the intelligence service wanted to use four methods to identify a certain person, who was suspected of wanting to sell classified information to a third party who was in contact with a foreign intelligence service. But even after additional intelligence was collected, very little was known about the buyer and the seller, the nature of the information and the intention of the persons or services involved. This meant '*notwithstanding the confirmation that the threat actually existed, that it was difficult to concretely assess the nature of the real or potential threat against the interest to be protected; that the spirit and letter of the law require more precise indications than those set out in the decision*' (free translation).

III.3.2.2.2. Enhanced justification in case of a second extension

A draft authorisation for the use of an exceptional method must be submitted to the SIM Commission, which must issue an opinion within a period of four days. Since the SIM Commission was unable to issue an opinion within that period, the authorisation was granted by the competent minister on the basis of Article 18, 10°, §3, third paragraph of the Intelligence Services Act. The Committee found that this related to a second extension of an exceptional method. Whereas '*the special circumstances that necessitated the extension of the exceptional method for a second time with regard to the target were adequately set out in the authorisation granted by the minister; That these reasons adequately show the threat that the target poses as well as the subsidiarity and proportionality of the method used*' (free translation).

III.3.2.3. Proportionality and subsidiarity requirements

III.3.2.3.1. Waiting for the results of the first method

In 2014, the Standing Committee I intervened five times in cases in which the intelligence service had authorised methods without waiting for the result of an earlier method. This problem first came to the fore in dossier 2014/2744. An intelligence service wished to check the contacts that a target maintained in Belgium on the basis of electronic communication data. The intention was to first list who the target called and by whom the target was called. But the method also aimed to immediately locate all the target's contacts. However, the Committee held that at the time of its decision '*it is impossible to establish which telephone numbers will be the subject of subsequent localisation*' (free translation)

and so it was impossible to verify the subsidiarity and proportionality of the localisation of such unidentified telephone numbers.

The same problem occurred in dossiers 2014/2774 and 2014/2778. The intelligence service first wanted to examine the incoming and outgoing numbers of a target's mobile telephone. It would then proceed to identify all numbers '*insofar as this will be necessary for the investigation*' (free translation). Up to that point, there was no problem, but the services wanted to locate all the identified numbers '*in order to give us indications about their identity*' (free translation). The Committee repeated that '*it is impossible to establish which telephone numbers will be the subject of such localisation at this time. It is therefore impossible for the Committee to already assess the subsidiarity and proportionality of the localisation method for those as yet unidentified numbers*' (free translation).

In the fourth dossier (2014/3253), an intelligence service wanted to simultaneously authorise four methods with regard to a person: identification of the electronic means of communication, 'surveillance' of those devices, localisation of the data obtained in this way and identification of all persons involved. The Committee held that the service ought to have used the first method first because '*in the absence of information obtained by the requested method, it is impossible to assess whether the principles of proportionality and subsidiarity were observed or, in other words, the legality of the three other requested methods arising from the first method*' (free translation).

Lastly, in dossier 2014/3493, the Committee reiterated that different steps must be taken when one wants to know, on the one hand, which means of communication a target is using (Article 18, 7°, §2 of the Intelligence Services Act[125]) and, on the other hand, with whom the target had a telephone call at a specific time (Article 18/8, 1° – tracing call data of electronic communication devices from which or to which calls are being or have been sent – in conjunction with Article 18/7, 1° – identifying the subscriber or user of an electronic communications service or means of electronic communication). The Committee held that '*the second part of the method, based on Article 18, 8°, §1 does not currently comply with the requirement of proportionality and subsidiarity*' (free translation).

III.3.2.3.2. Failure to demonstrate necessity

The issue of proportionality was also raised in another case. The intelligence service wanted to urgently use an exceptional method, inter alia, on a means of communication with a specific telephone number (dossier 2014/3424). However, the day after the authorisation was granted on the basis of the oral assent, the intelligence service discovered that the number had been erroneously omitted

[125] The service concerned had wrongly based its authorisation on Article 18/7, 1° of the Intelligence Services Act.

from the authorisation. The number in question was sent to the SIM Commission on the same day, but a typing error meant that an incorrect number was supplied. The SIM Commission then proceeded with suspension. The Committee confirmed that decision, but on different grounds. After all, it was clear from the information collected that the need to apply an exceptional method to the number had not been demonstrated. The Committee therefore found that the method did not conform to the requirement of proportionality.

III.3.2.3.3. Subsidiarity

Subsidiarity was the only issue in dossier 2014/2908. The SIM Commission had suspended the authorisation to carry out camera surveillance because the intelligence service had failed to clarify which information, originating from a foreign service, had prompted it to carry out surveillance. The Committee also regarded the initial decision to be inadequately motivated. It requested additional information and was told '*there was no need to use a specific method for the surveillance of the person concerned; indeed, no technical device was required for the intended surveillance*' (free translation). An ordinary method therefore sufficed for the surveillance. In other words, as the decision to use a specific method did not comply with the requirement of subsidiarity, the Committee ordered the method to be discontinued.

III.3.2.4. Legality of the method in terms of the techniques applied, data collected, duration of the measure, and nature of the threat

III.3.2.4.1. Cooperation from foreign services

The Committee has already held that the Belgian intelligence services may also cooperate with foreign partner services in relation to special methods, on condition that the Belgian service retains actual control over the method used.[126] In dossier 2014/2723, the Committee pointed to the need for further directives from the Ministerial Committee for Intelligence and Security[127]: '*the absence of directives from the Ministerial Committee for Intelligence and Security with regard to the conditions for cooperating with foreign intelligence services makes it necessary for State Security to act independently and on a case-by-case basis*' (free translation). However this does not affect '*the need to guarantee cooperation between the Belgian and foreign intelligence services, particularly when actions are taken within Belgian territory*' (free translation).

---

126 See, for example, STANDING COMMITTEE I, *Activity report 2013*, 162 (III.3.2.4.1. Monitoring of the implementation of the SIM).

127 The Royal Decree of 21 June 1996 on the establishment of a Ministerial Committee for Intelligence and Security was replaced by the Royal Decree of 28 January 2015 on the establishment of a National Security Council (*BOJ* 30 January 2015).

III.3.2.4.2. The SIM Act and the Vienna Convention on Diplomatic Relations of 18 April 1961

The Standing Committee I made four decisions during the reference period (dossiers 2014/2758, 2014/3148, 2014/3306 and 2014/3488) in which the Vienna Convention of 1961 came up for discussion. The Committee cannot deal with the content of these decisions in this Activity Report as they had to be classified as 'secret'. However, the Committee does emphasise that the Vienna Convention also applies to the operations of the intelligence services, which must therefore observe certain boundaries, and that there is a need for clear directives by the National Security Council, partly in view of the political responsibility that may result from certain activities of the intelligence services.

III.3.2.5. The consequences of an unlawful method or an unlawfully implemented method

The SIM Commission had partially suspended a method (dossier 2014/2724). The authorisation from the head of the service showed that the intelligence service concerned wanted to identify the electronic communication of two persons who were not identifiable at that stage. However this was apparently based on an error. The service involved did not intend to use the method and the Committee confirmed the decision of the SIM Commission.

III.4. CONCLUSIONS

Based on the figures from operating year 2014, the Standing Committee I has drawn the following general conclusions:

- Whereas an increase of around 13% was noted in 2013, the number of special intelligence methods used by the intelligence services decreased by 7% in 2014. This decrease related to the specific methods for both services, as there was a slight increase in the use of exceptional methods.
- For GISS, the increase in the use of exceptional methods was due to the rising number of tapping measures (26 as compared to 17), even though this remains a limited number in absolute figures.
- For State Security, the increase in the use of exceptional methods in 2014 was not attributable to the tapping measures (86 as compared to 81), but to searches (21 as compared to 6) and the opening of post (18 as compared to 6).
- In relation to GISS, the threat of 'Espionage' still requires the most frequent use of SIM methods, while SIM operations at GISS are aimed mostly at the fight against 'Terrorism/Extremism'.

– It should also be noted that the urgency procedure, in which only the Chairman of the SIM Commission is asked for advice, was used in 19 cases (as compared to 11 the previous year).
– The Standing Committee I made 17 decisions in 2014, as compared to 23, 39 and 38 in 2013, 2012 and 2011 respectively. One of the reasons for this decrease is the fact that the SIM Commission suspends fewer methods (15 and 17 in 2011 and 2012 respectively). Many legal issues have also been clarified in the case law of the Standing Committee I and the SIM Commission.

CHAPTER IX
RECOMMENDATIONS 2014

Based on the investigations concluded in 2014 and the processed SIM dossiers, the Standing Committee I has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred to individuals by the Constitution and the law (IX.1), the coordination and efficiency of the intelligence services, CUTA and the supporting services (IX.2) and, finally, the optimisation of the review capabilities of the Standing Committee I (IX.3).

IX.1. RECOMMENDATIONS RELATED TO THE PROTECTION OF THE RIGHTS CONFERRED TO INDIVIDUALS BY THE CONSTITUTION AND THE LAW

IX.1.1. FOCUS ON MASSIVE DATA CAPTURING AND POLITICAL AND ECONOMIC ESPIONAGE[128]

Both intelligence services must pay attention to the risks that new technologies may pose in relation to massive data capturing and economic and political espionage, even if these originate from 'friendly countries'. Risk analyses need to be drawn up in this regard, with attention given to the presence of international institutions within Belgian territory.

As far as State Security and GISS are concerned, attention to this phenomenon is essential in order to build up a solid information position and become familiar with the capabilities and procedures of other services, not only to be able to inform the authorities or take countermeasures, where applicable, but also to assess their own collection techniques.

In relation to State Security, attention to massive data capturing is obviously essential because this phenomenon forms a real threat to at least two interests to be protected by law, i.e. fundamental rights and freedoms and the sovereignty of the State. A host of information is already available from open sources or can be

[128] This recommendation stems from the first investigation into the revelations of Edward Snowden (II.1. The Snowden revelations and the information position of the Belgian intelligence services).

requested from the military intelligence service. An overall picture of the phenomenon and the associated risks can be formed on the basis of those elements. This could be translated into a phenomenon analysis[129] that is sent to the relevant authorities at regular intervals. The general public and companies also need to be made aware of the problem, now more than ever.

IX.1.2. DIRECTIVES ON COOPERATION WITH FOREIGN SERVICES[130]

In 2012, State Security drew up a detailed 'Instruction for bilateral cooperation with correspondents'. The Standing Committee I regarded this directive as particularly valuable. It did point out, however, that certain options taken by State Security would need the support of the political decision-makers, i.e. the members of the (former) Ministerial Committee for Intelligence and Security. One of the main aspects of that cooperation (which intelligence may be communicated to foreign services?) was only briefly covered in that directive. The Standing Committee I therefore repeats[131] its recommendation to State Security to immediately send its directive – supplemented with more precise rules on the exchange of information – to the National Security Council as the successor of the Ministerial Committee for Intelligence and Security.

The same recommendation applies to GISS, certainly since the Standing Committee I has been able to establish that there is close cooperation with foreign SIGINT departments (e.g. the NSA). Following on from State Security, GISS is working on a similar memorandum with 'verifiable criteria' for the purpose of cooperation with foreign intelligence services (in the broad sense). This memorandum was to have been finalised during 2014. The Committee highlights the importance of such a directive for GISS because – after approval by the National Security Council as well – it can offer a legitimised framework for alliances that the military intelligence service has already entered into.

---

129 The Standing Committee I has previously referred to the strengths of what State Security calls a 'phenomenon analysis': "'*The phenomenon analysis reveals a current topic that falls within the areas of interest and the scope of the missions entrusted to an intelligence service and that represents a major political and societal challenge, both today and for the years to come. It aims to describe this problem both in terms of its historical origins and as regards its ideology, organisation, structure and activities. It identifies the risks and challenges and sets out a 'risk assessment' intended for our political leaders, the administrative authorities concerned and the judicial authorities who are also confronted with this issue*", according to State Security in its first phenomenon analysis (free translation). Partly because such analyses are intended for wider distribution, they are well-suited to the issue of data capturing.

130 This recommendation stems from the following two investigations: 'II.1. 'The Snowden revelations and the information position of the Belgian intelligence services' and II.3. Use in criminal cases of intelligence originating from massive data capturing by foreign services.'

131 STANDING COMMITTEE I, *Activity Report 2012*, 75.

The Committee moreover recommends that the directives for both State Security and GISS should coincide, insofar as possible. According to the Committee, GISS can therefore take inspiration from the following elements that State Security has included in its aforementioned instruction:

- factors that can burden cooperation should be taken into consideration (e.g. interference, conflicts of interest, respect for fundamental rights, etc.);
- the statutory mission itself should always be safeguarded, certainly in matters such as terrorism and extremism, which quickly take on a judicial dimension;
- cooperation with foreign services must be fully transparent and traceable (to enable review by the Standing Committee I, for example);
- the cooperation should be periodically assessed.

The Committee also recommends that the assessment of the cooperation on the basis of the criteria should take place effectively and at regular intervals. The Snowden revelations have highlighted the need for this.

Even so, the Standing Committee I wants to avoid any misunderstanding about the fact that it is convinced that the Belgian intelligence services must continue to invest in solid cooperation with foreign services at both a bilateral and multilateral level.

IX.1.3. NEED FOR POLITICAL COVER FOR ALLIANCES[132]

The Committee holds the view that there must be greater transparency from the intelligence services about existing bilateral or multilateral alliances, first and foremost with regard to the competent ministers. After all, commitments or choices may be made in such alliances that require political assessment and cover. In other words, the competent ministers must be adequately informed so they are always able to assume their political responsibility. It must also be noted that what is – or is not – 'politically relevant' can change over time.

IX.1.4. NEED FOR POLITICAL GUIDANCE BY THE NATIONAL SECURITY COUNCIL[133]

The former Ministerial Committee for Intelligence and Security (now the National Security Council) was established as the political body responsible for steering the intelligence activities. Its task, by means of directives, is to set out

[132] This recommendation stems from the first investigation into the Snowden revelations (II.1. The Snowden revelations and the information position of the Belgian intelligence services).

[133] Idem.

the general intelligence policy, set the priorities of both intelligence services, ensure coordination between the services and lay down rules for international cooperation and data exchange. However, the Ministerial Committee did not meet after the Snowden revelations.

The Committee considers it desirable for the new National Security Council and, by extension, the Strategic Committee and the Coordination Committee for Intelligence and Security, to assume their steering role – on the basis of information from the two intelligence services – with regard to the phenomenon of massive data capturing and political and economic espionage. The Committee believes that this would allow Belgium to (at least partly) fulfil its positive obligation under Article 8 ECHR to protect the privacy of its citizens.

The Committee also refers to the lack of (legally required) formal approval by the Ministerial Committee/National Security Council for the list of companies whose SEP GISS must protect, as drawn up at the end of 2012.

IX.1.5. CRITICAL ASSESSMENT OF RULES OF THE INTERNATIONAL INTELLIGENCE CULTURE[134]

In the first investigation following the Snowden revelations, the Standing Committee I referred to a recommendation included in the draft report of the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament: *'Calls on the Member States, including when represented by their intelligence agencies, to refrain from accepting data from third states which have been collected unlawfully and from allowing surveillance activities on their territory by third states' governments or agencies which are unlawful under national law or do not meet the legal safeguards enshrined in international or EU instruments, including the protection of human rights under the TEU, the ECHR and the EU Charter of Fundamental Rights'*. The Standing Committee I notes that practice shows that 'supplying intelligence services' usually keep their sources (and thus the origin of intelligence) secret and that the 'receiving services' accept this. This type of understanding is part of the international intelligence culture, just like the third-party service rule, the quid pro quo principle, and the requirements of confidentiality.

The Committee reiterated that this does not mean that it outrightly supports these principles, but they cannot be abruptly and unilaterally breached.

---

134 This recommendation stems from investigation 'II.3. Use in criminal cases of intelligence originating from massive data capturing by foreign services.'

The Standing Committee I recommends that the National Security Council should investigate within a reasonable time what measures can be taken in this regard.

IX.1.6. RESTRICTIONS ON THE COLLECTION OF INTELLIGENCE AMONG LEGAL AND NATURAL PERSONS[135]

State Security may collect information on the threats it is monitoring from any person or organisation in the private sector (Article 16 of the Intelligence Services Act). Yet the party involved also remains bound by any professional secrecy this person or organisation is subject to and the requirements of the Data Protection Act. Both regulations impose restrictions on the disclosure of information to third parties (such as State Security). A citizen is moreover entitled not to cooperate in an intelligence investigation. For this reason, the Standing Committee I recommends that members of State Security pay particular attention in their contact with private individuals to how their conduct is perceived by people who are unaccustomed to having contact with the service. Attention should also be paid in training to the correct treatment of the citizens with whom members of State Security come into contact.

IX.1.7. UPDATING OF AVAILABLE INFORMATION IN THE CONTEXT OF NATURALISATIONS[136]

The Committee recommends that information supplied by State Security in relation to the acquisition of Belgian nationality should be systematically updated if that information relates to '*important facts inherent to the person*' (free translation) and can thus form an indication against awarding Belgian nationality.

---

135 This recommendation stems from investigation 'II.8. Complaint about how State Security monitors the manager of a Belgian export company'.

136 This recommendation stems from investigation 'II.7. Investigation into information provided by State Security in the context of a naturalisation dossier'.

IX.2. RECOMMENDATIONS RELATED TO THE COORDINATION AND EFFICIENCY OF THE INTELLIGENCE SERVICES, CUTA, AND THE SUPPORT SERVICES

IX.2.1. DEALING WITH THE CONCEPT OF 'FRIENDLY SERVICES'[137]

Both State Security and GISS seem to be dealing 'more cautiously' with friendly services or services from friendly countries. Although the Committee can understand this to a point, it recommends that the Belgian intelligence services take *every* threat seriously, even if it originates from friendly services or services of friendly countries. The Standing Committee I concurs with State Security when it states it is more appropriate to talk about 'strategic partners' than 'friendly services'.

IX.2.2. CLOSER COOPERATION BETWEEN THE TWO INTELLIGENCE SERVICES[138]

The Committee concluded that State Security and GISS never exchanged information in the period before the Snowden revelations and subsequently have only exchanged limited information about the threats posed by massive data capturing and political and economic espionage. The Committee firstly refers to the statutory obligation of these services to exchange information (Article 19 of the Intelligence Services Act). The Committee also refers to the existence of a cooperation agreement between the services (Protocol Agreement of 12 November 2004) aimed at the spontaneous exchange of information that falls within the scope of competence of the other service. The procedures described in this Protocol Agreement should at least have been followed after the revelations to consolidate their respective information positions. The Committee refers in particular to the option included in the Protocol Agreement of establishing an 'ad hoc cooperation platform' within which joint analyses could be drawn up. The contrasting situation that came to light in the dossier concerned (namely that GISS had a relatively significant amount of information but was not competent to monitor massive data capturing before the revelations versus the fact that State Security was competent but had little specific information about the phenomenon) could have been resolved within such a platform.

---

137 This recommendation stems from the first investigation into the Snowden revelations (II.1. The Snowden revelations and the information position of the Belgian intelligence services).

138 Idem.

IX.2.3. INTERDEPARTMENTAL COOPERATION IN RELATION TO CYBER SECURITY, ICT SECURITY AND CYBER INTELLIGENCE[139]

Certain aspects of the Snowden revelations point to weaknesses in the IT network security systems of both private companies and public institutions. The Committee therefore emphatically repeats that more attention must be paid to cyber and ICT security (INFOSEC) and that these issues – which do not fall solely within the remit of the intelligence services – require interdepartmental cooperation. For example, there is a crucial role for the National Security Council to play in this matter.

The Committee also refers in this regard to the past approval of a draft decree by the Council of Ministers on 19 December 2013 for the establishment of a Centre for Cyber Security in Belgium at the Chancellery of the Prime Minister. This centre was officially established by means of the Royal Decree of 10 October 2014.

Additional resources were also allocated at the time to implement the cyber security strategy, as approved at the end of 2012. Some of these resources were intended for GISS so as to enable this service to increase its capacity and pay more attention to cyber intelligence. However, the Standing Committee I is convinced that cyber security and intelligence will require continued investment in the coming decades.

IX.2.4. ADVERSE CONSEQUENCES OF FRAGMENTATION AND SECRECY WITHIN GISS[140]

The fact that a very limited number of people within GISS have direct access to SIGINT, as well as the strict confidentiality that surrounds this issue, can have made it more difficult to form an overall picture of the SIGINT capacities and strategies of foreign countries. The Committee therefore believes that GISS must consider how to strike the right balance between need to know and need to share.

IX.2.5. TERRITORIAL SCOPE OF THE SIM ACT[141]

The territorial scope of application of the SIM Act must be explained in light of technological developments. Pending any legislative initiative, the Committee

139 Idem.
140 Idem.
141 Idem. In the same sense, STANDING COMMITTEE I, *Activity Report 2013*, 170.

interprets this arrangement, as a precaution, to mean that the SIM method may only be used for communications when the signal of the communication to be captured is on Belgian soil.

IX.2.6. EXPLANATION OF THE INT ARRANGEMENT[142]

The Belgian INT arrangement, which allows GISS to intercept foreign communications, was established when it was essentially radio signals that were being intercepted. There have been so many technological developments since then that this arrangement needs to be reviewed by the legislature. The revelations of Edward Snowden have confirmed this finding. Aspects that need to be examined as part of such a review are the extent to which interceptions must – or must not – be focused, the correct scope of the possibility to 'search' signals, the extent to which the annual Interception Plan needs to be detailed, the possibility of carrying out data mining in bulk information, and whether foreign SIGINT operations must be placed within a broader 'international mandate'.

IX.2.7. RECOMMENDATIONS WITH REGARD TO CLOSE PROTECTION

As part of its investigation into 'State Security and its close protection assignments'[143], the Standing Committee I identified several problems and formulated a number of specific recommendations, including:

- the ratio between the number of managers of the Close Protection Service and the number of staff members carrying out the work ('span-of-control') is very large. This does not create a workable situation.
- the Committee was able to conclude that some people who need protection are not always 'risk-aware'. Nonetheless, State Security, and thus ultimately the Belgian State, is accountable in case of an incident. Urgent diplomatic arrangements therefore have to be made with the foreign diplomats in this regard. The creation of such a model is not the sole responsibility of State Security, and possibly not even its responsibility in the first place. The Standing Committee I believes that it is for the political decision-makers (Interior, Foreign Affairs and Justice) to conduct an evaluation/re-evaluation (and thus reorientation) in the near future in this regard.

---

142 Idem. Also see Chapter IV. Monitoring the interception of communications broadcast abroad.

143 See Chapter II.4.

– the Standing Committee I recommends reassessing and examining the permanent protection assignments, as a priority, to see whether they could be carried out differently, so as to use fewer resources.
– the Standing Committee I recommends paying continued attention to eliminating overtime.
– the investigation showed that the specific application of the threat levels did not produce a consistent picture in the field. There was only a very loose connection between the resources deployed in the field and the threat levels set by CUTA. Therefore, the Standing Committee I recommends that the services involved should agree on a workable model or classification and then apply this consistently. In the opinion of the Standing Committee I, a classification that is based solely on 'threat' does not allow enough room for nuances. The Standing Committee I therefore concurs with the suggestion made by the governmental Crisis Centre to include the concepts of 'protection measures' versus 'precautionary measures' in the classification as a real threat will not exist in all cases. All VIPs are not directly threatened, for instance, but precautionary measures must still be taken to uphold Belgium's reputation as a host country. The attitude of the VIP to be protected should also be included in the model as a relevant factor or variable.

IX.2.8. BETTER SUBSTANTIATION OF THE INTERFERENCE BY THE CHURCH OF SCIENTOLOGY[144]

The Standing Committee I took note of State Security's overall analysis of the many forms of interference that the non-profit association *Scientologykerk van België vzw/Église de scientologie de Belgique asbl* practices in regard to the authorities. However, the Committee determined that State Security's own observations had never identified means that were 'illegal' and used by the movement to approach political policymakers. On the other hand, State Security has a number of indications which give rise to suspicion that '*fraudulent or clandestine means*' (free translation) were used. The Committee therefore made the recommendation that State Security would be better able to demonstrate the interference by this movement by giving structure to its analysis on the illegal, fraudulent and clandestine means being used to approach authorities and political policymakers in Belgium.

144 This recommendation stems from investigation 'II.5. Complaint by the Church of Scientology against State Security'.

IX.2.9. COOPERATION AGREEMENTS AGAINST PROLIFERATION[145]

In order to tackle proliferation more effectively, the Standing Committee I recommends that the various authorities enter into formal alliances. This is necessary due to the complex nature of the phenomenon, in terms of both its technical nature and regulations and jurisdiction. These cooperation agreements should be entered into between the federal and regional levels, on the one hand, as regards coordinating regulations and determining sanctions and, on the other hand, among all services that have any responsibility in the field for supervision and review.

IX.3. RECOMMENDATION RELATED TO THE EFFECTIVENESS OF THE REVIEW: STRICT APPLICATION OF ARTICLE 33 §2 OF THE REVIEW ACT[146]

In relation to its review role, the Standing Committee I refers once again[147] to the obligation under Article 33 of the Review Act to '*on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services*' (free translation). This obligation also applies to arrangements, MOUs or agreements entered into internationally, whether at a bilateral or multilateral level.

145 This recommendation stems from investigation 'II.8. Complaint about how State Security monitors the manager of a Belgian export company'.

146 This recommendation stems from the first investigation into the Snowden revelations (II.1. The Snowden revelations and the information position of the Belgian intelligence services).

147 An earlier investigation has already been conducted in this regard: STANDING COMMITTEE I, *Activiteitenverslag 1996*, 28–32 (Report on the application of Article 33, 2° of the Review Act by the intelligence services); *Activiteitenverslag 2001,* 218–220 (The essential information that Standing Committee I believes it needs for the due performance of its task); *Activiteitenverslag 2002,* 27 (The automatic provision of certain documents by intelligence services to Standing Committee I); *Activiteitenverslag 2006,* 12; *Activity Report 2013*, 172.

ACTIVITY REPORT 2015

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2015

Appendices

PREFACE – ACTIVITY REPORT 2015

A shooting at the head office of the French satirical weekly magazine 'Charlie Hebdo' in early January 2015 claimed the lives of twelve victims. A hostage situation, which developed almost simultaneously in a Paris supermarket, resulted in a further five deaths. The perpetrators were radicalised Muslims with ties to Islamic State (IS).

Just a few days later, there was a large anti-terror operation in Verviers, in which two returned Syria fighters were killed and a third was wounded. These events have since been followed by terrorist attacks and further attempts in Europe and the rest of the world. Shootings in the centre of the Danish capital on 14 and 15 February resulted in several fatalities and casualties. Two months later, a man was arrested in France for planning attacks on Paris churches. On 26 June, an employer was beheaded in the French region of Isère, while a few alert servicemen foiled an attack on the high-speed Thalys train on 21 August. Other terrorist acts happened outside Europe, with Tunisia being particularly hard hit.

Several deadly attacks took place in Paris on 13 November 2015. The death toll among the victims reached 130. These gruesome acts were perpetrated by returning foreign terrorist fighters. Fairly soon after the attacks, information emerged pointing to a close connection with Belgium.

The terror threat kept a firm hold over Belgium until the last second of 2015. For the second time in a few years, the New Year's Eve fireworks were cancelled[148] and the threat level was raised to level 4. However, this proved to be just a harbinger of things to come: Brussels, Istanbul, Nice, Munich…

The wave of attacks has obviously strongly shaped the Standing Committee I's agenda. Investigations were launched into the information position of the intelligence services and CUTA prior to the terrorist acts in Paris, Zaventem and Brussels.

However, the Committee had already started long before that with a number of investigations that examined certain aspects of the monitoring of radical Islamism. An initial investigation into this matter started even before the 9/11 attacks. But since 2012, the Committee has opened many specific investigations into this issue. Examples have included investigations into monitoring extremism in the army, paying particular attention to radical Islamism. And, in 2014, investigations were opened into the Joint Information Box (a list of

148 STANDING COMMITTEE I, *Activity Report 2008*, 9–22 ('II.1. The terror alarm around the turn of the year').

radicalised persons and groups) of CUTA, into the exchange of information between State Security and the prison system (focusing on intelligence relating to extremism and terrorists), as well as into the intelligence position of the intelligence services regarding foreign terrorist fighters and the failed attack on the high-speed Thalys train. The results of a number of these investigations are detailed in this annual report.

These same attacks have obviously also shaped the agenda of the Belgian government, which has taken numerous initiatives. Some of those initiatives have a direct impact on how the Standing Committee I operates. For instance, it was recently instructed – together with the Control Agency for Management of Police Information (COC) – to audit the new dynamic database for foreign terrorist fighters. The upcoming Passenger Name Record scheme also promises to be a new supervisory task for the Committee. The same applies to the monitoring of foreign interceptions by GISS, which may be expanded. Hence a thorough review of the Belgian Intelligence Act of 30 November 1998 is on the cards. Lastly, a sharp increase in the number of files for the Appeal Body for security clearances, certificates and advice cannot be ruled out. After all, an increasing number of more stringent security screenings are being performed.

In the battle against barbaric terrorism, into which our society has been plunged today, every player in the security chain must assume responsibility for their own actions and 'shift into a higher gear'. Likewise, the Standing Committee I will, where possible, continue making proposals for enhancing the efficiency of the intelligence and security services, while guaranteeing respect for fundamental rights, fundamental freedoms and the rule of law.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2016

CHAPTER II
REVIEW INVESTIGATIONS 2015

In 2015, the Standing Committee I finalised nine investigation reports. It also drew up two additional investigation reports at the request of the Monitoring Committee and an interim report at its own initiative.

The nine finalised investigations included two opened at its own initiative, two at the joint initiative of Standing Committees I and P (concerned with aspects of the operation of CUTA), three following complaints, and two at the request of the Parliamentary Monitoring Committee.

The nine final reports and the interim report (II.1 to II.10) will be discussed briefly below.

This will be followed by a summary and brief description of the investigations that are still ongoing (II.11). The eight investigations opened in 2015 are also referred to in this latter section. Six of these new investigations were started following a complaint, one officially at the Committee's own initiative, and one at the request of the Monitoring Committee.

The Committee received a total of 22 complaints or reports in 2015. After verifying some objective information, the Committee rejected 14 of these complaints or reports because they were manifestly unfounded (Article 34 of the Review Act) or because the Committee did not have jurisdiction for the matter in question. In the latter cases, the complainants were referred, wherever possible, to the competent authorities. The other eight complaints from 2015 resulted in the opening of seven different investigations.

II.1. JOINT SUPERVISORY INVESTIGATION INTO THE JOINT INFORMATION BOX OF CUTA

In September 2012, a press report referred to problems that had arisen with the Joint Information Box (JIB).[148] This was a list managed by CUTA containing the names of persons and organisations that had played a key role in the radicalisation process and against whom or which certain administrative or judicial measures could be adopted. It was thus not a list of radicalised persons,

[148] K. CLERIX, '*Sharia4Belgium helpt strijd tegen radicalisering*' (Sharia4Belgium helps in the fight against radicalisation), *MO* Magazine*, September 2012.

but of radicalising persons or groups. From 2006, entries on the list were determined by the National Task Force (NTF) that brings together representatives of the various services involved in the fight against radicalisation. According to the press release, there was not enough cooperation within the NFT for compiling and updating the JIB. The Standing Committees I and P then opened an investigation to determine whether this instrument effectively and efficiently contributed to the identification and knowledge of radicalising elements at all the authorities involved.[149] The Committees focused for this purpose on the JIB as it functioned from 2009 to 2014.[150]

II.1.1. THE CREATION OF THE JIB

The JIB was first established in 2005. As one of the outcomes of the Radicalism Action Plan (R Plan) of 2004, it offered an overview of radicalisation within Belgian society and of the administrative and judicial options for tackling the problem. Since the Action Plan was aimed at all forms of radicalism (Muslim extremism, the far left, the far right, and animal rights activism), it also applied to the JIB. Various 'axes' or channels used to radicalise, including radio, television, prisons, cultural centres, etc., were identified in the Radicalism Action Plan. The existence of those axes would also extend to the JIB.

The JIB was initially drawn up without any specific working arrangements.[151] The list was at first managed for a short period by State Security, and then by the Mixed Anti-Terrorist Group (ATG). In 2006, the ATG was transferred to CUTA and the coordination unit took over the management from that date.

When the National Task Force was established in 2006, its task was to '*assume responsibility for coordinating and monitoring intelligence gathering for the purpose of analysing this intelligence and deciding on whether or not it should be included in the JIB*' (free translation). However, real arrangements were made only in 2009.

Until then, the services tried to monitor the issues mentioned in the initial R Plan. However, in the absence of clear directives, they experienced many problems.

---

149 The investigation was opened on 13 November 2012 and finalised in April 2015.

150 During the course of the investigation, CUTA indicated that it would adjust the way in which the JIB functioned. A working group within CUTA put forward various proposals in this regard. However, the investigation was closed before the intended changes were implemented. The Standing Committees I and P established that there was a clear intention to consider a new work process. An attempt has already been made to address one of the shortcomings identified by the Committees (the absence of a clearly defined purpose of the JIB). CUTA did not raise any other aspects in its reaction at the time that called into question the Committees' findings.

151 The memorandum creating the JIB was to have established a number of substantive and functional working arrangements.

II.1.2. THE FUNCTIONING OF THE JIB FROM 2009 TO 2014

In 2009, the representatives of the services involved reached a formal agreement on the functioning of the JIB. However, an unambiguous vision regarding its purpose was not set out. Most of the players seized on this as a point of criticism, which could explain why there were different views on the scope of the persons or entities to be included.[152] It was also stated that the relationship with other lists (such as the action plans of the intelligence services, the list of 'groups to be monitored', and later the list of 'Syria fighters') was not always clear.

Since 2009, the inclusion or deletion of an entity to or from the list was subject to a clear procedure for which strict criteria (the 'parameters'[153]) were applied and for which consensus among all services involved was required.[154] All this meant that cooperation in the JIB was a rather formalistic and time-consuming activity.

The JIB would have worked around the following seven axes: 'Ideologies and preachers', 'Cultural centres and non-profit organisations', 'Propaganda centres', 'Internet and the web', 'Radio and television', 'Groups' and 'Prisons'. The members of the NTF were formally designated: CUTA, State Security, GISS, the Federal and Local Police, the Anti-Terrorism Unit of the FPS Foreign Affairs, the Governmental Coordination and Crisis Centre (GCCR) and the Federal Prosecutor's Office. Some of these services were designated as the 'pilot' of one or more axes.[155]

CUTA drew up a record for every entity on the list containing all[156] relevant information and the measures to be adopted. CUTA pointed out significant differences in the provision of information. The contribution by State Security was initially limited. The participants noted that serious debate was often lacking with regard to the measures to be adopted for an entity. Some services also noted that it was neither their task nor area of expertise to propose measures.

CUTA was responsible for drawing up and keeping the records.[157] However, this service did not regard itself tasked with enhancing the information provided by analysing it or requesting additional information. It made its contribution in

152 Two schools of thought therefore existed: those who wished to retain a limited JIB and those who wanted a far quicker process for adding entities.

153 For example, 'the call to use violence' was one of the parameters. The list of parameters was an attempt to implement necessary objectification and prevent the ill-considered inclusion of an entity. An entity had to fit within at least two parameters.

154 If no consensus was reached on inclusion after a debate, the Board for Intelligence and Security, as it was known at the time, was advised of this fact.

155 State Security was the 'pilot' of five axes.

156 Interestingly, a lot of information was included for some entities, with very little for others.

157 CUTA's duty to store JIB data is enshrined in Article 9, §§1 and 2 of the Threat Assessment Act.

a fairly minimalist way, despite its statutory mandate to prepare threat assessments on extremism.[158]

The services that cooperated in the JIB could not consult the list and the information therein directly. They initially received printed records or a CD-ROM with the current state of affairs via CUTA every six months (and subsequently more frequently).

II.1.3. THE CONTENT OF THE JIB IN 2014

The Standing Committees I and P had the content of the JIB list audited in September 2014. At that stage, the list contained the names of only 97 'entities', of which around two-thirds were persons and one-third was groups.[159]

Most of the entities were linked to the 'Propaganda centres' axis, followed by the 'Internet and the web' axis.

It transpired, in relation to the 'measures to be adopted' for the listed persons, that these were all the subject of an alert in the Schengen Information System.[160] Fourteen of these were also the subject of an alert in the National General Database (BNG/ANG); two people in the BNG/ANG were specifically flagged in relation to counterterrorism. The rest of the list mentioned only 'measures to be adopted'. It was not always clear to the Committee how the measures to be adopted would be able to curtail the radicalising character of a person.

The same findings applied to the groups included in the list. There was for the most part only one measure, namely 'inclusion on the list of groups to be monitored'. This list is managed by the Federal Police under the responsibility of the Minister of the Interior. The purpose of this list is to (be able to) monitor these entities very closely. As in the case for persons, the number of 'other measures' stated for groups was limited. According to the Committees, the added value of the JIB in the fight against radicalisation was also very limited in this regard.

II.1.4. GENERAL CONCLUSIONS OF THE STANDING COMMITTEES I AND P

The Committees found that cooperation among the various services can result in significant positive effects for the JIB. The services are thus encouraged to

158 See Article 8 of the Threat Assessment Act.

159 The Committees also noted that certain names, which could reasonably be assumed to belong in the JIB, were not entered on the list, while other names did not seem to be in keeping with the purpose of the list.

160 The purpose of these alerts is to be able to monitor the cross-border movements of a person within the Schengen area. However, most people were already the subject of an alert when they were included in the JIB.

meet each other in a regular and structured manner and to exchange operational information in the area of radicalisation. They are also encouraged to produce joint, concrete results, namely a list of radicalising elements and associated measures. However, the Committees felt that the manner in which the Joint Information Box functioned, despite being in operation for twelve years, contributed little to this. The JIB likewise offered scant added value in the fight against radicalisation.

The services experienced the operations as time-consuming and complex and found the required efforts to be disproportionate to the returns. This had various demonstrable causes.

Firstly, there was too much uncertainty about the exact purpose of the list. The Committees held the view that a list of persons and groups that have a radicalising effect on their environment and that should therefore be the target of coordinated administrative, police, and judicial measures, is valuable both for the security services and policymakers. This purpose ought to be unambiguously formulated and communicated to all players involved (whether at federal, community, or local level). Depending on this purpose, objective criteria should be defined to determine inclusion in or deletion from this list.

Secondly, the Committees found that the measures detailed within the JIB for the known vectors of radicalisation were marginal. The search for appropriate measures lagged too far behind. However, the Committees pointed out that the services already forming part of the JIB operations were not well-placed to propose a broad range of measures in certain cases, either because they did not have optimal knowledge of the possible measures or because they possibly were not responsible for their implementation.

II.2. MANAGEMENT, USE AND AUDIT OF 'SPECIAL FUNDS'

In 2011–2012, the judicial authorities started two criminal investigations into the possible misuse by intelligence agents of funds intended for the payment of informants.[161] Investigation Service I was engaged in both investigations, given its judicial assignment.[162] As the information in possession of the Standing Committee I pointed to possible structural problems, it was decided at the beginning of September 2012 to open a themed investigation into the manner of

[161] The first, which opened in 2011, related to possible financial embezzlement by GISS intelligence agents. This investigation was completed in 2013: the case was dismissed. The second investigation, which opened in 2012, related to possible financial embezzlement by a member of State Security. Investigation Service I completed this investigation in February 2014.

[162] STANDING COMMITTEE I, *Activity Report 2013*, 97–98 ('Chapter VI. Criminal investigations and judicial inquiries').

managing, spending, and auditing funds intended for the payment of State Security and GISS informants.[163]

However, in view of the current criminal investigations, the investigation was immediately suspended. The investigation resumed at the end of March 2014. The comprehensive final report was approved in June 2015.

II.2.1. PURPOSE OF THE INVESTIGATION

Like every public service, the intelligence services also receive State funding for the performance of their statutory tasks. The normal rule for spending this money is that there must be full transparency and auditing. However, because certain tasks of State Security and GISS are unforeseeable or must remain secret, a large portion of their budget escapes that 'normal rule'. That portion is better known as the 'special funds'. Although the amount of those funds form part of the budget allocated to the services, special rules apply to their management, use, and auditing.[164]

The term 'special funds' – which moreover has no statutory definition – is often thought to refer to money that is intended for paying informants. But these funds are also used for other purposes. The Committee therefore decided to include those other aspects in the investigation.

Contrary to other countries[165], there is no body specifically entrusted with auditing special funds in Belgium. In principle, auditing the proper spending of this portion of State funds falls under the authority of the Court of Audit. However, given the special and secret nature of these funds, this auditing is not really effective.[166] Nonetheless, there are specific reasons to support a solid auditing of how those funds are spent.[167]

---

163 The Standing Committee I had already investigated the budgets of State Security and GISS in 1994 (STANDING COMMITTEE I, *Activiteitenverslag 1995* (Activity Report 1995), 105–109). The investigation limited itself at the time to a description of the use of the funds, the amounts involved, management, and the audit procedures.

164 In terms of budgetary planning, the 'special funds' also differ from the other budgetary items of public services because the designated use of the funds does not have to be justified or described at the time of planning.

165 In France, for example, the *'Commission parlementaire de vérification des fonds spéciaux'* (Parliamentary Commission for Auditing Special Funds) was entrusted with this task.

166 The General Policy Director of the Minister of Justice audits the spending of State Security's special funds. Since 2006, only the Head of the Armed Forces audits GISS's special funds, four times a year. On the suggestion of the Court of Audit, since 2010 this has been done in the presence of the chairman of the Standing Committee I (STANDING COMMITTEE I, *Activiteitenverslag 2013* (Activity Report 2013), 95 and *Activiteitenverslag 2014* (Activity Report 2014), 96).

167 *'There are four main reasons why external oversight of intelligence service finance is important:*
– *the principles of democratic governance require the allocation and use of public funds to be closely scrutinized;*

The Committee investigated, inter alia, what constitutes 'special funds', the amounts involved, and how these are divided. It also checked how the resources are used and how these 'special funds' interact with 'normal' budgets. Lastly, the regulatory framework was studied to investigate what scrutiny mechanisms exist, both internally (within the services) and externally (Court of Audit, Inspectorate of Finance, Standing Committee I, etc.).

II.2.2. LEGAL FRAMEWORK

There is no act, royal or ministerial decree, ministerial circular, or directive[168] that defines the funds and lays down rules for their use and auditing. There is thus a statutory void.

However, the two services have issued their own directives on the use of the funds. Although the Committee regarded this as a positive development, these directives do not suffice to guarantee the appropriate use of the funds. More fundamentally, the Committee found that it was not the task of the services themselves to decide on the purpose and use of the funds and the audit procedures, obviously on the understanding that these services must enjoy autonomy in the operational use of the funds.

The Committee was able to conclude that the personnel of both intelligence services who were involved in the management of the funds were aware of these internal directives. However, this did not necessarily apply to the agents in the field, who only make occasional use of the special funds.

II.2.3. FINDINGS WITH REGARD TO GISS

Contrary to the position with State Security, special funds that are allocated to GISS are not detailed in the annual Budget Act that is voted on by Parliament. Even the overall operating budget of GISS (personnel, operating, and investment costs) is not included in this. Only the overall defence budget is stated. The

---

– *financial records can provide insights into the behaviour and performance of intelligence services;*
– *intelligence service secrecy limits the ability of the public to scrutinize service activity;*
– *the nature of intelligence work creates a variety of financial risks, including the risk of the misuse of public funds.*'

in A. WILLS, 'Financial Oversight in Intelligence Services', in *Overseeing Intelligence Services – a toolkit,* H. BORN and A. WILLS (eds.), DCAF, 2012 (www.dcaf.ch), 151–180.

168 Article 18 of the Intelligence Services Act stipulates that the services, during the performance of their duties, may make use of staff '*in accordance with the directives of the Ministerial Committee*' (now the National Security Council) (free translation). These directives would specifically have to relate to the management and purpose of the special funds. Such directives are lacking at present.

amounts that GISS ultimately receives for its normal funding and the 'special funds' are allocated by Defence's Directorate-General for Budget and Finance.

The Standing Committee I holds the view that the transparency of services benefits from the publication of both the overall GISS budget and that of the special funds, without giving details of operations, targets, methods used, etc.[169] The Committee points out that the publication of the amount of the funds allocated to GISS has never jeopardised the secret nature of its activities. The publication of these figures must allow Parliament to better assume its role of 'financial controller'.

As stated above, GISS has drawn up various internal directives for the management of funds. The basic directive clearly defines the conditions under which the funds can be used. There are also specific directives for the use of money from what are known as 'sub-funds'.[170] Some of these directives – such as those from the HUMINT sections – are very detailed; however, a similar arrangement is lacking for the other 'sub-funds'. The Committee has found shortcomings in relation to the organisation of these 'sub-funds'. The Committee was also not convinced of the added value of working with 'sub-funds'. These gave rise to confusion and significantly increased the risk of the non-compliant use of the allocated funds. The Committee established, for example, that some expenses did not meet the required criteria (e.g. the confidential or secret nature of the assignment and its urgency, as a result of which the normal procurement procedure could not be followed). Other expenses therefore had to be paid from other budgets and not the 'sub-funds' (e.g. the payment of regulatory remuneration to the civilian personnel of GISS). The Committee did find that some sections of GISS (such as the HUMINT or operational zone sections) need to be autonomous in order to carry out their assignments. The provision of cash is absolutely necessary for this purpose. But the Committee was in favour of centralised management for the other 'sub-funds'.

The Committee found that GISS did not use the accounting records for the management of funds as a control instrument at the time of the investigation. In other words, the accounting data did not serve to provide a more effective and efficient management of the service.

The Committee also noted that the formal requirements for the expense procedures were not recorded. As expenses were insufficiently documented, it could be difficult to determine during subsequent audits whether they complied with the directives. After all, it is important for this purpose to know the reason for the expense, which body made the procurement decision, and which body can confirm the validity of the expense.

It also transpired, in relation to the 'sub-funds', that the accounting software programs allowed retrospective editing. The Committee recommended that it

169 In the same context, see A. WILLS, *l.c.* 156 *et seq.*

170 The 'central fund' of GISS is subdivided into twenty 'sub-funds' for specific expenses.

should not be possible to alter accounting entries that had already been made. The Committee also established that some funds had developed their own accounting system that was incompatible with the central fund's accounting system.

A final finding by the Committee related to the payment of human sources, who did not sign any receipts for the payments they received. However, State Security staff did sign receipts.

II.2.4. FINDINGS WITH REGARD TO STATE SECURITY

As stated, the amount of the special funds that are allocated to State Security is visible in the budget of this service. That amount is stated under the item 'security measures' and in 2013 amounted to approximately € 1.5 million. State Security has set out clear and precise directives for its personnel in relation to the management of the budget.

Since 2014, State Security has made use of an 'electronic fund', which is accounting software for the funds. It is an efficient system because it allows the special accounting officer to permanently and directly audit the accounting records of the funds through the sections. The program registers the accounting entries in real time. As these entries cannot be subsequently changed, this is an important element in combating fraud.

The special accounting officer has an important function within State Security, in managing the funds and auditing their daily use. However, the Committee concluded that the funds were not optimally managed in the absence of the special accounting officer. The Committee was therefore of the opinion that it was essential to guarantee the continuity of this position. A replacement must therefore be arranged in his absence (which was not the case at the time of the investigation). In the context of the same concerns regarding continuity, the Committee found that it was necessary to describe the working procedures of the special accounting officer.

Lastly, the investigation showed that State Security had a limited amount of 'operating capital' in cash at its disposal. This 'legacy from the past' was probably accrued by transferring part of the surplus from the special funds each year. The Committee believed that the existence of such capital could constitute a legal problem: firstly because the annual surplus of the funds that was retained to increase this 'operating capital' was entered as an expense and, secondly, because State Security determined for itself which portion of that surplus would be retained each year, without any form of external audit. The Committee felt it was necessary for the legality of this 'operating capital' to be analysed in conjunction with the competent authorities (FPS Justice and the Court of Audit). The procedures and control measures by which State Security may retain the annual fund surpluses should also be recorded.

II.3. TRACKING DOWN AND MONITORING EXTREMIST ELEMENTS AMONG DEFENCE PERSONNEL

During the course of 2011–12, GISS gave various briefings to the Standing Committee I on the issue of military personnel with links to the far right and criminal motorcycle gangs. During the same period, press reports also appeared[171] regarding the presence of extremist and even jihadist militants in the Belgian Armed Forces. In June 2012, the Standing Committee I therefore decided to open a review investigation into GISS's approach to this problem.[172] The Committee approached the theme from five questions.

II.3.1. WHAT RULES IN RELATION TO FUNDAMENTAL FREEDOMS APPLY TO DEFENCE PERSONNEL?

All military and civilian Defence personnel enjoy constitutional rights like anyone else, more specifically the freedom of expression, of association, and of religion.[173] Different provisions relating to the status of military and civilian personnel do however stipulate that they must abide by the Constitution and laws and defend the moral and material interests of the State. Specific emphasis is laid on the dangers of membership of an 'organisation with a dubious reputation'. 'Extremism' as such is not forbidden, but specific acts or statements of an extremist ideology, both within and outside the professional context, can be punished because they are contrary to disciplinary, ethical, and military regulations.

II.3.2. WHAT POWERS DOES GISS HAVE IN THIS REGARD?

The legislature explicitly assigned the monitoring of extremist activities to State Security (Articles 7 and 8, 1° (c) of the Intelligence Services Act). However, that does not prevent GISS from legitimately monitoring military or civilian Defence personnel, at least insofar as they constitute a threat to the department or its

171 P. HUYBERECHTS, *Het Nieuwsblad*, 22 November 2012 ('*Leger vreest infiltratie door moslim-extremisten*' (Army fears infiltration by Muslim extremists)); A. LALLEMAND, *Le Soir*, 22 November 2012 ('*Des islamistes dans l'armée: 'L'État doit mieux se protéger*' (Islamists in the army: the State needs to protect itself better)).

172 The final investigation report was approved in November 2015.

173 For example, GISS took the view that Salafism – in the sense of a strict interpretation of Islam – falls under freedom of religion. Extremism and radicalism only exist if a believer rejects the rights and obligations that are recognised in international treaties and conventions, the Constitution, and national laws.

operations. After all, GISS has jurisdiction in respect of all threats against the interests it must protect. This monitoring thus falls within the scope of GISS's statutory mandate, namely to gather intelligence on activities that could threaten the Armed Forces' fulfilment of their tasks, the military security of the personnel and facilities, or even the protection of military secrets (Article 11 of the Intelligence Services Act).

GISS is also entrusted with carrying out security investigations for the purpose of granting security clearances to Defence personnel and security verifications for candidate military personnel.[174] These powers are also relevant to the fight against extremism within Defence (see below).

II.3.3. WHO DOES GISS REGARD AS EXTREMIST?

GISS has identified four extremist movements in its Intelligence Steering Plan, which it traces and monitors within Defence: radical Islamism, the far right, criminal motorcycle gangs[175] and the far left/ecopacifism. Only the first three movements are monitored as a priority and to an equal degree.

Statistics from GISS on the recent monitoring of these three phenomena have shown that a rather limited number of individuals[176, 177] are involved or, in one exceptional case, a small group of people. In the few cases cited in the media, this mainly involves former military personnel who have become the focus of attention after their military service because of their extremist statements and/or because they have gone to fight in Syria, driven by their radical Islamic convictions. However, on completion of the investigation, there was no known case of any military personnel in active service who would have taken such a step. There have already been military personnel in active service who had been criminally convicted for their membership of a far-right, terrorist group.[178] A

174 Article 9, 1° (9) of the Belgian Act of 28 February 2007 determining the status of military personnel of the active Armed Forces.

175 Strictly speaking, membership of a criminal motorcycle gang does not fall under the legal definition of 'extremism'. This does not mean that GISS cannot monitor this activity: such clubs are interested in the experience and technical knowledge of military personnel and the fact that they have access to weapons and other military material. In this sense, these clubs may constitute a threat to interests that GISS must protect (see II.3.2).

176 In the context of radical Islamism, some thirty people attracted the attention of GISS in 2010–12. Three of them were under strict monitoring because of their active religious proselytism within the Armed Forces. Another thirty cases were investigated in 2013–14. Thirteen military personnel were monitored to some degree. A further fifty cases were investigated in 2015 alone. Four people turned out to be actively involved in radical Islamism.

177 The following statistics were available for military personnel with far-right links: in 2006–07, some 76 active military personnel had probable ties to a far-right movement. No new cases were found between 2010 and 2012. The service investigated two cases in 2013 and 2014.

178 In 2014, fourteen members of the neo-Nazi group *Bloed, Bodem, Eer en Trouw,* including eleven military personnel, were convicted of racism and negationism. A number of the

limited number of people were also monitored because of their extremist beliefs (inspired by different ideologies), but no serious offences were established.

The Committee found that the extent of the problem of extremism within the Armed Forces generally remained limited and was no greater than extremism in similar population and age categories in civil society. Nonetheless, the Committee emphasised that this phenomenon must not be underestimated in view of the tasks entrusted to military personnel and the means at their disposal.

II.3.4. HOW DOES GISS MONITOR EXTREMIST ELEMENTS WITHIN DEFENCE?

Extremist military personnel are tracked down and monitored in different ways.

First, each candidate military personnel is subject to a security verification. According to the preparatory work of the Act, the purpose of this screening, which is carried out by GISS, is to eliminate candidates with an extremist and/or judicial past from the selection process.

Once recruited, many military personnel and members of the civilian personnel (especially those requiring a security clearance) are subject to a security investigation. This investigation – which is more in-depth than the verification and must be repeated at least once every five years – can also reveal extremism. The discovery of circumstances that can affect a person's reliability (such as extremist connections) can lead to the refusal or withdrawal of a security clearance.

Outside the context of security verifications and investigations, GISS relies on the units, chiefs of police, and the heads of services to detect and report suspicious acts.[179] The results of these sources of information vary depending on the quality of the personal contact that the GISS investigators have established with the unit commanders. For instance, the Committee concluded that in practice, relevant facts and security incidents are brought to the attention of GISS only once the person involved is subjected to a new security investigation and thus not at the moment the facts or incidents occur. The investigation of several specific cases has also shown that it would be useful for the personnel of

---

accused were also found guilty of terrorism, gang formation, and the illegal possession of weapons.

179 The directive on 'Membership of organisations with a poor or questionable reputation' of the Directorate-General for Human Resources requests all chiefs of police to inform GISS if they suspect a member of their personnel of activities that could endanger military security. In 2013–14, GISS ran a campaign to inform and make chiefs of police aware of the problem of motorcycle gangs with a questionable reputation. Meetings were held and a memorandum was distributed.

GISS and military units to have more precise indicators in order to recognise suspicious situations in good time.

In addition to 'internal' information, GISS also receives information and intelligence from other public authorities, specifically the police, judicial authorities, and State Security. However, this does not happen systematically.

Lastly, GISS can take the initiative to conduct an intelligence investigation if it receives notice of indications of suspicious behaviour. It should be pointed out that it is not permitted to systematically and generally verify all Defence personnel members, independently of any such indication.[180] The Committee stated that such a possibility also did not seem justified at the time of the investigation.

Although the Committee's investigation has shown that GISS performs its duties seriously in this regard, it concluded that the monitoring of extremism was not adequately documented and quantified. This could partly be explained by the involvement of several divisions and subdivisions. In order to be able to manage this problem in the best possible way, GISS must have a general and updated picture of the situation.

II.3.5. WHAT MEASURES CAN BE ADOPTED?

Based on a prior verification by GISS, candidate military personnel can be excluded from the selection procedure. It must also be noted that the number of candidate military personnel who are excluded due to extremism is very low. The most negative opinions are usually based on 'normal' criminality, such as the use of drugs.

People who do not obtain security clearance or whose clearance is withdrawn due to extremist activities do not lose their status as military or civilian personnel; they can only be barred from positions that require such a clearance. The data gathered as part of a security investigation may also not be used for other purposes (e.g. disciplinary cases).

It goes without saying that Defence employees who are guilty of criminal or disciplinary offences inspired by extremism can be suspended, transferred, dismissed, etc.[181] GISS does not bear any responsibility for these administrative and disciplinary measures; the service is also not always advised thereof.[182]

---

180 Such systematic and general screening is possible only as part of the recruitment procedure.

181 If a person is no longer a member of Defence, GISS will end the monitoring, unless he/she still maintains contact with former Defence colleagues.

182 For example, GISS stated that it had not received any feedback about the fact that Defence had dismissed four extremists in a given period. With regard to these dismissals, see: *Ann.* Chamber of Representatives 2012–13, 17 January 2013, CRIV53PLEN125, 1442–1444.

II.3.6. GENERAL CONCLUSION

The Standing Committee I concluded that GISS monitored extremism within National Defence correctly and fairly efficiently. The investigation showed that dangerous situations were discovered in time, and that very few or no cases have so far occurred of persons who had emerged unnoticed as dangerous extremists during their service. It appears as though anxiety about extremist military personnel or persons that follow military training because of extremist convictions is less well-founded that certain media would have implied.

II.4. THE MONITORING OF SYRIA FIGHTERS BY THE TWO INTELLIGENCE SERVICES: AN INTERIM REPORT

Since 2013, the Syrian conflict has been a magnet for foreign terrorist fighters (FTF)[183] from all over the world. Relatively speaking, a large number of those people came from Belgium. The Standing Committee I therefore decided in October 2014 (thus before the 2015 attacks in France and Belgium) to open an investigation into '*the information position of the two intelligence services (GISS and State Security) regarding the recruitment, mission, stay and return to Belgium of young adults (Belgian and other nationals living in Belgium) who are leaving or who have left for Syria or Iraq and the exchange of intelligence with various authorities*' (free translation).[184] The investigation had to answer the following questions: how are intelligence services monitoring the problem, how are they organised, and what is their information position? The investigation covered the period from 2012 – after all, that is when the first reports of 'returnees' (fighters who returned to their country of origin) emerged – until 2015.

At the start of 2015, a first, interim report was drawn up for the Monitoring Committee. The preliminary conclusions of that report are set out below.[185]

The Committee wishes to point out that the challenges faced by the Belgian intelligence services in this regard are very substantial. Obviously these services

---

183 Initially, no reference was made to FTF. Reference was made to Belgian freedom fighters (who left for Iraq, Syria, etc. for humanitarian purposes) or – later – to Belgian foreign fighters (with military objectives).

184 The Standing Committee I had already investigated similar matters before. In 1999, there was an investigation into how the intelligence services monitored a threat from within the Armed Islamic Group (GIA) (STANDING COMMITTEE I, *Activiteitenverslag 2001* (Activity Report 2001), 89 *et seq.*). And in 2007, the monitoring of radical Islamism by the intelligence services was explained (STANDING COMMITTEE I, *Activiteitenverslag 2007* (Activity Report 2007), 9 *et seq.*). Among other things, attention was paid to State Security and GISS monitoring of the *filières* whose aim was to recruit jihadi fighters for 'sensitive zones' (Afghanistan, Pakistan, Iraq, etc.).

185 The investigation was completed in February 2016.

also had to respond to certain 'crises' in the past as well. But the real impact on their organisation in those cases was limited. The current phenomenon is of a different nature: it is particularly complex, the threat has developed at unprecedented speed, an exceptionally large number of people are involved, and it has spread almost worldwide.

II.4.1. THE GEOPOLITICAL CONTEXT AND THE PRIORITIES OF STATE SECURITY AND GISS

From December 2010, there was a wave of protests, uprising, and revolutions throughout the Arab world; the 'Arab Spring' had begun. There were revolutions in Tunisia, Egypt, Libya, and Yemen, a civil war in Syria, demonstrations and protests in Bahrain, Jordan, Morocco, Algeria, Iraq, Oman, and the Palestinian territories, and occasional protests in Mauritania, Saudi Arabia, Sudan, Lebanon, and Kuwait. The causes differed from country to country: oppression, unfair elections, corruption, price increases, lack of political freedom, and unemployment. Time and again, the incumbent governments were held accountable.

The region has long been a theatre of violence, particularly Iraq where the organisation 'Islamic State in Iraq' has operated since October 2006, and also interfered in the Syrian civil war. This organisation later adopted the names 'Islamic State in Iraq and Syria' (ISIS) and 'Islamic State in Iraq and the Levant' (ISIL). In June 2014, Abu Bakr al-Baghdadi claimed that he had established a new worldwide caliphate, thereby assuming both religious and civilian power. The terrorist movement has since been known as Islamic State (IS) or DAESH.

Many of the young adults who left Belgium and other countries for Syria and Iraq joined IS; others chose different armed groups to fight against the regime of the Syrian president Assad or that were involved in conflicts against each other.

The existence and operation of these '*filières*' from within Belgium to conflict areas abroad was not a new phenomenon for State Security. Since 2001, the service's attention had already been drawn to the problem of Iraqi and Afghan *filières*.[186] For example, State Security had to deal with the *Mujahideen* who went to Afghanistan to participate in paramilitary training or fighting. The problem of these people returning and the danger of them creating networks in Belgium was also recognised at the time of the Iraq crisis. In 2005–2006, these *filières* were one of the priorities of State Security. The problem continued to be monitored in the years that followed. Although State Security was already aware of the *filières* from Belgium to foreign theatres of war, this did not mean it could predict their movement to Syria becoming a top priority in 2011. During that year, State Security did pay attention to the growing uprisings in Syria in its

186 STANDING COMMITTEE I, *Activity Report 2007*, 92–93.

Activity Report, but noted in regard to the *filières* that *'the prospective European fighters who are about to leave, […] will focus on conflict areas, more specifically Somalia and Yemen'* (free translation). Furthermore, *'even if Belgium is normally not directly threatened, the territory is still regarded as a transit area […]. The passage of Islamic radicals arranged via Belgium can be explained by different factors, including […] the presence of networks that falsify documents, but also the geographically central location of our country in Europe, and the availability of low-cost airlines'* (free translation). In mid-2012, the service reported the first case of a returnee and the problem was raised as such for the first time in the 2013 Action Plan. The Syrian problem has since obviously featured far more prominently in the Action Plans of this service.

GISS has also been familiar with the *filières* phenomenon for some time, although the service declared in 2007 that it had not paid special attention to the movement of people to sensitive zones (Pakistan and Afghanistan) due to a lack of personnel and input. According to the service, it did not perform any systematic checks on the phenomenon, but did receive information from abroad from time to time.

There are two steering plans at GISS in which annual priorities are recorded. The steering plan of the Security Intelligence Division focuses mainly on domestic military phenomena[187] and threats, while the steering plan of the Intelligence Division focuses on foreign threats. While the themes of transnational jihadism and radical Islam have always been included in the two steering plans over the years, the Syria problem was first expressly included in the steering plan of the Intelligence Division in 2013. It is mainly this division that monitors foreign fighters and returnees. It also plays an important role in putting the phenomenon in the relevant regions into context. Moreover, this role fulfils the task entrusted to GISS in the Circular of 25 September 2014 regarding information management and the measures for monitoring foreign fighters who reside in Belgium.[188] In order to tackle 'terrorism' on a global scale, GISS has brought together the personnel of these two divisions in a Joint Cell. As stated, GISS studied the Syrian problem mainly from a broad, geopolitical context. The creation of this Joint Cell, in which more domestic aspects and the foreign ramifications of the problem are both discussed, was a manifestation of this.

---

187 The department that deals with 'Security' within this Division (i.e. the previous Division S) also plays a role in monitoring the phenomenon of 'extremism', but in this case specifically within Defence. Its task is to detect personnel who may pose a security risk to Defence because of their membership of or approach to extremist (jihadist) groups or ideologies (also see Chapter II.3 in connection with extremism in the army).

188 This circular was replaced by the Circular of the Ministers of the Interior and Justice of 21 August 2015 on the exchange of information relating to and the monitoring of foreign terrorist fighters from Belgium. This task is no longer included in that circular.

II.4.2. THE WORK VOLUME AND ALLOCATED PERSONNEL AND RESOURCES: AN INITIAL ASSESSMENT

The Committee found that the Syrian crisis has had a very profound impact on State Security operations. Quantitative indicators in relation to work volume (particularly incoming and outgoing flows of information and the number of applied special intelligence methods) have shown a very sharp increase. However, this work volume was not accompanied by a numerical reinforcement of the services. Instead, it was tackled by internal transfers, a reorientation of staff towards the Syria problem, or additional overtime. The increasing work volume has resulted in problems. After all, the totality of the areas that State Security must monitor has come under pressure. The workload of the personnel who are directly involved was heavy. Although the Standing Committee I found that the departments and personnel concerned performed their duties diligently and enthusiastically, it assessed this situation as risky and unstable. Structural solutions were necessary. The Standing Committee I also identified a specific gap: managerial vacancies were not systematically filled. This needed to be addressed.

Like State Security, the work volume at GISS has increased significantly.[189] This has been partly overcome by internal transfers. The Committee also found that GISS has started a number of projects since 2010 (including CYBERHUMINT, HUMINT, OSINT, and SOCMINT) to improve its information position with regard to international terrorism. The problem of the Syria crisis and the Belgian foreign fighters were obviously part of this. The Committee felt it was appropriate to monitor the progress of these projects.

II.4.3. THE INFLUENCE ON THE ORGANISATION AND THE STRATEGY: AN INITIAL ASSESSMENT

The Standing Committee I took the view that the 'Syria file' not only formed a pivotal moment for the State Security services that are directly involved, but also for the intelligence service in its entirety. There were indications that the 'Syria file' served as the catalyst for changes in the entire organisation. For example, steps were taken to formulate a new strategy that would lead to structural changes. These included the strategy itself (determining which areas could be given more or less attention) as well as the transition from the situation today

[189] In this first interim report, the Committee mainly limited itself to discussing the monitoring of the Syrian problem from a 'domestic perspective'. In relation to GISS, this meant that the efforts of the Intelligence Division, which operates mostly abroad, were not yet taken into consideration.

('*as-is*') to the desired future situation ('*to-be*'). Such a transition involves more than 'simply' shifting structures and personnel; it also affects the core of intelligence work, namely building up information positions in certain areas. This generally takes many years and requires a high level of specialisation. This implies long-term planning since an area that seems less important today may become a priority tomorrow.

For its part, GISS has sought for a number of years now to approach international terrorism thematically. Partly for this purpose, the terrorism analysis capacity of the Intelligence Division and the previous Counter-Intelligence Division were merged into one bureau in 2010. An examination of how this bureau operates revealed shortcomings in 2013. For this reason, GISS implemented a reorganisation in 2014 and turned the bureau into a Joint Cell. The Standing Committee I concluded that GISS then had a structure that could study and monitor radicalism, terrorism, and the *filières*. But the Committee added that this Joint Cell faced significant challenges: decisive management, different databases, personnel that were not being replaced, etc.

II.5. PERSONNEL OF THE INTELLIGENCE SERVICES AND SOCIAL MEDIA

Social networks such as Facebook, LinkedIn, and Netlog have undergone significant developments in the last few years, resulting in an enormous number of users worldwide. Social network services now form part of the daily life of very many people.

In November 2012, the Belgian press reported that personnel of the Belgian intelligence services had disclosed their professional capacity on those social networks.[190] This would not be without risks: after all, employees of an intelligence service who reveal their capacity expose themselves to threats or to attempts to approach them from foreign services, according to an anonymous source from the intelligence world.

At the request of the former Monitoring Committee in the Senate, the Committee opened an investigation in December 2012. The Senate wanted further information about the extent of the phenomenon, the associated risks, and the measures that could be adopted.[191] The investigation was completed in

---

190 N. VAN HECKE, *De Standaard*, 26 November 2012 ('*Belgische spionnen online te vinden*'); X., *7sur7.be*, 26 November 2012 ('*Des espions belges s'exposent sur le net*'); K. VAN EYKEN, *Het Laatste Nieuws*, 26 November 2012 ('Belgische spionnen online te vinden'). The information was even picked up by the international press. C. DEWEY, *The Washington Post*, 26 November 2012 ('Belgian intelligence workers outed on Facebook, LinkedIn'); X., *Voix de la Russie*, 27 November 2012 ('*Les espions belges se sont déclassifiés sur les réseaux sociaux*').

191 The Senate also wanted the problem investigated for the personnel of CUTA. A joint investigation with the Standing Committee P was started for this purpose (see Chapter II.6).

April 2015. The results of this investigation were discussed within the new Monitoring Committee in the Chamber of Representatives in July 2015. Following the discussion, the Members of Parliament wanted further information and the Committee therefore conducted an additional investigation and looked at various matters including whether the two intelligence services had issued mandatory directives on the problem, what action they had taken with regard to personnel who were active on social network sites, and what had been done with their profiles. The Monitoring Committee also wished to know whether it was legally possible to prohibit intelligence service personnel from being active on social network sites, even in a private capacity. The Standing Committee I obtained an opinion from the Privacy Commission regarding this latter question.[192] The additional investigation was completed in December 2015.

The results of the initial and additional investigations are both summarised below.

II.5.1. THE EXTENT OF THE PHENOMENON

State Security confirmed that it had checked shortly after the press reports of 2012 whether certain employees had revealed their capacity on LinkedIn. According to State Security, this was not the case. State Security could not perform the same check for Facebook since it did not have a profile that gave it access to the users' profiles.

GISS also stated that it was unaware of cases in which members of its personnel[193] had publicised their capacity. It checked four social network sites for that purpose.

In 2014, the Committee also carried out a limited check on LinkedIn itself. It identified the names of 17 people who publicised the fact that they were members of one of the two services. On request, State Security confirmed that five active and two former members of its service had stated their capacity or former capacity on LinkedIn.[194, 195] Four people stated that they were members of the service, without this ever having been the case. Six active and two former

192 See Opinion no. 45/2015 of 13 November 2015 with regard to the request for an opinion from the Standing Committees I and P on the possibility of prohibiting members of the intelligence services and CUTA from being active on social networks, even in a private capacity (www.privacycommission.be/nl/adviezen-cbpl?page=2).

193 For some positions, it is obvious that the capacity is made public (e.g. the head of the service, contact person for recruitment, and trade union representatives).

194 Other members of State Security were also found on this network. However, they made no mention of their capacity.

195 If the profile of a State Security employee refers directly or indirectly to the service, the person involved is asked (thus not formally obliged) to remove the reference from his/her profile, according to State Security. The incident would still be included in the relevant agent's security file.

members of GISS turned out to be on this social network site. However, not all of them explicitly identified themselves as members of GISS; they mostly introduced themselves as members of Defence. Nonetheless, their position could be determined from the information they posted on the network. The two former members went as far as releasing sensitive information.[196]

In relation to 'the extent of the phenomenon', the Committee concluded on the one hand that it is very limited and, on the other hand, that the services had gained a better picture of it over time. Both services conceded that it was difficult to know precisely how many of their agents were active on social network sites. As stated, initially State Security could not check this phenomenon itself because it had no profile on the relevant networks.

II.5.2. RISKS ASSOCIATED WITH THE USE OF SOCIAL NETWORK SERVICES

There are obviously 'general' risks associated with the use of social network sites, such as invasion of privacy or the possible misuse of private data. However, the Senate wished to be informed about the risks that apply specifically to the agents involved and their services.

It transpired that neither State Security nor GISS had analysed the specific risks associated with the phenomenon.[197] Even so, it is evident that such risks exist: sensitive or classified information can be unwillingly compromised; foreign services can try and recruit Belgian agents based on an analysis of personal data; the internet identity can be cloned and lead to the publication of false information; some information can be used for the purpose of blackmail; agents and their families can become the targets of violence, etc.[198]

Partly because initially neither service had insight into the problem (see above), it should not be surprising that they were not really aware of the risks. According to the Committee, it is also clear from some of State Security's answers that this service truly underestimated the risks. The management of the service later showed it was prepared to take the risks seriously. The Committee therefore found that there have been favourable developments in this regard since 2014.

---

196 On request, GISS stated that '*the profiles of personnel found on social media were removed or altered so there is no longer any link to the professional capacity*' (free translation). However, GISS did not give any formal instructions to this effect.

197 In 2009, a study was carried out within GISS on the protection of sensitive data in operational army units. This showed that military personnel on missions sometimes (unwillingly) share sensitive information in connection with operations, military plans, infrastructure, equipment, and personnel on social network sites.

198 Some of these risks were described in the framework policy document of 13 May 2013 on the use of social media by the members and services of the Federal Police. The Standing Committee I regarded this as a valuable document for the intelligence services.

II.5.3. MEASURES THAT ARE BEING AND CAN BE ADOPTED

Several measures can be taken to limit or eliminate the aforementioned risks. The Committee studied different options and questioned State Security and GISS in this regard.

The first option for consideration was whether to simply ban personnel from having a presence on social network sites or to limit such a ban to the ICT networks of the service. Neither State Security nor GISS have issued such a ban. However, the use of the ICT resources of the service for private purposes is regulated.

According to the Privacy Commission, prohibiting strictly personal activities on social media, outside the workplace and working hours, would be excessive. Such a ban may therefore be imposed at work and during working hours. The employer has a limited right of control at that time. The officials concerned must obviously be notified of the applicable instructions in advance.

Another option is to draw up rules for (and thus not simply ban) private activities on social network sites. Because freedom of expression is not an absolute right, it is possible to protect other interests (such as the security of the State or the safety of military personnel). At the time of the investigation, State Security had not issued any specific directives with regard to the use of social network sites by its employees. The personnel were continually reminded about the requirements of professional secrecy and discretion, including in private. This means, inter alia, that personnel must take care not to directly or indirectly publish their capacity or that of a colleague via social media. The Privacy Commission held the view that such a ban was justified. State Security also made its personnel aware of this during briefings. In May 2014, State Security announced that it would draw up a specific directive for the use of social network sites.

There were also no specific instructions regarding the private use of social network sites in force at GISS. Obviously there were relevant provisions regarding the use of social network sites for professional activities. At the end of this investigation, GISS proposed in an internal document that the discretion of personnel was required under all circumstances and explicitly referred to the use of social media.

Another option – namely a general ban on revealing their identity and professional capacity, regardless of the circumstances – did not apply in any of the services. State Security does impose a general obligation to exercise discretion regarding identity and capacity as a member of the service, except when in contact with other bodies. The same applies to GISS: when using the internet and social network sites, it is forbidden to publish or exchange information that could reveal a direct link between the user or another member of GISS and their capacity as personnel, except when express authorisation has

been granted for this purpose. This directive is regularly explained during security briefings and training sessions. GISS also provides Defence personnel who are active on social networks with smartcards, setting out a number of do's and don'ts.

A further option is to monitor the ICT use of personnel and the content of their messages (a priori or a posteriori). Although this is not clear from a privacy perspective, the law does offer a number of possibilities. For example, the 'open profile' of an agent can be checked as a result of a security investigation. This can obviously also be done as part of an intelligence investigation. The intelligence services can moreover examine the 'non-public' parts of messages by using special intelligence methods. The services reject a general, preventive monitoring of the content of their personnel's messages in private as disproportionate and infeasible.

Lastly, the Standing Committee I also investigated countermeasures that could be adopted in case of security incidents and paid attention to the reaction capabilities of the services during such incidents (e.g. withdrawing a security clearance and disciplinary action).

II.5.4. GENERAL CONCLUSION

As a general conclusion, the Committee found that for the most part both intelligence services followed a preventive approach in relation to this problem. This stemmed mostly from the concern of not wishing to restrict their agents' freedom of expression. This preventive approach consisted of making personnel aware of the risks and regularly pointing out their obligations with regard to confidentiality and discretion. However, the Committee was of the opinion that referring to general security rules did not suffice. Although an absolute ban on the use of social network sites is not possible (as it would be contrary to rights and freedoms), the special security conditions for intelligence agents must be taken into account when adopting specific measures. The Committee made various concrete recommendations in that regard (see IX.2.3).

II.6. PERSONNEL OF CUTA AND SOCIAL MEDIA

In 2012, the Monitoring Committee of the Senate asked not only for an investigation to be conducted into the possible presence of personnel of the two intelligence services on social network sites (see II.5), it also asked for an investigation into the same problem for personnel of the Coordination Unit for Threat Assessment. This investigation had to be conducted in conjunction with the Standing Committee P. On 20 December 2015, the two Committees decided

to open a joint investigation into '*the manner in which CUTA deals with the publication of the identity and professional capacity of its personnel online on social media*' (free translation).[199]

The Members of Parliament of the Monitoring Committee also wanted further information in this case. The Committee therefore conducted an additional investigation in which it looked at what results the recently established CUTA's 'steering committee' could already produce and how the service had reacted to the fact that four of its personnel were active on social media. The Monitoring Committee also wanted to know whether it was legally possible to prohibit CUTA personnel from being active on social network sites, even in their private capacity. The Standing Committees I and P obtained an opinion from the Privacy Commission regarding this latter question.[200]

The results of the initial and additional investigations are both summarised below.

II.6.1. THE EXTENT OF THE PHENOMENON

CUTA also learnt via the press that some of its personnel had published their name and professional capacity on social networks such as LinkedIn and Facebook. However, CUTA had also received that information via its own ICT department. This department carried out regular random checks on the internet to see what information could be found about CUTA members. CUTA deemed the extent of the phenomenon to be 'insignificant'. On the one hand, it only involved three active and one former member of the service. On the other hand, no sensitive information was disclosed. During subsequent questioning in 2015, the management confirmed it was unaware of any new cases.

II.6.2. RISKS ASSOCIATED WITH THE USE OF SOCIAL NETWORK SITES

The Standing Committees I and P found that it was essential for CUTA members to be very aware of, and to pay attention to, the opportunities that social network sites provide to foreign intelligence services: they can monitor people closely with a view to espionage or recruiting informants.

CUTA did not deny the existence of those risks but stated that their significance needed to be put into perspective. Firstly, the names of all CUTA

199 The investigation was completed on 12 March 2015.

200 See Opinion no. 45/2015 of 13 November 2015 with regard to the request for an opinion from the Standing Committees I and P on the possibility of prohibiting members of the intelligence services and CUTA from being active on social networks, even in a private capacity (www.privacycommission.be/nl/adviezen-cbpl?page=2).

analysts are in the public domain because they are published in the Belgian Official Journal at the time of appointment. Secondly, CUTA stated that it does not have any operational duties and does not perform activities inherent to intelligence services.[201] Lastly, the management trusted the professionalism of its personnel and the security training given to them.

II.6.3. MEASURES THAT ARE BEING AND CAN BE ADOPTED

Most CUTA personnel are seconded from other services (mainly police and intelligence services) and remain subject to the status and ethics of their service of origin. The Royal Decree of 23 January 2007 on CUTA personnel also contains a number of provisions by which regulations and any control over their conduct on social network sites must be taken into account. For example, Article 37 states that the analyst must comply with their duty of discretion regarding everything involving their professional activity, even in their private life.

Every CUTA member, moreover, holds a security clearance. As a result of the granting or renewal of such a clearance, an investigation can also be conducted into the 'open profiles' on network sites, namely information to which access is not limited by the person in question.[202]

If an intelligence service receives information that the conduct of a CUTA employee on social network sites could give rise to a security threat, the information 'with limited access' can also be obtained without the knowledge of the person involved. However, a special intelligence method must be used for this purpose.

In the most recent version of the 'security instructions' intended for personnel, special attention was paid to the duty of discretion during the use of social media. Personnel were also given a number of security briefings in 2014 and 2015.

Lastly, a 'steering committee' was created within CUTA that was given four assignments: (a) to draw up a list of the potential security problems; (b) to perform a risk analysis for each of these problems; (c) to then prioritise the actions to be taken; and, finally, (d) to propose measures to be adopted in relation

---

201 The Committees did not agree with this statement. The evaluation work performed by CUTA mainly consists in processing and analysing information of the intelligence services, which is often classified. Even if CUTA is not authorised to gather intelligence itself, it is tasked with processing and analysing the information. This contributes to the intelligence cycle. Employees of CUTA are therefore subject to the same obligations regarding professional secrecy and discretion and are exposed to similar security risks as the personnel of the intelligence services.

202 Consulting social media is not expressly mentioned in the regulations as a means of gathering information during a security investigation. In the opinion of the Committees, it can be equated to consulting open sources.

to investment, instructions, and awareness. In 2015, this steering committee finished listing the problems and documented the prioritisation of actions. The security linked to the use of ICT tools in the broad sense was an essential part of this. A working group was also set up whose task was to prepare internal rules for the proper use of social media. However, the initiatives were suspended as priority had to be given to the problem of foreign terrorist fighters and the events that occurred in Paris and Brussels.

As for the members of the intelligence services, the question for CUTA employees is the extent to which preventive checks on the private and professional use of social media sites are possible. Since all employees must hold a security clearance, their hierarchy must be able to ascertain that they are continuing to comply with the security conditions under all circumstances, particularly when they use ICT tools as part of their duties. The prior consent of the employee in question is not required for such a check. The Committees also held the view that the CUTA hierarchy must be able to generally check the conduct of its employees on social media.

In its opinion, the Privacy Commission stated that prohibiting strictly personal activities on social media, outside the workplace and working hours, would be excessive. Such a ban may therefore be imposed at work and during working hours. The employer has a limited right of control at that time. Those concerned must obviously be notified of the applicable instructions in advance.

II.6.4. GENERAL CONCLUSION

Since only four members of CUTA personnel were active as such on social media, CUTA initially minimised the extent of the problem and rightly pointed out that the names of all CUTA analysts could easily be found online. According to the Standing Committees I and P, CUTA seemed to become more aware of the problems and risks during the course of 2014.

The Committees were of the opinion that by creating a steering committee to deal with security problems, an important step was taken in thoroughly tackling the problem. However, the role of that committee, the appropriate detection methods, and their boundaries need to be carefully defined.

Due to its concern not to limit its employees' freedom of expression, the CUTA management has mainly adopted a preventive approach to the use of social network sites, more specifically by raising the awareness of its personnel. They are regularly reminded of their duty of discretion.

However, the Committees were of the opinion that invoking general security instructions did not suffice. Although an absolute ban on the use of social network sites is not possible (as it would be contrary to rights and freedoms), the special security conditions for the employees involved must be taken into account when adopting specific measures. Prevention by drawing up rules of good conduct and

a posteriori checks (social media policy) seem to be the key. The Committees formulated many concrete recommendations in this regard (see IX.2.4).

II.7. INTERNATIONAL CONTACTS OF CUTA

One of the assignments of the Coordination Unit for Threat Assessment (CUTA) is to maintain contact with 'similar foreign or international services'. In early May 2013, the Standing Committees I and P decided to investigate how CUTA carries out that task.[203] After all, in the preceding period, the Committees had received anonymous letters complaining that the former director was making too many official trips and maintaining dubious contacts with certain foreign intelligence services and authorities.[204] He had allegedly also tried to influence certain cases in favour of certain countries. Lastly, he was accused of having discussed the exchange of information with a foreign service and mutual access to databases without any mandate.

The final report was approved on 22 June 2015 and discussed shortly afterwards in the Monitoring Committee of the Chamber of Representatives. That committee asked the Committees to conduct an additional investigation into the presence of two communication systems at CUTA. These systems were provided by two foreign services. The Committees investigated the IT security of the CUTA and the legality of both systems.[205]

II.7.1. THREE PRIOR INVESTIGATIONS INTO SIMILAR MATTERS

This was not the first time that the Committee had investigated the international contacts established by CUTA.

The first investigation was carried out in 2009.[206] It focused mainly on the director's official trips. However, the Committees did not establish any significant dysfunctions.

Another investigation was conducted during 2011 into a mission that CUTA had planned to the Democratic Republic of Congo.[207] The purpose of this mission

---

203 'Joint investigation into how CUTA maintains international relationships with similar foreign or international services pursuant to Article 8, 3° of the Threat Assessment Act of 10 July 2006'.

204 In order to examine this aspect of the investigation, what the intelligence services and federal police knew about the contacts that CUTA had made with certain foreign services, how those services experienced the contacts, and how they reacted to them were also investigated.

205 The additional report was finalised on 11 August 2015.

206 STANDING COMMITTEE I, *Activity Report 2009*, 146.

207 STANDING COMMITTEE I, *Activity Report 2011*, 125.

would have been to allow CUTA to gain a better idea of the security situation on the ground and the possible presence of radical, extremist, or terrorist groups in that country. The Committees pointed out, inter alia, that the legislature did not want CUTA to gather intelligence in the country itself, instead of the support services.

The third investigation – also in 2011 – dealt with Belgian representation at international meetings on terrorism.[208] The Committees observed that the Belgian police, intelligence services, and CUTA regularly participated together in international meetings on the fight against terrorism and/or extremism. However, this happened without much consultation or coordination. The investigation brought various one-off problems to light.

In the three investigations, the Standing Committees I and P recommended that CUTA always ensure that its specific identity does not lead to confusion among the foreign services and bodies with which it has contact. As the coordination unit is not an intelligence service, the Committees found it essential that attention should be paid to this actively and systematically in its communications and operations, both in Belgium and abroad. It was therefore recommended that CUTA should take great care in the preparation and performance of its assignments abroad and strictly limit its study trips. Lastly, the Standing Committees I and P also called for the Ministerial Committee for Intelligence and Security, as it was known at the time, to draw up a directive as soon as possible in order to precisely define the 'similar services' with which CUTA could maintain 'specific contacts'.[209]

II.7.2. LEGAL FRAMEWORK

Articles 8, 9, and 10 of the Threat Assessment Act were particularly important to this investigation.

As stated, CUTA is made responsible for maintaining specific contacts with similar foreign or international services (Article 8, 3° of the Threat Assessment Act). It falls to the National Security Council to explain what this means. This had not been done by the time the investigation ended. The Committees pointed out that such an exercise would not be straightforward, given the diversity of the structures that countries have put in place to coordinate the analysis of the terrorist and/or extremist threat.[210]

Article 9 of the Threat Assessment Act forms the statutory basis for the database and working files of CUTA. This provision obliges the director to adopt

---

208 STANDING COMMITTEE I, *Activity Report 2011*, 135.

209 The recommendations made by the Committees were only implemented recently. The National Security Council issued a directive in that regard at the start of 2016, which obviously did not fall within the scope of this investigation.

210 In this regard, see STANDING COMMITTEE I (ed.), *Fusion Centres Throughout Europe, All-Source Threat Assessments in the Fight Against Terrorism*, Antwerp, Intersentia, 2010, 220 p.

appropriate technical and organisational measures to prevent unauthorised persons from gaining access. Any link between the database of CUTA and other national or foreign information systems is strictly prohibited.

Lastly, there is Article 10 of the Threat Assessment Act. This provision limits the communication of CUTA evaluations to specific Belgian services and authorities; foreign or international authorities or bodies are not mentioned. Article 8 of the Threat Assessment Act, moreover, stipulates that the data which the coordination unit receives from abroad must be forwarded to the competent Belgian services.

II.7.3. CONCLUSIONS OF THE STANDING COMMITTEES I AND P

A first part of the investigation focused on official foreign trips by members of CUTA. The figures provided show that the number of assignments performed abroad was not excessive.

The frequency of Belgian contacts with certain foreign authorities and services was likewise not problematic. It proved that CUTA is approachable, which is noteworthy.

However, the Committees held the view that the organisation of contacts with foreign countries was not the result of a clear and carefully thought-out strategy. The same applies to contacts with other services; these seemed instead to be the result of personal initiatives that were taken in response to external requests and opportunities.

The Committees also found reporting on the contacts to be lacking, both within and outside the organisation. There was seldom any clear added value, except for possible knowledge acquired by an employee who was sent on a mission.

The contacts established by CUTA with foreign and international services that are not 'similar' services were problematic because they could cause confusion in relation to the responsibility of the different Belgian services.

The investigation also showed that CUTA sometimes obtains information from foreign services that is not systematically forwarded to the competent Belgian authorities. CUTA moreover conceded that it also gave information to those foreign services. This working method was contrary to Article 8, 3° and Article 10 of the Threat Assessment Act.

Without minimising the above conclusions, the Committees emphasised that the Ministerial Committee for Intelligence and Security (now the National Security Council) had still not issued any directive at the time of the investigation that regulated these international contacts (as required by the Threat Assessment Act). Such a directive had to explain what CUTA could and could not do in this regard.[211]

---

[211] However, the Committees added that CUTA had never taken any initiative in relation to its competent ministers to clarify this issue.

The Standing Committees I and P shared the concerns expressed by the heads of the intelligence services on how the director of CUTA at the time managed his international contacts. The Committees believed that the director, in view of the contacts that he made with different foreign partners – some long before his appointment to the position – must at least have created the impression that he did not work carefully enough. He also failed to maintain an adequate distance in relation to certain services whose activities were being closely monitored by State Security and GISS, even if the Ministers in charge had approved him making those official contacts.

The lack of transparency, traceability, and reporting in relation to these contacts meant, moreover, that the objectivity of certain evaluations were placed in doubt by the Belgian intelligence services. That finding was particularly disturbing.

The Standing Committees I and P were also very concerned about how the director of CUTA at the time maintained certain foreign contacts; these contacts were perceived as encroaching on the area of responsibility of State Security and GISS and were thus problematic for cooperation with those services. The situation needed to be thoroughly reconsidered.

The Committees once again found that CUTA had failed to comply with its statutory obligation to submit an activity report twice a year on its strategic objectives, activities, and organisation to the National Security Council, which in turn had to forward that report to the oversight bodies.

As stated, the Committees conducted an additional investigation into the two communication systems that CUTA shared[212] with two foreign services. This investigation confirmed and illustrated the earlier conclusions, particularly as regards contact with non-homologous services and the exchange of operational information and personal data. Apart from the evident need to exchange information on extremism and terrorism internationally, both Committees commented that the established conduct was contrary to the letter and spirit of the Threat Assessment Act. Moreover, it did not take into account the powers and obligations of other federal services and authorities, which could disrupt international cooperation and mutual relationships.

II.8. WRONGFULLY MONITORED BY THE INTELLIGENCE SERVICES?

In February 2014, a person of North African origin who resided in Belgium lodged a complaint that he was being monitored in an 'oppressive way' by the intelligence services. The complainant alleged that he had no idea why he would attract attention: he had never had any problems in his country of

212 The systems are no longer operational.

origin or in the Asian country where he had worked for several years. He argued that he had no criminal record or links to terrorism or radical environments.[213]

According to the complainant, his problems began in 2011. He was detained for six hours at a foreign airport that he had travelled to for work purposes. A security manager purportedly later told him that his name appeared on a list of the American Transportation Security Agency (TSA). He explained that he had been monitored since then on every subsequent trip to this country. A visa application for a third country had also been refused. He was then transferred to the Belgian headquarters of the company.

The complainant explained that he had been the target of monitoring operations since his arrival in Belgium in May 2012 and feared that various intelligence services were unlawfully monitoring him. This feeling was strengthened by the unusual treatment he received twice at Zaventem Airport in Brussels. He was checked by the Airport Police and even detained briefly when he wanted to take a flight.

The Standing Committee I examined whether the complainant had actually attracted the attention of State Security or GISS and, if so, what the information position and actions of the intelligence services were.

II.8.1. THE FACTS

In November 2011 – i.e. when the complainant was not yet in Belgium – CUTA, GISS, and State Security received a request for information about him from a foreign intelligence service. He purportedly sympathised with a radical Muslim preacher.

Following the request from the foreign service and in the absence of any information about the complainant, CUTA asked Federal Police to issue an alert about him in the general police database under the 'Terrorist Information context' for a period of six months.

State Security on its part conducted an administrative investigation.[214] This did not show that the complainant was part of any Islamic environments. The foreign partner service was notified of this.

As the complainant did not appear in its database and there was no direct link to its statutory mandates, GISS took no action in this regard.

---

213 The investigation was opened on 3 July 2014. The final report was sent to the chairman of the Monitoring Committee and the Ministers of Justice and Defence in February 2015.

214 State Security consulted its own database and other existing databases (the police database, the National Register, the Immigration Service, etc.) in this regard. The service also confirmed having carried out searches on social networks such as Facebook.

On 28 May 2012, the complainant landed at Zaventem Airport.[215] A day later, the foreign intelligence service provided new information, this time to State Security, CUTA, and the Federal Police. The service stated that the complainant had left the Asian country where he was working. As this document did not contain any new information, State Security decided not to conduct any further investigation. State Security did ask the partner service for a risk analysis and threat assessment. The response was that an analysis of his e-mail traffic had not revealed any crucial information.

In August 2012 – after a short stay abroad – the complainant was checked by the airport police upon his arrival at Zaventem.[216] He was in fact interviewed on this occasion. A copy of the report was forwarded to CUTA, GISS, and State Security. However, the reporting officers did not find any significant information.

In the same month, CUTA asked the three support services involved whether the complainant had any ties to radical, Islamic environments. State Security responded that it did not have any additional information.

At the start of 2013, State Security received a new request for information, this time from the intelligence services of the Asian country where the complainant had been living. The request contained detailed information about his suspected membership of a radical, Islamic movement. State Security then opened a new investigation and relied on its intelligence channels among other resources. A more thorough investigation was therefore conducted, for which purpose the service worked proportionately: for example, no special intelligence methods were used. All actions undertaken were lawful.

In March 2013, State Security passed on the result of its investigation to the relevant foreign service. Once again, there proved to be no links with any Islamic environments. However, the result of this additional investigation, even though negative, was not communicated to CUTA. The information of the Asian country was also not divulged outside State Security.

Since March 2013, State Security has not received any new information or questions relating to the complainant.

II.8.2. THE PROBLEM WITH TERRORISM LISTS

There are strong indications that the problems experienced by the complainant abroad were related to the problem with terrorist lists.[217] For example, the complainant purportedly appeared on a list of the American Transportation

---

215 Despite the fact that there was an alert out on him, the complainant was not checked when he first arrived in Belgium.

216 This check therefore happened when the complainant arrived in Belgium for the second time.

217 In this regard, see P. DE HERT and K. WEIS, '*Europese terrorismelijsten. Beperkte rechtsbescherming*' (European terrorism lists. Limited legal protection), *Nieuw Juridisch Weekblad*, 2009, 199.

Security Agency (TSA). He was also temporarily placed on a Belgian 'list', namely the general police database.

The Committee pointed out that States and multilateral bodies use various lists in the fight against terrorism and for the protection of civil aviation. For example, the purpose is to subject those appearing on the lists to thorough checks, forbidding them to fly, or to make reports to the authorities that issued the alert. Such lists are based on national and/or international law (e.g. United Nations resolutions or European Union directives).

The Standing Committee I does not doubt the usefulness or necessity of such lists, quite the contrary. Recent terrorist acts have shown that intelligence is sometimes not adequately shared with other countries. Equally, the Committee does not want to exclude valid reasons or suspicions that could have existed or did exist in the complainant's specific situation to place him on such a list.

In this case, the Standing Committee I was able to establish, within its area of responsibility, that the Belgian services acted professionally and correctly in relation to the complainant and the foreign services.

However, from the civilian's perspective, being placed on a list remains problematic. After all, it is not an obvious step to assert one's rights with regard to security measures that are often taken on the basis of procedures that occur without the knowledge of the person involved (no notice, no defence). These procedures, including their secret nature, may be legitimate, insofar as the reasons and purposes thereof are likewise legitimate and insofar as the implementation of the measures is not excessive.[218] There are indeed examples which show that placing people on terrorism lists can lead to disproportionate consequences.[219] Experience also shows that it is not always an obvious step to remove people from such lists.

II.8.3. CONCLUSIONS OF THE INVESTIGATION

The Committee stressed that the complainant was not the target of monitoring operations by the Belgian intelligence services. It was likewise not responsible for the alert in the 'Terrorist Information context'. However, it is very likely that the complainant was monitored by the intelligence services of the Asian country where he had been living for a while.

---

218 In relation to these lists, also see STANDING COMMITTEE I, *Activiteitenverslag 2005* (Activity Report 2005), 158–168.

219 Maher Arar is a Canadian/Syrian dual national who was regarded as a terrorism suspect based on Canadian reports during a stopover in the United States, surrendered to Syria, and tortured there. He was later acquitted of all suspicions and received compensation. See http.//ccrjustice.org/ourcases/current-cases/arrar-v.ashcroft.

The Committee also found no indication that State Security was being 'manipulated' by a partner service. There were, moreover, no indications that foreign services took action against the complainant on Belgian soil.

The Belgian intelligence services acted legally and proportionally in this case and did not exceed their powers. They never participated in the monitoring activities as described by the complainant. The Committee found that State Security had effectively managed this case.

Lastly, the Committee asked whether and to what extent the Belgian intelligence services have a 'positive obligation' towards a resident under the Belgian Constitution[220] or the ECHR to protect him against any unfounded accusations by foreign intelligence services or authorities and, where applicable, to stop an invasion of his privacy.

II.9. COMPLAINT REGARDING THE DISCLOSURE OF PERSONAL INFORMATION BY AN INTELLIGENCE AGENT TO A THIRD PARTY

A private individual lodged a complaint with the Standing Committee I at the start of October 2014. According to the complainant, the content of personal e-mails that he had sent to a member of the Ministry of Defence had ended up with his employer via the military intelligence service. He was dismissed shortly afterwards. The employer explicitly referred to the fact that it was placed in possession of the relevant e-mails by an employee of GISS. The investigation had to clarify how GISS had handled the case, whether the service had complied with the applicable legislation, and whether intelligence had indeed been passed on to a third party.[221]

The e-mails in question ended up at GISS via the member of the Ministry of Defence. After all, the complainant stated in his message – as a joke, it later transpired – that he had forwarded a computer virus. GISS is the designated service to investigate such a potential threat; it forms part of its statutory assignments.

In addition to the IT investigation, GISS also gathered intelligence on the complainant in order to be able to assess the potential threat. This also fell within the scope of its powers.

The result of this technical investigation (which revealed that there was no threat) was generally brought to the attention of the security officer of the

220 For example, see Article 191 of the Belgian Constitution: '*Any foreign national on Belgian soil enjoys the protection granted to persons and property, other than in case of the statutory exceptions*' (free translation).

221 The investigation was completed in June 2015. The Standing Committee I was obviously not competent to look at the reason and legality of the complainant's dismissal.

company where the complainant worked. The statutory basis for this report can be found in Article 19 of the Belgian Act of 30 November 1998 governing the intelligence and security services.[222] The Committee stated that sending all the e-mails to the security officer without the permission of those concerned seemed to be incompatible with the Personal Data Protection Act.

GISS also forwarded the e-mails to the National Security Council (ANS/NVO), which was authorised to withdraw any security clearance granted to the complainant and the company. Although the threat in this case was not serious, the complainant's conduct could have constituted a security problem. The reporting of the e-mails to the ANS/NVO thus appeared to be legitimate from this perspective.

Lastly, the Committee found that GISS had not adequately coordinated the different aspects of the problems and not acted in full compliance with the statutory or regulatory procedures that apply in case of security incidents.

II.10. STATE SECURITY AND THE APPLICATION OF SICK LEAVE REGULATIONS

In mid-2014, a protection assistant of State Security filed a complaint. After a period of sick leave, he was[223] placed on non-active service for the full period of medical exemption and then received an order to repay a substantial amount. This decision was made because there had been issues during his sick leave with regard to the mandatory medical check-up. He also complained about the fact that he was forced to use up his overtime before resuming his work.

The Committee decided to open an investigation into '*how State Security interprets and implements the work rules, in particular the rules on sick leave*' (free translation).[224]

The investigation showed that State Security is well aware of the applicable work rules and has issued internal directives with regard to personnel. However, the rules and internal directives were not observed in this case.

In relation to the overtime issue, the Standing Committee I also referred to its investigation into State Security's performance of its statutory close protection

---

222 *'The intelligence and security services shall communicate the information referred to in Article 13, 2°, only to the relevant ministers and the relevant judicial and administrative authorities, to the police services, and to any competent bodies and persons who are the target of a threat as referred to in Articles 7 and 11 […]'* (free translation) (Article 19 of the Intelligence Services Act).

223 Article 62 of the Royal Decree of 19 November 1998 on authorisations and leave granted to government department staff.

224 In February 2015, the final report was sent to the Minister of Justice and the chairman of the Monitoring Committee.

assignments.[225] The problems established in that investigation still applied at the time of the investigation into the complaint.

Lastly, the Committee referred to a lack of communication by the administrative services of State Security, both with internal personnel and field service personnel.

II.11. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2015 AND INVESTIGATIONS INITIATED IN 2015

This section contains a list and brief description of all investigations opened in 2015 and those investigations that were continued during the operating year 2015 but could not yet be completed.

II.11.1. PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL AND THE SNOWDEN REVELATIONS

The Snowden revelations gave insight into top secret programmes, mainly of the US National Security Agency (NSA). These revelations resulted in many parliamentary, judicial and intelligence investigations throughout the world, including in Belgium. The Standing Committee I opened four investigations, which of course were closely connected with each other.

Three of the four investigations were completed in 2014.[226] A last investigation[227] deals with the possible implications of these foreign programmes on the protection of the scientific and economic potential of the country. Its aim is to check whether the Belgian intelligence services:

- have paid attention to this phenomenon;
- have identified any real or potential threats to the Belgian scientific and economic potential;

---

225 In this regard, see: STANDING COMMITTEE I, *Activity Report 2014*, ('II.4. State Security and its statutory close protection assignments'), 45–52, especially 50.

226 See STANDING COMMITTEE I, *Activity Report 2014*, 11–45 ('II.1. The Snowden revelations and the information position of the Belgian intelligence services', 'II.2. Protection of privacy and massive data capturing' and 'II.3. Use in criminal cases of intelligence originating from massive data capturing by foreign services').

227 'Investigation into the attention that Belgian intelligence services pay (or do not pay) to potential large-scale threats to the Belgian scientific and economic potential originating from electronic surveillance programs on communication and IT systems used by foreign countries and/or intelligence services' (free translation).

– have notified the competent authorities and proposed protection measures; and
– have sufficient and adequate resources to monitor this problem.

Besides, at the request of the former Monitoring Committee in the Senate, the consequences of the PRISM programme and/or other similar systems for the scientific and economic potential of the country were also examined. The report was completed at the beginning of 2016.

II.11.2. ISSUE OF FOREIGN FIGHTERS AND THEIR CONTINGENT IN SYRIA

Since 2013, the Syrian conflict has been a magnet for foreign terrorist fighters from all over the world. It is certainly the case that a relatively large number of those fighters are from Belgium.

The Standing Committee I therefore decided to open an investigation in October 2014 into '*the information position of the two intelligence services (GISS and State Security) regarding the recruitment, mission, stay and return to Belgium of young adults (Belgian and other nationals living in Belgium) who are leaving or who have left to Syria or Iraq and the exchange of intelligence with various authorities*' (free translation). Various topics came up for discussion: what mandate do the Belgian intelligence services have in this regard and how were/are they managed? Do the intelligence services have any insight into the recruitment and departure phase? Do they have an idea of the composition of these fighters in Syria? Are they aware of the activities that these fighters are developing locally? Are developments abroad being translated into possible domestic threats? If so, which threats? What about monitoring and the approach upon their return? How are the relevant services (GISS, State Security, CUTA and the police) cooperating in this regard? How is this being reported on and to whom?

At the start of 2015, a first, interim report was drawn up for the Monitoring Committee (see Chapter II.4 in this regard). The final report was completed in 2016.

II.11.3. STATE SECURITY AND THE COOPERATION PROTOCOL WITH PENAL INSTITUTIONS

An investigation was opened on 1 October 2014 into how State Security implements the '*protocol agreement governing cooperation between State Security and the Directorate-General for the Execution of Penalties and Disciplinary Measures*' (free translation). Two prior investigations were the direct reason for

this investigation.[228] The aim was to assess whether the agreement is being efficiently implemented, whether State Security is able to extract useful information for its purposes and, albeit on the margin, whether the exchange of information on detainees is in accordance with the protection of the rights of individuals guaranteed by the Constitution and the law.

The investigation was completed in 2016.

II.11.4. MONITORING A POTENTIAL THREAT AGAINST A FOREIGN VISITOR

In March 2015, an agent of State Security's External Services approached the Investigation Service of the Standing Committee I to complain about how the Analysis Services purportedly worked in a certain case. More specifically, the complaint related to how information was gathered and analysed with regard to the imminent visit of the Congolese physician Dr Mukwege to Belgium. He had long opposed the current regime in Congo. According to the complainant, CUTA had not been correctly informed of all relevant information in order to duly evaluate the potential threat to the doctor.

The investigation was completed in 2016. The results were discussed within the Parliamentary Monitoring Committee.

II.11.5. A COMPLAINT AGAINST AN INDISCREET COLLEAGUE

In July 2015, a senior officer of GISS filed a complaint with the Standing Committee I alleging that a GISS employee had divulged data relating to his personal and professional life in a public area in the municipality where both he and the employee lived. He even feared that this could have consequences for his safety and that of his family.

The complainant approached the management of GISS on two occasions but did not receive any decisive response. He finally filed his complaint with the Standing Committee I. The complaint covered both the alleged indiscretions and the manner in which GISS had responded to them.

The final report was approved in 2016.

---

228 STANDING COMMITTEE I, *Activity Report 2011*, 114–117 ('II.3. Information position and actions of the intelligence services with r egard to Lors Doukaev') and *Activity Report 2012*, 28–33 ('II.3. Possible monitoring of an individual during and after his detention in Belgium').

II.11.6. A COMPLAINT CONCERNING WHETHER OR NOT A PAYMENT IS DUE

A former State Security inspector filed a complaint with the Standing Committee I in April 2015. He stated that he was forced to repay a (small) amount that he purportedly wrongly received from the special funds. After failing to defend his position with State Security, he approached the Standing Committee I. He also stated that the problems he had experienced with his direct hierarchy had prompted him to leave State Security.

The Committee then opened an '*investigation following a complaint by a former State Security agent regarding the management of the departmental fund of a provincial post*' (free translation). This investigation was also completed in 2016.

II.11.7. A CONTROVERSIAL INTERVENTION BY TWO PROTECTION ASSISTANTS?

An incident with two members of what was State Security's Close Protection Service occurred during an assignment on a public road in June 2015. The protection assistants, who were responsible for the security of a dignitary, noticed the car of a private individual following right behind them, which ignored their orders to maintain a distance. When the vehicle of the driver in question stopped, the protection assistants intervened and allegedly acted brutally. One of them even drew his weapon. The driver of the car related these facts to the Committee.

The investigation into the intervention was completed in 2016.

II.11.8. A COMPLAINT CONCERNING AN INTERVENTION BY CUTA

In 2015, the Standing Committee I, together with the Standing Committee P, opened an investigation into how CUTA had played a role in revoking an airline pilot's licence. The person involved filed a complaint alleging that CUTA had wrongly drawn up a threat assessment that could subsequently be used to revoke his pilot's licence.

Most of the investigative acts were completed in 2015. The investigation will be finalised in the second half of 2016.

II.11.9. INDIVIDUAL THREAT ASSESSMENTS BY CUTA

In March 2015, the Standing Committees I and P opened a joint investigation into '*how the CUTA determines the threat level posed by or to an individual, into*

the consequences that this threat level has for the division of duties, the measures to be adopted and the exchange of information among the services involved, as well as into the practical implications for the person involved and his monitoring' (free translation). This occurred at the request of the Monitoring Committee in the Chamber of Representatives, which wished to be informed of the following questions:

- What criteria does CUTA apply to determine the threat level in relation to an individual?
- Which body sets out the tasks of the services involved once the threat level has been determined?
- What operational measures result from a specific threat level and which service is tasked with their coordination?
- How are the flows of information among the various services organised?
- What are the concrete implications for an individual who is the target of a specific threat level?
- How is the 'classification' of this individual monitored by the local police and administrative authorities?

An interim report was sent to the Monitoring Committee in February 2016. The final report is scheduled for the second half of 2016.

II.11.10. SPECIFIC DYSFUNCTIONS WITHIN CUTA

The Standing Committees I and P received two anonymous letters in the second half of 2015. These referred to 'irregularities' and 'serious structural problems' within CUTA. For example, experts allegedly had to perform tasks that formed part of the analysts' statutory assignments. Certain people were also purportedly seconded to CUTA with disregard for the applicable rules.

The Committees later also received a complaint about the internal functioning of CUTA. The complainant referred, inter alia, to how his secondment was ended.

The Committees covered all these issues in a joint investigation. The final report is scheduled for the second half of 2016.

II.11.11. INVESTIGATION INTO THE INFORMATION POSITION OF THE TWO INTELLIGENCE SERVICES BEFORE THE PARIS ATTACKS

Several deadly attacks took place in Paris on 13 November 2015. Suicide bombers blew themselves up in the vicinity of the *Stade de France* and raids were carried

out on the patios of cafés and restaurants in the French capital. Hostages were simultaneously taken and fired upon in the Bataclan concert hall. The death toll among the victims reached 130. A fourth attack was planned close to the *La Défense* business district. The attacks were perpetrated by returning foreign terrorist fighters under the control of the IS terrorist group.

Fairly soon after the attacks, information emerged pointing to a close connection with Belgium: several terrorists were from or resident in Belgium, the vehicles used for the attacks had been rented in Belgium, Belgian safe houses were involved, the explosive belts had probably been assembled in an apartment in Schaarbeek, etc.

The Standing Committee I opened an investigation almost immediately,[229] but waited before performing the first investigative acts. After all, in the turbulent weeks and months that followed the attacks, State Security and GISS could not be expected to free up much time for the Committee and its investigative service.

The investigation was completed in 2016.

[229] '*Investigation into the information position of the two intelligence services, prior to the evening of 13 November 2015, regarding the individuals or groups that perpetrated or were involved in the Paris attacks*' (free translation). At the start of 2016, the same investigation was opened jointly with the Standing Committee P regarding the information position of CUTA.

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS 2015

This chapter includes further figures on the use of special intelligence methods by State Security and GISS, as well as on the manner in which the Standing Committee I performs its jurisdictional role in this matter. It is based on the report on the use of special methods by the intelligence services that is drawn up annually for Parliament pursuant to Article 35 §2 of the Review Act.

The Committee wishes first of all to refer to the agreement of 16 November 2015 between the National Bank of Belgium (NBB) and State Security, by which the latter would be given access, on simple request, to the data included in the Central Information Point (CIP). This is a database in which all banking, exchange, credit and savings institutions must divulge the identity of their clients and their account numbers. State Security held the view that consulting such a database constituted an ordinary method (namely as provided for in Article 14 of the Intelligence Services Act). However, the Committee did not agree with this. Although the Committee found that State Security's initiative showed that the service was actively tapping into useful channels of information, it referred to Article 18/15 §1, 1° of the Intelligence Services Act. This article regards requesting lists of bank accounts as an exceptional method. No reservation is made in this regard about the institution from which the information is obtained. Accordingly, even if the NBB is not regarded as a 'bank' or 'financial institution' within the meaning of Article 18/5 §2 of the Intelligence Services Act, the lists are still 'protected' by the mechanism of the exceptional method. If State Security therefore wishes to obtain lists of bank accounts from the CIP, an exceptional method must first be requested. The Minister of Justice stated that, pending additional consultation, State Security must apply the SIM procedure for the purpose of searching the CIP.[230]

[230] *Ann.* Chamber of Representatives 2015–16, 6 January 2016, CRIV54COM301, 3, Q. no. 8170.

III.1. FIGURES WITH REGARD TO THE SPECIFIC AND EXCEPTIONAL METHODS

Between 1 January and 31 December 2015, a combined total of 1,392 authorisations were granted by the two intelligence services for the use of special intelligence methods: 1,271 by State Security (of which 1,143 specific and 128 exceptional) and 121 by GISS (of which 87 specific and 34 exceptional).

The following table draws a comparison with the figures of previous years.

	GISS		State Security		TOTAL
	Specific method	**Exceptional method**	**Specific method**	**Exceptional method**	
2013	131	23	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392

Whereas a decrease of 7% was registered in 2014, there was a somewhat larger increase in the number of special intelligence methods in 2015. The growth came entirely in the number of specific methods used by State Security (from 976 in 2014 to 1,143 in 2015). There was a significant decrease in both the special methods used by GISS and the exceptional methods used by State Security.

Three categories are distinguished for each service below: specific methods, exceptional methods, and the interests and threats justifying the use of these methods.

III.1.1. METHODS WITH REGARD TO GISS

III.1.1.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015
Entry into and surveillance of or in places accessible to the public, using a technical device	14	7	4
Entry into and searching of places accessible to the public, using a technical device	0	0	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator	0	0	0

[231] In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

NATURE OF SPECIFIC METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015
Inspection of identification data for electronic communications, requesting the cooperation of an operator, or direct access to data files	66 methods	67 methods	55 methods
Inspection of call data for electronic communications and requesting the cooperation of an operator	15	12	12
Inspection of localisation data for electronic communications and requesting the cooperation of an operator	36	28	16
TOTAL	**131**[231]	**114**	**87**

The trend observed in 2014, namely that less use was made of 'Observations' and 'Localisations', continued in 2015. A reduction in the number of identifications has also been noted, while 'Inspections of call data' have remained stable.

III.1.1.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER IN 2013	NUMBER IN 2014	NUMBER IN 2015
Entry into and surveillance in places not accessible to the public, with or without a technical device	1	1	3
Entry into and searching of places not accessible to the public, with or without a technical device	0	1	0
Setting up and using a fictitious legal person	0	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	0	0	0
Collecting data on bank accounts and banking transactions	5	5	3
Penetrating an IT system	0	03	3
Monitoring, intercepting and recording communications	17	26	25
TOTAL	**23**[232]	**36**	**34**

In relation to exceptional methods, the number of tapping measures remained stable (25 in 2015 compared to 26 in 2014), in contrast to 2013 when there was a significant increase.

232 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

III.1.1.3. Interests and threats justifying the use of special methods[233]

GISS may use specific and exceptional methods in respect of three of its assignments, each of which is related to the safeguarding of specific interests:

- the intelligence assignment focused on threats against, for example, the inviolability of the national territory, the military defence plans, and the scientific and economic potential in the area of defence (Article 11, 1° of the Intelligence Services Act);
- the military security assignment focused, for example, on safeguarding the military security of defence personnel, military installations, and military IT and network systems (Article 11, 2° of the Intelligence Services Act);
- the protection of military secrets (Article 11, 3° of the Intelligence Services Act).

NATURE OF THE TASK	NUMBER 2013	NUMBER 2014	NUMBER 2015
Intelligence assignment	111	109	112
Military security	15	5	6
Protection of secrets	28	36	4

As regards to the nature of the assignment, the status quo was maintained for the 'intelligence assignment' and 'military security'. However, there was a sharp decrease in the 'protection of secrets' (from 36 in 2014 to only just 4 in 2015).

NATURE OF THREAT	NUMBER 2013	NUMBER 2014	NUMBER 2015
Espionage	94	123	101
Terrorism (and radicalisation process)	6	7	4
Extremism	24	15	13
Interference	1	0	4
Criminal organisation	16	2	0
Other	13	0	0

In relation to the nature of the threat, the trend of using fewer SIM methods in the fight against terrorism and extremism continued in 2015 (30 in 2013, 22 in 2014, and only 17 in 2015). This may be surprising given the relative increase in these threats in 2015. There was also a downward trend in the use of SIM methods against the threat of 'espionage' in 2015 (101 compared to 123 in 2014).

233 Each authorisation may involve multiple interests and threats.

III.1.2. METHODS WITH REGARD TO STATE SECURITY

III.1.2.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015
Entry into and surveillance of or in places accessible to the public, using a technical device	109	86	86
Entry into and searching of places accessible to the public, using a technical device	0	0	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator	0	0	0
Inspection of identification data for electronic communications, requesting the cooperation of an operator or direct access to data files	613 methods	554 methods	663 methods
Inspection of call data for electronic communications and requesting the cooperation of an operator	136	88	33
Inspection of localisation data for electronic communications and requesting the cooperation of an operator	244	248	361
TOTAL	**1102**	**976**	**1143**

As indicated above, the total number of authorisations for the use of specific methods by State Security has increased. In 2015, a significant increase could be noted in the 'Inspections of identification data' (554 in 2014 compared to 663 in 2015) and in the 'Inspections of localisation data' (from 248 in 2014 to 361 in 2015). However, 'Inspections of call data' decreased (from 88 to 33 in 2015). In relation to 'Observations', the number of monitored persons almost doubled (71 in 2014 compared to 141 in 2015).

III.1.2.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015
Entry into and surveillance in places not accessible to the public, with or without a technical device	6	9	6
Entry into and searching of places not accessible to the public, with or without a technical device	6	21	8
Setting up and using a fictitious legal person	0	0	0

234 In one case, the authorisation related to one of the protected professional categories, namely a lawyer, doctor, or professional journalist.

NATURE OF EXCEPTIONAL METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015
Opening and inspecting post, whether or not entrusted to a postal operator	6	18	5
Collecting data on bank accounts and banking transactions	11	8	6
Penetrating an IT system	12	18	16
Monitoring, intercepting and recording communications	81	86	87
TOTAL	**122**[234]	**156**	**128**

The decrease in the number of exceptional methods used is due mainly to the sharp decrease in the number of 'Searches' (9 in 2015 compared to 21 in 2014) and the number of cases of 'Opening post' (18 in 2014 compared to only 5 in 2015). This is in contrast to the number of cases of 'Listening to communications' that continued to rise slightly (from 81 in 2013, to 86 in 2014, and 91 in 2015).

III.1.2.3. Interests and threats justifying the use of special methods

The following table lists the threats (and potential threats) for which State Security issued authorisations for the use of specific and exceptional methods. Of course, a single method may be directed against multiple threats. State Security may use specific methods in the context of all threats falling within its competence (Article 8 of the Intelligence Services Act). Exceptional methods may not be used in the context of extremism and interference. However, they are allowed in the context of the process of radicalisation that precedes terrorism (Article 3, 15° of the Intelligence Services Act). The Act uses the following definitions (free translation):

1. Espionage: seeking or providing information which is not accessible to the public and the maintenance of secret relationships which could prepare for or facilitate these activities;
2. Terrorism: the use of force against persons or material interests for ideological or political reasons with the aim of achieving its objectives by means of terror, intimidation or threats;

Process of radicalisation: a process whereby an individual or a group of individuals is influenced in such a manner that this individual or group of individuals is mentally shaped or prepared to commit terrorist acts;

3. Extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or aims, regardless whether they are of a political, ideological, religious or philosophical nature, which in theory or in practice conflict with the principles of democracy or human rights, with the proper functioning of democratic institutions or with other foundations of the rule of law;

4. Proliferation: trafficking in or transactions with respect to materials, products, goods or know-how which can contribute to the production or the development of non-conventional and very advanced weapon systems. In this context, this refers to the development of nuclear, chemical and biological weapons programmes and the transmission systems associated with them, as well as the persons, structures and countries involved;
5. Harmful sectarian organisations: any group with a philosophical or religious purpose or which appears to be such and which, in terms of its organisation or practices, carries out harmful illegal activities, causes harm to individuals or society, or violates human dignity;
6. Interference: an attempt to use illegal, fraudulent or clandestine means to influence decision-making processes;
7. Criminal organisations: any structured association of more than two people that endures over time, aiming to carry out criminal acts and offences by mutual agreement, in order to acquire direct or indirect benefits in terms of capability, where use is made of intimidation, threats, violence, trickery or corruption, or where commercial or other structures are used to conceal or facilitate the commission of crimes. This means the forms and structures of criminal organisations which have a substantial relationship to the activities referred to in the above threats, or which could have a destabilising impact at a political or socio-economic level.

Bearing in mind that various threats may be at play for each authorisation, the figures are as follows:

NATURE OF THREAT	NUMBER 2013	NUMBER 2014	NUMBER 2015
Espionage	359	319	253
Terrorism (and radicalisation process)	580	499	812
Extremism	246	267	171
Proliferation	15	33	30
Harmful sectarian organisations	9	0	0
Interference	8	10	10
Criminal organisations	9	8	0

The above figures on the use of SIM methods show that 'Terrorism' has remained the absolute priority at State Security (from 499 in 2014 to 812 in 2015). However, this means that fewer authorisations have been noted in relation to threats linked to 'Extremism' (171 compared to 207 in 2014) and 'Espionage' (from 319 in 2014 to 253 in 2015). The use of the available SIM resources has thus partly shifted to the fight against terrorism.

The competence of State Security is not determined merely by the nature of the threat. The service may take action only in order to safeguard certain interests:

- the internal security of the State and maintenance of democratic and constitutional order, namely
  a) the security of the institutions of the State and the protection of the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to every constitutional state, as well as human rights and fundamental freedoms;
  b) the safety and physical and moral protection of persons and the safety and protection of goods;
- the external security of the State and international relations: the protection of the inviolability of the national territory, the sovereignty and independence of the State, the interests of the countries with which Belgium is striving towards a common goal, and the international and other relationships which Belgium maintains with other States and international or supranational institutions;
- safeguarding the key elements of the scientific or economic potential.

Bearing in mind that different interests may be at play for each authorisation, the figures are as follows for 2015:

NATURE OF INTEREST	NUMBER 2013	NUMBER 2014	NUMBER 2015
Internal security of the State and maintenance of democratic and constitutional order	1177	1100	1258
External security of the State and international relations	1160	1075	1150
Safeguarding the key elements of the scientific or economic potential	11	10	4

III.2. ACTIVITIES OF THE STANDING COMMITTEE I AS A JURISDICTIONAL BODY AND A PRE-JUDICIAL CONSULTING BODY

III.2.1. STATISTICS

This section deals with the activities of the Standing Committee I in relation to specific and exceptional intelligence methods. Attention will only be paid to the jurisdictional decisions made in this regard. However, it must first be stressed

that the Committee subjects *all* authorisations to use special methods to a prima facie investigation, with a view to a referral or otherwise.

Article 43/4 of the Intelligence Services Act states that a referral to the Standing Committee I can be made in five ways:

- at its own initiative;
- at the request of the Data Protection Commission;
- as a result of a complaint from a citizen;
- by operation of law, whenever the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and has prohibited the use of the data;
- by operation of law, if the competent Minister has issued an authorisation based on Article 18/10, §3 of the Intelligence Services Act.

In addition, a referral may also be made to the Committee in its capacity as a pre-judicial consulting body (Article 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure). In that case, the Committee gives its opinion on the legitimacy of the use in a criminal case of intelligence acquired by means of specific or exceptional methods. The decision to ask for the Committee's opinion rests with the examining courts or criminal courts. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

METHOD OF REFERRAL	NUMBER IN 2013	NUMBER IN 2014	NUMBER IN 2015
1. At its own initiative	16	13[235]	16
2. Data Protection Commission	0	0	0
3. Complaint	0	0	0
4. Suspension by SIM Commission	5	5	11[236]
5. Authorisation by Minister	2	1	0
6. Pre-judicial consulting body	0	0	0
TOTAL	**23**	**19**	**27**

Once the referral has been made, the Committee may make various kinds of interim or final decisions. However, in two cases (1 and 2 below) a decision is made before the actual referral.

1. Decision to declare the complaint to be null and void due to a procedural defect or the absence of a personal and legitimate interest (Article 43, 4°, first paragraph of the Intelligence Services Act);
2. Decision not to take any action with regard to a complaint that is manifestly unfounded (Article 43, 4°, first paragraph of the Intelligence Services Act);

235 In two cases, the Committee's decision was only made in January 2015.

236 In one case, the referral was made in 2015 but the Committee's decision was made in 2016.

3. Suspension of the disputed method pending a final decision (Article 43, 4°, last paragraph of the Intelligence Services Act);
4. Request for additional information from the SIM Commission (Article 43, 5°, §1, first to third paragraphs of the Intelligence Services Act);
5. Request for additional information from the relevant intelligence service (Article 43, 5°, §1, third paragraph of the Intelligence Services Act);
6. Investigation assignment for the Investigation Service I (Article 43, 5°, §2 of the Intelligence Services Act). Reference is made here to the large body of additional information that is collected by the Investigation Service I in a more informal manner before the actual referral and information that is collected at the Committee's request after the referral;
7. Hearing of the SIM Commission members (Article 43, 5°, §4, first paragraph of the Intelligence Services Act);
8. Hearing of the head of service or the members of the relevant intelligence service (Article 43, 5°, §4, first paragraph of the Intelligence Services Act);
9. Decision about secrets relating to an ongoing criminal investigation or judicial inquiry to which the members of the intelligence services are privy, after consultation with the competent magistrate (Article 43, 5°, §4, second paragraph of the Intelligence Services Act);
10. Decision of the Chairman of the Standing Committee I, after having heard the head of service, if the member of the intelligence service believes that he must maintain the confidentiality of the secret information to which he is privy because its disclosure would be prejudicial to the protection of sources, the protection of the privacy of third parties, or the performance of the tasks of the intelligence service (Article 43, 5°, §4, third paragraph of the Intelligence Services Act);
11. Discontinuation of a method if it is still in use or has been suspended by the SIM Commission and an order stating that the information obtained through this method may not be used and must be destroyed (Article 43, 6°, §1, first paragraph of the Intelligence Services Act);
12. Partial discontinuation of an authorised method. This refers to a situation in which, for example, the use of a method is limited in time, and not to the situation in which several methods have been approved in a single authorisation by a head of service and the Committee discontinues only one of them.
13. Total or partial lifting of the suspension and ban imposed by the SIM Commission (Article 43, 6°, §1, first paragraph of the Intelligence Services Act). This means that the method authorised by the head of service was found to be partially lawful, proportionate and subsidiary by the Committee.
14. No competence of the Standing Committee I;
15. Unfounded nature of the pending case and no discontinuation of the method;

16. Advice given as a pre-judicial consulting body (Articles 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure).

The Standing Committee I must deliver a final decision within one month of the day on which a referral has been made to it in a particular matter (Article 43, 4° of the Intelligence Services Act). This period was respected in all dossiers.

NATURE OF DECISION	2013	FINAL DECISION 2013	2014	FINAL DECISION 2014	2015	FINAL DECISION 2015
1. Invalid complaint	0		0		0	
2. Manifestly unfounded complaint	0		0		0	
3. Suspension of method	0		3		2	
4. Additional information from SIM Commission	0		0		0	
5. Additional information from intelligence service	0		1		1	
6. Investigation assignment of Investigation Service	50		54		48	
7. Hearing of SIM Commission members	0		0		2	
8. Hearing of intelligence service members	0		0		2	
9. Decision regarding investigation secrecy	0		0		0	
10. Sensitive information during hearing	0		0		0	
11. Discontinuation of method	9		3		3	
12. Partial discontinuation of method	5		10		13	
13. Lifting or partial lifting of ban imposed by SIM Commission	2	23	0	17	4	26
14. No competence	0		0		0	
15. Lawful authorisation / No discontinuation of method / Unfounded	7		4		6	
16. Pre-judicial advice	0		0		0	

The Standing Committee I made 26 decisions in 2015, compared to 17 in 2014. This increase was due to the fact that the Committee itself intervened more often in 2015 (from 13 to 16 times), but also because the SIM Commission suspended authorisations more often (from 5 times in 2014 to 11 times in 2015).

It is worth mentioning that the Standing Committee I also heard members of the SIM Commission for the first time, in two dossiers.

III.2.2. DECISIONS

The final decisions delivered by the Standing Committee I in 2015 are briefly presented below. The summaries have been stripped of all operational information. Only those elements relevant to the legal issue have been included. The Committee had to take the necessary care in this regard, as many of the decisions needed to be classified (seven as CONFIDENTIAL; five as SECRET; two as TOP SECRET). The Committee has therefore sometimes had to refrain from explicitly including certain elements of the legal issue.

The decisions have been divided into five categories:

- legal or procedural requirements prior to the implementation of a method;
- justification for the authorisation;
- proportionality and subsidiarity requirements;
- legality of the method in terms of the applied techniques, data collected, duration of the measure, and nature of the threat;
- consequences of an unlawful method or an unlawfully implemented method.

Where relevant, some decisions are included under several categories.

III.2.2.1. Legal or procedural requirements prior to the implementation of a method

III.2.2.1.1. Prior notification to the SIM Commission

A specific method may be used only after notification of the authorisation has been given to the SIM Commission (Article 18, 3°, §1, second paragraph of the Intelligence Services Act). In dossiers 2015/4355, 2015/4356 and 2015/4199, the Commission was notified of an authorisation although the method had already been started earlier, or the Commission was given late notice of the extension of the method. The SIM Commission therefore suspended the part of the methods that occurred before the notification. In each case, the Standing Committee I confirmed those decisions.

III.2.2.1.2. Proposal for authorisation, assent and allowing use of an exceptional method

An intelligence service made a proposal for authorisation to use a tapping measure for one month (dossier 2015/4170). The SIM Commission gave its assent for this purpose. However, the final authorisation from the head of service allowed the tapping measure for 48 hours (and thus not for one month). Although this was in accordance with the assent, the Committee stated that '*this reduction of the period is not a problem*' (free translation).

A different problem arose in dossier 2015/3713. The intelligence service was authorised to monitor the communications of a target for two months. The method did not end once the period expired, but the service forgot to request an extension. The service noticed this itself after a few days and notified the SIM Commission. The SIM Commission suspended the method from the end of the first (and lawful) mandate. The Committee decided that it '*must find that the method was unlawful from midnight on [xxx] 2015, in view of the absence of a decision to extend the method*' (free translation).

In a third dossier (2015/3718), authorisation was granted to monitor a certain mobile telephone belonging to a target. But the service proceeded to monitor a second telephone that the target used. When it discovered this, the SIM Commission partially suspended the method since there was no draft authorisation for this purpose and no assent had been obtained. '*Whereas the SIM Commission rightly stated in its decision on partial suspension that it had not granted any assent for that part of the method. It then rightly announced a partial suspension with regard to the second mobile telephone*', according to the Committee (free translation).

Lastly, in dossier 2015/3545, the SIM Commission issued a negative opinion in respect of a draft authorisation. The head of service still authorised the exceptional method in error. When the error came to light, the method was immediately halted. It was also subsequently declared unlawful by the Committee. '*Whereas in the absence of an assent of the SIM Commission, the exceptional method cannot be implemented in view of Article 18/10 §3, second paragraph, and no appeal is possible against that decision of the SIM Commission*' (free translation).

III.2.2.1.3. Mandatory information in the authorisation

In four dossiers, the Standing Committee I had to consider whether certain details must be included in an authorisation granted by a head of service. These details included the date of the decision, the name of the target, and the correct statutory provision in relation to the service's competence.

In this case, the authorisation for a specific method was not dated (dossier 2015/4065). The Committee decided that this did not invalidate the decision,

contrary to what is stipulated in Article 18/10 §2, first paragraph of the Intelligence Services Act for exceptional methods.

By definition, the name of the target also does not have to be stated in the decision (dossiers 2015/4064 and 2015/4065). The Committee decided that since stating the identity of a target is not required by law and that he was identifiable in another manner, there was no problem in assessing lawfulness, proportionality and subsidiarity in this case. The Committee also emphasised that the obligations of confidentiality by which a member of an intelligence service is bound cannot preclude the controlling task, as described in Article 43, 5°, §§1 and 4 of the Intelligence Services Act.

In the last dossier (2015/3687), the intelligence service involved quoted an incorrect statutory provision. The service wished to use a technical resource to determine where and when a target used his mobile telephone. The numbers that he contacted could then be identified. The Committee noted that the service '*wrongly relied on Article 18, 4° of the Intelligence Services Act in conjunction with Article 18, 7°, §1, first paragraph of the Intelligence Services Act as the legal basis for the method*' (free translation). Article 18, 4° of the Intelligence Services Act provides only for the observation of persons, property, places or events. The technical resource used was employed only to identify telephone numbers. The Committee held that '*the operation as a whole must be considered when classifying the method*' (free translation) and that the service should therefore have relied only on Article 18, 7°, §1, first paragraph of the Intelligence Services Act for both parts of the method. However, this did not make the method unlawful.

III.2.2.1.4. Emergency procedure when requesting information from an operator

An intelligence service urgently proceeded to inspect, identify and locate the call data of a certain telephone (Article 18, 7° §2 and Article 18, 8°, §2 of the Intelligence Service Act) (dossier 2015/4171). The required oral decision of the head of service was confirmed by a reasoned written decision. Notice of this decision was given to the SIM Commission, which required additional information regarding the duration of the method. However, under reference to an earlier ruling (dossier 2011/227), the Committee noted that a number of other elements were missing from the decision: the name of the intelligence officer making the request, the time and date of the request, and the time and date of the written confirmation. '*Whereas the absence of information regarding the above elements does not permit the Standing Committee I to assess whether the conditions as set out in Articles 18, 7°, §2 and 18, 8°, §2 of the Intelligence Services Act, for relying on the procedure for an urgent request, have been met*' (free translation). At the request of the Committee, the service

concerned was able to supply this information. The method was therefore found to be lawful.

III.2.2.1.5. Legitimacy of the emergency procedure

Since an exceptional method had to be used very urgently, the intelligence service asked the chairman of the SIM Commission whether it was possible in that case to obtain a very quick decision from the full Commission (dossier 2015/3530). It would otherwise have to follow the emergency procedure under Article 18, 10°, §4 of the Intelligence Services Act. The chairman recommended using this exceptional procedure since it would have been impossible, in his opinion, to convene the Commission that same day. They also agreed to obtain only the chairman's oral opinion. A few days later, the chairman confirmed his oral opinion and, pursuant to Article 10 of the Royal Decree of 12 October 2010, he shared his decision with the other members of the Commission. The Committee decided that '*the chairman of the SIM Commission held that it was not possible to convene the Commission on a Friday afternoon, for reasons of his own and over which it is not for the Standing Committee I to express an opinion; Whereas the Standing Committee I nonetheless notes that this decision was made on a Friday afternoon, during normal office hours, and that if one or more members of the SIM Commission are unable to act, substitute members are appointed who can be contacted to replace the member or members unable to act; Whereas the Standing Committee I must assess in this case whether the decision of an intelligence service to rely on the emergency procedure is lawful or not; Whereas the urgency of the situation and seriousness of the threat in this case meant that the procedure referred to under Article 18, 10°, §4 had to be used without delay*' (free translation).

The method was therefore authorised for 48 hours. However, since this period ended during the weekend and it was essential to continue with the method, it had to be decided whether the extension would be applied for via the ordinary or the exceptional procedure (dossier 2015/3531). The service in question once again contacted the chairman of the SIM Commission for this purpose. Both the service and the chairman were aware that an extension of the method would be needed and that this would have to be done during the weekend. Even so, the chairman opted not to convene his Commission immediately or during the weekend. The Committee noted that '*a meeting of the SIM Commission before the expiry of the 48 hours was possible by calling the other members and/or their substitutes; Whereas the Standing Committee I must assess in this case whether the decision of the intelligence service to rely on the emergency procedure is lawful or not; Whereas in similar circumstances, the Standing Committee I has already decided that if it is impossible, for whatever reason, to convene the SIM Commission for a decision on an exceptional method, the intelligence service may use another statutory procedure, such as approaching the*

competent minister without waiting for the expiry of the four-day period under Article 18, 10°, §3 of the Act (SIM dossiers 2012/1308 – 2012/1309 – 2013/2327 and 2013/2328' (free translation).

III.2.2.2. Justification for the authorisation

Decisions to use special methods must be justified in an adequately accurate manner. As is the case every year, the Standing Committee I has had to draw attention to this obligation several times.

An intelligence service wished to obtain as much information as possible about the Belgian contacts of several foreign mobile telephone numbers (dossier 2015/4101). It also wished to gather certain localisation and identification data for this purpose. Since no justification was provided on these aspects of the method, '*the two methods are unlawful in the absence of justification*' (free translation) (dossier 2015/4101).

The Committee found that justification was also lacking for the methods in the authorisation in dossiers 2015/4150 and 2015/4170. It therefore decided these methods were also unlawful.

In its decision to perform an observation, the head of the service stated in one section of the decision that the method would last two months, but the text later referred to a one-month period (dossiers 2015/4163). The Committee also found that in the past, a method that only lasted one month was proposed in each case for the same target. '*Whereas, partly in view of the contradiction regarding periods in the SIM decision, the Standing Committee I therefore finds that the method can be applied for a one-month period only*' (free translation). The Committee therefore decided that the method was partially unlawful.

III.2.2.3. Proportionality and subsidiarity requirements

A method not only has to comply with a number of statutory requirements, but it must also be proportional to the underlying threat and may not be more intrusive than is necessary.

An intelligence service wanted to identify the means of communication of a person, inspect his communication data, and localise the origin and destination of the communications for an extended period (15 months) (dossier 2015/3818). The services wanted to determine whether or not that person '*could be involved or not in a recruitment process by a foreign country*' (free translation). While the Committee found that '*the potential threat is real, given the origin of the target and the practices of the country involved, and that ordinary methods do not make it possible to obtain the required information*' (free translation), it did have questions relating to proportionality: '*the method for identification (Article 18, 7°, §1, first paragraph) and inspection (Article 18, 8°, §1, first paragraph) make it possible to obtain useful information but localisation (Article 18, 8°, §1, second*

paragraph) seems disproportionate at this stage in relation to the real seriousness of the described threat, in view of the more intrusive nature of this method' (free translation).

In two dossiers (2015/3999 and 2015/4000), the service wished to apply a number of specific methods to a target for a six-month period, whom it was known would be on Belgian soil for a few days. The service confirmed that the methods would be used only at that moment. The Committee decided, in view of the specific elements of the case, that the six-month period was disproportionate and held that '*under the current state of affairs, the method can be applied for one month only*' (free translation).

In dossier 2015/4154, the service involved wished to use three specific methods: tracing call data, as well as identifying and localising every Belgian number in contact with a foreign number. The Committee held that '*the principles of proportionality and subsidiarity are complied with only insofar as the method of localisation is limited to the localisation of the traced telephone numbers at the moment of communication with the foreign target. The identified numbers can indeed never be subject of general localisation, thus also beyond the contacts they have with the foreign target'* (free translation). The Committee therefore found that '*the specific method […] as specified above, is lawful*' (free translation).

If an intelligence service wishes to extend the observation of a specific location with a fixed camera by one year (the method had already been used for several years by then), the question of proportionality arises (dossier 2015/4199). The Committee pointed out that '*the Intelligence Services Act does not lay down any special procedures for extending or renewing a specific method, except for the fact that the head of service's new decision must comply with the conditions set out in Article 18, §3 of the Act; that the Act does not impose stricter conditions for assessing proportionality and subsidiarity*' (free translation). Since the camera images could provide information about an organisation that is regarded as a terrorist organisation and because intelligence work necessarily takes a long time, the Committee had no objection to this extension. The Committee also pointed out that earlier work had produced results. '*The Committee has already ruled on several occasions that a one-year period is reasonable given the assignments of the intelligence services that often entail working in the medium to long term; that this particular detail of the nature of intelligence work differs essentially from police work that is specifically aimed at tracing the perpetrators of a crime*' (free translation).

Finally, in the last three dossiers, the Committee has reverted to its established case law which states that the results of earlier methods must first be known in certain cases before it can be determined whether the subsequent methods are proportional and subsidiary.

For example, an intelligence service wished to use specific methods to obtain maximum data in regard to a certain mobile telephone number: the inspection

of incoming and outgoing calls; the localisation of calls, for which purpose the service wanted to go back a year in time; the identification of the numbers obtained if they could not be obtained via an ordinary method; the history of the users of the mobile telephone numbers since their first activation; checking in which mobile telephones this number has been used, and – finally – checking the identity of the users of these telephones. The Committee held that this last method was unlawful. The results of the other methods had to be obtained first (dossier 2015/3842).

The same problem arose in dossier 2015/4101. An intelligence service wished to obtain numerous details about the Belgian contacts of several foreign mobile telephone numbers. For this purpose, the service would first inspect the call data of those foreign numbers in order to filter the Belgian numbers on that basis. However, in the same decision, the service wanted to simultaneously perform a whole series of methods on the numbers obtained. The SIM Commission proceeded with a partial suspension: '*given that it is not possible at the moment of notification to subject the results of methods that are still to be performed to the legality, subsidiarity and proportionality test before proceeding with a special intelligence method*' (free translation). The Committee also found that the service should first determine whether and which Belgian numbers were in contact with the foreign numbers and identity the users. '*Whereas it is not currently possible to assess the lawfulness, proportionality and subsidiarity of any other method relating to these Belgian numbers, which may be identified via the legal methods*' (free translation).

In the last dossier (2015/4322), the service wished to first inspect the call data from a certain mobile telephone and then identify the persons with whom the target had been in contact during the last year. However, the intention was to also inspect the call data of the other telephone numbers of this target. The Committee held that the latter was not permitted. '*Whereas the third requested method relates to several numbers that are not yet known and for which the service requests inspection of incoming and outgoing calls and their localisation; that even if the holder of the mobile telephone that is the subject of the method is known, it is possible that he has used anonymous prepaid cards, which would have to be subject to special tracing, or that he has used cards that were loaned to him by other people who may or may not have ties to the person targeted; that in view of the absence of a more precise identification, it is not currently possible to assess compliance with the principles of proportionality and subsidiarity for these obtained numbers*' (free translation).

III.2.2.4. Legality of the method in terms of the techniques applied, data collected, duration of the measure, and nature of the threat

The intelligence services obviously cannot use just any method to gather information about someone. The law sets clear boundaries on various levels: For

what kind of threat and in order to protect which interest may a method be used? Which acts may and may not be performed in this regard? By whom, in respect of whom, and in respect of which data? How long may a technique be used? May the measures be used outside Belgium? And so on… The Standing Committee I has explained some of these boundaries in some decisions.

III.2.2.4.1. Specific (and serious) threat against a specific interest to be protected

An intelligence service wished to apply a special method to a person who could potentially provide useful information but who did not constitute a threat himself (dossier 2015/4064). The Committee stressed that the law did not provide for the use of SIM methods in such cases. However, it was clear from the decision that the person involved was developing activities that fell under the service's scope of competence. The Committee therefore held that those activities justified the method.

The Committee held in dossier 2015/4320 that the special methods were used partly for a problem that fell outside the particular service's scope of competence. The service wished to observe a specific person who was on the run at that time and a number of other persons who were suspected of concealing the fugitive. The Committee held that '*the person who is the initial target of the method has not been located and that person is moreover being actively sought by the judicial authorities for his participation in very serious unlawful acts; that it is therefore not possible at the moment to observe this person and, if he is discovered, the services must inform the judicial authorities so he can be arrested; whereas there is currently no intelligence purpose in respect of this person, but there is a judicial purpose that must, moreover, take precedence*' (free translation). This reasoning did not apply to *against them; that it is indeed necessary for the intelligence service to be able to better identify and monitor the persons who give any form of logistic support to the person at large*' (free translation).

III.2.2.4.2. Cooperation by foreign services

The Standing Committee I has already held that the Belgian intelligence services may also cooperate with foreign partner services in relation to special methods, on condition that the Belgian service retains actual control over the method used.[237]

The Committee repeated that case law in dossier 2015/3823. A Belgian intelligence service granted authority to listen to and record conversations. A special feature of the case was that the monitoring equipment would be installed by a foreign intelligence service. The foreign service would only examine any

[237] See for example STANDING COMMITTEE I, *Activity Report 2013*, 83 and *Activity Report 2014*, 85–86.

conversations when the target was abroad. The information obtained would then be shared with the Belgian service. According to Article 13, 1°, §2, fifth paragraph of the Intelligence Services Act, the SIM Commission had consented to the foreign agents installing the technical resource. The Committee specified that '*intervention by [foreign] colleagues can be limited to only necessary and direct help or assistance, insofar as this is essential for the success of the method. That the [Belgian service] must therefore oversee this method itself very strictly in order to be and remain master of the operation on Belgian soil. Whereas the Standing Committee I also instructs the [Belgian service] to strictly oversee the further development of the method and, more specifically, to oversee what happens with the recorded communication. That it seems, after all, that the conversations will firstly be processed by the [foreign] service on [its] soil and only subsequently be shared with the [Belgian service]. That in this regard, the [Belgian service] must also be and remain the master of the operation and comply with the necessary obligations regarding the transcription of relevant passages and later destruction of the recording*' (free translation). As additional information showed that the Belgian service could comply with these requirements, the Committee found that the authorisation was lawful.

III.2.2.4.3. The SIM Act and the Vienna Convention on Diplomatic Relations of 18 April 1961

The Committee once again made a decision (dossier 2015/3805) that featured the Vienna Convention of 1961.[238] An intelligence service wished to use a specific method. Because the SIM Commission wanted to check whether the method was consistent with the requirements of this Convention, it asked the service twice for additional information. Nonetheless, the Commission did not gain an adequate insight into the precise nature of the method and proceeded to suspend it. The Standing Committee I held that this suspension on was correct, given that there was a possibility that the method contravened the Convention.

III.2.2.5. Consequences of an unlawful method or an unlawfully implemented method

An intelligence service wished to apply an exceptional method in conjunction with several specific methods. Since it turned out that the exceptional method had not been lawfully requested (see III.2.2.1.2 above – dossier 2015/3545), the SIM Commission also suspended the specific methods '*due to their direct connection with the exceptional method*' (free translation). However, the Standing Committee I took a different view. '*Whereas the Standing Committee I found that the specific methods were not linked with the exceptional methods to such a degree*

238 Also see in this regard STANDING COMMITTEE I, *Activity Report 2014*, 85.

that the fate of the latter automatically determined the fate of the other methods and that the head of service, in his proposed decision and in the decision itself, has adequately justified these specific methods, methods that are still important for the service' (free translation).

III.3. CONCLUSIONS

Based on the figures from operating year 2015, the Standing Committee I has drawn the following general conclusions:

- Whereas a decrease was registered in 2014, the number of special intelligence methods in 2015 returned to 2013 levels. The growth in comparison to 2014 resulted entirely from specific methods used by State Security (from 976 in 2014 to 1,143 in 2015). There was a significant decrease in both the special methods used by GISS and the exceptional methods used by State Security.
- The increase in specific methods at State Security was mainly in the number of 'Inspections of identification data' (from 554 to 663) and from 'Inspections of Localisation data' (from 248 to 361). 'Inspections of call data' decreased (from 88 to 33).
- Despite the slight decrease in the number of exceptional methods at State Security, a slight increase can be noted in the number of tapping measures: from 81 in 2013, to 86 in 2014 and 91 for 2015.
- In relation to GISS, the trend of using fewer SIM methods in the fight against terrorism and extremism seems to have been continued in 2015 (30 in 2013, 22 in 2014, and only 17 in 2015). This may be surprising given the relative increase in these threats in 2015. There was also a downward trend in the use of SIM methods against the threat of 'Espionage' in 2015 (101 compared to 123 in 2014).
- In relation to State Security, the number of SIM methods pertaining to 'Terrorism' has not only increased in absolute figures but also increased enormously in relation to the other threats, such as 'Extremism' and 'Espionage'. The use of the available SIM resources has thus partly shifted to the fight against terrorism.
- It should also be noted in relation to exceptional methods that the emergency procedure, in which only the chairman of the SIM Commission is asked for advice, is being used more and more: 11 times in 2013; 19 times in 2014, and 25 times in 2015.
- The Standing Committee I made 26 decisions in 2015, compared to 17 in 2014. This increase was due to the fact that the Committee intervened more itself in 2015 (from 13 to 16 times) but also because the SIM Commission suspended more often (from 5 times in 2014 to 11 times in 2015).

CHAPTER IX
RECOMMENDATIONS 2015

Based on the investigations concluded in 2015, the Standing Committee I has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred to individuals by the Constitution and the law (IX.1), the coordination and efficiency of the intelligence services, CUTA and the support services (IX.2) and, finally, the optimisation of the review capabilities of the Standing Committee I (IX.3).

IX.1. RECOMMENDATIONS RELATED TO THE PROTECTION OF THE RIGHTS CONFERRED TO INDIVIDUALS BY THE CONSTITUTION AND THE LAW

IX.1.1. SECURITY INVESTIGATIONS AND SOCIAL MEDIA

The Committee recommends that people who are the subject of a security investigation should be given express notice of the fact that the consultation of open sources – including public profiles on social media – is one of the methods for gathering information that can be used for the purpose.[239]

IX.1.2. THE BATTLE AGAINST EXTREMISM IN THE ARMY VERSUS FUNDAMENTAL RIGHTS

In order to avoid rushing to judgement, the monitoring of radical Islamism in the army requires a critical mindset and caution when analysing the conduct of people. GISS must be able to distinguish between conduct that, in the light of freedom of religious worship, is in accordance with normal religious experience and, on the other hand, behaviour that points to radical and sectarian derailment.[240]

---

239 See 'Chapter II.5. Personnel of the intelligence services and social media' and 'Chapter II.6. Personnel of CUTA and social media' in this regard.

240 This recommendation stems from the investigation into tracking down and monitoring extremist elements among Defence personnel (Chapter II.3).

IX.1.3. ACCURATE INFORMATION AND THE RIGHTS OF CITIZENS[241]

The Standing Committee I recommends, in relation to requests for information from foreign services or the placement of people on lists, that the intelligence services take special care regarding the accuracy of their intelligence and the legal validity of transmitting information (both nationally and internationally), in view of the potential consequences for those involved.

An attempt must be made, moreover, to achieve a balance between collective security requirements on the one hand and the rights of citizens who appear on such lists on the other hand. This could be via multilateral arrangements regarding the creation of an ombudsman position, for example, or external oversight of these lists. After all, national bodies such as the Standing Committee I currently do not have jurisdiction to check the validity and lawfulness of these lists and their contents.

IX.2. RECOMMENDATIONS RELATED TO THE COORDINATION AND EFFICIENCY OF THE INTELLIGENCE SERVICES, CUTA, AND THE SUPPORT SERVICES

IX.2.1. RECOMMENDATIONS ON THE JOINT INFORMATION BOX[242]

The Standing Committees I and P formulated various recommendations in order to fundamentally review the Joint Information Box (JIB) system, a list managed by CUTA with the names of people and organisations that play a key role in the radicalisation process:

- The role of each cooperating service needs to be clarified. This also applies to CUTA, which, as the assessment service, can prove its added value in relation to the information that is provided by the support services. CUTA takes an overly minimalist approach to its role as a threat assessment body in relation to the JIB list. CUTA should play a more active role in coordinating the analysis. The service can estimate the specific threat that each entity poses in relation to radicalisation;
- On the other hand, it seems appropriate for another service (e.g. the Governmental Coordination and Crisis Centre) to be designated and assume responsibility for coordinating the implementation of the measures;

241 See 'Chapter II.8. Wrongfully monitored by the intelligence services?'

242 See 'Chapter II.1. Joint supervisory investigation into the Joint Information Box of CUTA'.

- Working with parameters provides the guarantee that inclusion in the JIB is not random. A system of criteria is indeed necessary to maintain objectivity;
- The Standing Committees I and P stress the need to include information in the JIB that comes from local and national services in the field. The local levels must be able to incorporate their findings into the system and at least receive feedback on the inclusion or non-inclusion in the list and any measures. It is indeed the case that the first signs of radicalisation are often found at local level (via the community police officer or local units of the intelligence services, for example). The Committees hold the view that a thorough procedure should be worked out to create the most adequate possible flow of information, with respect for the existing structures;
- Information and analyses must be distributed as quickly and as widely as possible among the players involved, obviously taking into account any classification and the 'need to know'. Where necessary, certain people (for example at regional or local level) must have a security clearance;
- Given the diversity and specific nature of measures that must or can be taken with regard to carriers of radicalisation[243], the proposal, imposition, detailing, and monitoring of measures must be entrusted, if necessary, to better placed bodies or working groups, so JIB players can focus on their core task: submitting and analysing intelligence. Where relevant, parties other than federal security services must be included in the debate. After all, detecting, neutralising or limiting the radicalising effect of a person or a group cannot occur at federal level alone.

The Standing Committees I and P announced their support for all plans made in this regard so that the JIB may in the near future develop into the instrument of choice for identifying and managing the carriers of all forms of radicalisation in our society as widely as possible. The Committees also stated that they would review the changes announced by CUTA to the working procedure of the JIB at a later stage.

IX.2.2. RECOMMENDATIONS ON MANAGING AND AUDITING SPECIAL FUNDS[244]

IX.2.2.1. A legal framework

A statutory or regulatory provision must be drawn up that clearly and precisely describes the management of the special funds. It is, moreover, absolutely necessary for similar controls to be introduced, both internally and externally,

243 This refers to people who have a radicalising effect on third parties.
244 See 'Chapter II.2. Managing, use and audit of "special funds".'

for both intelligence services. Among other things, the regulatory provisions must lay down the procedures according to which the services involved may retain any annual surpluses. It is also appropriate to adequately involve the services in the budget cycle.

IX.2.2.2. Specific recommendations concerning special funds and GISS

- The amounts that GISS receives for its normal expenses (that covers personnel, operating, and investment costs) and the annual amount of the special funds must be clearly identifiable in the Budget Act for Defence that Parliament approves each year.
- GISS must adapt the organisation of the 'sub-funds'. This must be done taking into account the purpose of some funds (for example, operational autonomy for certain divisions). As far as the other funds are concerned, the Committee deems it advisable to centralise their management.
- GISS must draw up a standard and integrated regulatory framework for the funds (in their adapted form). More specifically, the procedures for expenditure must be formalised to enable efficient control by the hierarchy and provide added value. The accounting records of these funds should also be available as a control instrument by using a standard and reliable IT system.
- GISS and the other Defence services must find regular funding for expenditures to which the criteria of 'confidentiality' and 'extreme urgency' do not apply. In this way, more resources will be released for operational costs.

The Committee pointed out that changes to the regulations may not jeopardise GISS assignments. It emphasised that these funds were absolutely essential for GISS operations. The recommendations of the Committee may not result in this service losing the use of part of the funds. According to the Committee, the management of the GISS funds must be optimised in consultation with the service. The Committee also stated that GISS must search on the one hand for alternative financing together with other Defence services and, on the other hand, strive on the basis of the current available funds to integrate the use of those funds into its security strategy.

IX.2.2.3. Specific recommendations concerning special funds and State Security

- State Security must add value to the performance of the duties of the special accounting officer by drawing up a precise job description, by training personnel for this position, and by organising continued professional development in this regard;

– State Security must ensure that the continuity of the position of special accounting officer is guaranteed. More specifically, this requires the appointment of a deputy[245] and drawing up of work procedures.

IX.2.2.4. Regular information sessions

The Committee urges the organisation of regular information sessions on the conditions for using the funds to be presented for all personnel of both GISS and State Security.

IX.2.3. THE USE OF SOCIAL MEDIA BY PERSONNEL OF STATE SECURITY AND GISS[246]

The Standing Committee I recommends that the management boards of the intelligence services should take the initiative to make the regulatory framework (laws, Royal Decrees, internal directives, code of ethics, etc.) explicit in relation to the general attitude towards loyalty and prudence on social networks and in relation to the control measures that can be used for that purpose.

The Committee previously[247] recommended that State Security, in implementation of Article 17 of the Royal Decree of 13 December 2006 on the status of officials of the External Services of State Security, should draw up a proposal for a code of ethics and submit this for approval to the Minister of Justice. The Committee recommends that the said code should describe what is meant by the obligation of neutrality and discretion on the part of State Security officials. The Committee also called for strict compliance with this code through a quick and consistent application of the disciplinary procedure in case of non-compliance. The Standing Committee I repeats this recommendation and believes that such a code of ethics must set rules of conduct for the 'proper use' of social media.[248]

The Committee further orders the management of the services to adopt special measures that indicate how the use of ICT and the behaviour of agents on social network services, both for professional and personal purposes, can be monitored in a proactive manner. These measures must naturally take account

---

245 This recommendation has since been implemented with the appointment of a deputy special accounting officer.

246 See 'Chapter II.5. Personnel of the intelligence services and social media'.

247 STANDING COMMITTEE I, *Activity Report 2011*, 181 (IX.2.8 A code of ethics for State Security agents').

248 The Committee also holds the view that the opinions and rules in the charters for the use of social networks as proposed by the Federal Police, the Belgian Cyber Security Guide, or the French and American military authorities can serve as a useful source of inspiration in drawing up that code of ethics, provided that the special assignments entrusted to members of the intelligence services and the conditions regarding confidentiality and secrecy under which they must work are taken into account.

of the principles regarding purpose, proportionality, and transparency in relation to the special assignments of the services.

A procedure must also be introduced that allows for any damage to the person concerned and the service to be assessed in case of an incident, to respond in an appropriate way, and to adopt corrective measures in order to avoid repetition.

Notwithstanding any withdrawal of the security clearance, the hierarchical authorities must consider imposing possible disciplinary sanctions in case of a proven contravention of the security rules and the duty of discretion.

Lastly, the services must preventively draw their agents' attention to the risks associated with their presence on social media and must be able to formulate general recommendations and adopt security measures that indicate which precautions must be taken and which conduct can be avoided on the networks concerned.

IX.2.4. THE USE OF SOCIAL MEDIA BY PERSONNEL OF CUTA[249]

The Standing Committees I and P have formulated the following recommendations with regard to the use of social network services by personnel of CUTA:

- The efforts that the management of CUTA have already made to tackle the security risks associated with the presence of its personnel on social network sites (more specifically in the context of the steering committee) must be continued;
- Initiatives must be taken to make the regulatory framework of CUTA (laws, Royal Decrees, internal directives, and code of ethics) explicit in relation to the general attitude towards loyalty and prudence that is expected of its employees on social networks and in relation to the monitoring measures that can be used for that purpose;
- The National Security Council (ANS/NVO) must give everyone who is the subject of a security investigation express notice that the consultation of open sources, including public profiles on social media, is one of the methods for gathering information that can be used in that regard;
- Rules for 'proper use' ought to be drawn up for the personnel who make use of those new means of communication;
- As part of the existing rules[250], targeted searches ought to be introduced to check whether those rules – which could always be adapted to the evolution

249 See 'Chapter II.6. Personnel of CUTA and social media'.

250 More specifically, Collective Labour Agreement no. 81 on the protection of the privacy of employees in relation to the control of electronic online communication data (e-mails, internet use, internet, intranet, extranet, SMS, chat, discussion forums, etc.).

of the means of communication – are applied properly, both preventively by means of random checks and reactively in the case of incidents or indications of dysfunctions linked to the risky behaviour of personnel on social media;
- Personnel of CUTA must be informed about how the use of ICT and the conduct of employees on social network sites, whether for professional or private purposes, can be proactively controlled. These provisions must naturally take account of the principles of purpose, proportionality, and transparency, adapted in this case to the special assignment of the services;
- A procedure must be introduced to estimate the damage and respond in order to intercept and/or manage any inappropriate circulation of information that is harmful for the employee and, by extension, for the service. According to the example of the OPSEC[251] methodology, this procedure would have to provide corrective measures that must be adopted in order to avoid a repeat of such an incident and limit its consequences;
- CUTA employees must be clearly informed about the fact that the following measures can be adopted if it is proven that the security measures and duty of discretion have been contravened:
  a) the withdrawal of the security clearance;
  b) a disciplinary hearing in accordance with the disciplinary system for CUTA analysts;
  c) an end to the secondment of the employee concerned and his/her referral to the authorities of the service of origin when a seconded employee is involved.
- The application of the above principles and measures must be assessed taking account of the specific tasks entrusted to those involved within the intelligence community and the conditions of confidentiality and secrecy under which they must work.

IX.2.5. INTERNATIONAL RELATIONS OF CUTA[252]

Having due regard for the respective political and managerial responsibilities of each body that is involved in making international contacts, the Standing Committees I and P have formulated the following recommendations:

---

251 OPSEC or 'Operations Security' is defined as '*a process that involves the identification and protection of generally unclassified critical information or processes that can be used by a competitor or adversary to gain real information when pieced together. Although the information sought under OPSEC isn't classified, it could give a competitor or other adversary advantage. OPSEC focuses on the identification and protection of information that could give enemies clues or capabilities to put one in a disadvantage*' in www.techopedia.com.

252 See 'Chapter II.7. International contacts of CUTA'.

- The contacts that CUTA makes with similar (or dissimilar) foreign services must be transparent and traceable as regards the competent ministers, FPS Foreign Affairs, and the Belgian police and intelligence services;
- The National Security Council must issue a directive in order to ensure specific international contacts of CUTA with similar foreign or international services in accordance with Article 8, third paragraph of the Threat Assessment Act.[253] To that end, it would seem necessary for the directive to explain what bodies can be strategic partner services of CUTA, which types of alliances can be entered into with those services, and how to determine whether or not they are 'similar'.[254]

According to the Standing Committees I and P, this directive would have to include at least the following rules:

- That CUTA must keep an updated list of the foreign services with which it maintains or wishes to maintain international contacts; that this list must be submitted to the National Security Council and will be published in the CUTA's six-monthly reports;
- That for this purpose, the support services involved and clients of CUTA must be informed and consulted before contact is made with a foreign service, similar or otherwise, more specifically State Security, GISS, the Federal Police, and FPS Foreign Affairs. After all, such contacts and forms of cooperation that could risk the political responsibility of the government and/or reputation of the country in the international community require a political evaluation and cover. In other words, the competent ministers must be adequately informed so that they can assume political responsibility at all times[255];
- That any contacts which CUTA wishes to make with certain foreign intelligence services must from now on be made via the channel of State Security or GISS;
- That any contacts which CUTA wishes to make with certain foreign police services must from now on be made via the channel of the Commissioner General, Department for International Police Cooperation (CGI) of the Federal Police;

---

253 Agreements have already been concluded between CUTA and State Security to provide a solution to the problems caused by certain international contacts of CUTA. However, the Committees held the view that a structural solution required the National Security Council to issue a directive in that regard.

254 The recommendation has since been implemented in the sense that the National Security Council issued such a directive during the course of 2016. However, it has not yet been assessed whether the directive has taken all the rules formulated below into account.

255 See also a previous recommendation along the same lines: STANDING COMMITTEE I, *Activity Report 2014*, 89 ('IX.1.3 Need for political cover for alliances').

- That the experts who are seconded from the police or intelligence services to CUTA must be involved in those contacts;
- That every bilateral contact made with a foreign service must be subject to a prior SWOT (Strength, Weaknesses, Opportunities and Threats) analysis;
- That every alliance thus entered into with a foreign service must be subject to a periodic evaluation on the basis of SWOT criteria;
- That, at the very least, a member of CUTA must draw up a written and detailed report for each foreign mission, setting out the contacts made and their nature; that these reports must be sent to the relevant police or intelligence services;
- That every disclosure of information to a third-party service must be noted in an appropriate register;
- That a list of the international contacts of CUTA and the participation of its employees in events abroad must be included in every six-monthly report that the service must draw up pursuant to Article 10 §4 of the Threat Assessment Act;
- That CUTA must draw up an internal directive to determine which practical and security rules must be followed when members of its management and/or personnel travel abroad as part of their professional activity;
- That CUTA makes use of secured international connections of the intelligence services when corresponding with foreign services;
- That CUTA itself no longer sends or distributes reports to foreign embassies.

On the other hand, the Committees deem it appropriate that both State Security and GISS invite CUTA to consultative meetings with foreign intelligence services, especially if these deal with information regarding threats that fall within the scope of competence of CUTA. CUTA could, moreover, make use of the opportunity to test hypotheses and obtain first-hand information. In this way, the services concerned could strengthen their mutual trust with a view to better cooperation.

These recommendations of the Standing Committees I and P are in keeping with their earlier joint position[256]:

- CUTA is not an intelligence service;
- it is not part of CUTA's remit to gather intelligence, in Belgium or abroad, even if only to fill gaps that it considers the intelligence services or support services to have left;
- it is important that this body ensures that there is absolutely no ambiguity regarding its legal mandate, both in its communication and its contacts with other Belgian or international services.

256 STANDING COMMITTEE I, *Activity Report 2011*, 125–128 ('II.5 A planned foreign mission by CUTA').

IX.2.6. THE BATTLE AGAINST EXTREMISM IN THE ARMY[257]

GISS must pay special attention to all signs of conversion to radical Islamism, among both civilian and military personnel of Defence. The same vigilance is warranted in respect of far-right tendencies and criminal motorcycle gangs, which are sometimes regarded as less problematic in the units.

The Committee therefore recommends that GISS command gives clear instructions in that regard to the competent divisions and tasks them with identifying unambiguous indicators of radicalisation with a view to compiling documentation about this problem.

To this end, GISS must ensure that all useful information channels are optimised. Broad attention must be paid, for example, to the quality of contacts with the different units and other services of Defence. Those in charge and the chiefs of police of the units must be made aware of the issue, more specifically via regular intelligence briefings.

Lastly, it is recommended that communication channels and procedures, both with the disciplinary authorities within Defence and with the police services and judicial authorities, should be evaluated. GISS must always be advised in due time of administrative measures, sanctions or convictions in relation to a Defence employee. This type of communication must occur more systematically so the measures to be adopted can be examined, particularly with regard to security clearances. Any problems in the flow of information must be brought to the attention of the minister so that he/she can remedy these problems.

IX.2.7. THE REVIEW OF THE SECURITY REGULATIONS OF GISS[258]

The Committee recommends that GISS should bundle all provisions relating to military security (including INFOSEC directives) into a single document (IF5). GISS confirmed in 2015 that it had started with this.

---

257 These recommendations stem from the investigation into tracking down and monitoring extremist elements among Defence personnel (Chapter II.3).

258 See 'Chapter II.9. Complaint regarding the disclosure of personal information by an intelligence agent to a third party'.

IX.2.8. A COMPREHENSIVE REPORT INTO SECURITY INCIDENTS[259]

GISS should draw up a comprehensive report of every security incident that examines and analyses all dimensions (not only technical, but also in relation to conduct), especially when the person involved holds a security clearance. This report must be forwarded to the competent security authority, together with any proposed decision.

IX.2.9. FINALISING THE WORK RULES[260]

The Standing Committee I recommends that State Security should quickly finalise and approve its work rules. This document must cover at least the aspects of working hours, sick leave and prevention. In relation to prevention, it is worth recommending that State Security quickly creates an appropriate structure in order to comply with its legal obligations. Among other things, State Security must recruit a prevention officer and set up a network of confidential advisers.

IX.2.10. SENDING ALL RELEVANT INFORMATION TO CUTA[261]

The Standing Committee I recommends that the intelligence services should systematically forward all relevant information and the results of investigations that they should conduct in relation to current cases to CUTA, even when such an investigation does not yield any results of evidential value.

IX.3. RECOMMENDATION RELATED TO THE EFFECTIVENESS OF THE REVIEW

IX.3.1. INTERNATIONAL RELATIONS OF CUTA

The Standing Committees I and P insisted that the contacts that CUTA makes with similar (or dissimilar) foreign services must also be transparent and traceable for both oversight bodies. The Committees further recommend that certain elements of those contacts be included in the activity reports that CUTA must send to both Committees via the National Security Council (Article 10, §4 of the Threat Assessment Act).

---

259 See 'Chapter II.9. Complaint regarding the disclosure of personal information by an intelligence agent to a third party'.

260 In this regard, see: 'Chapter II.10. State Security and the application of sick leave regulations'.

261 See: 'Chapter II.8. Wrongfully monitored by the intelligence services?'

APPENDIX

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT

[Amendments brought until 8/12/2016]

CHAPTER I – GENERAL PROVISIONS

Article 1
Both a Standing Police Services Review Committee and a Standing Intelligence Agencies Review Committee shall be established. In particular, review shall relate to:
1° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the police services on the one hand and the intelligence and security services on the other;
2° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the Coordination Unit for Threat Assessment;
3° The way in which the other support services satisfy the obligation laid down in Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.
An Investigation Service shall be established for each of these committees.

Art. 2
The review governed by this Act does not relate to judicial authorities nor to the actions taken by them in the exercise of the prosecution function. The review does not relate to the administrative police authorities either.
The review referred to in this Act is governed without prejudice to the review or inspection governed by or by virtue of other legislation. In the event of review or inspection governed by or by virtue of other legislation, the review referred to in

this Act relating to the activities, methods, documents and directives of the police services and of the intelligence and security services, shall only be undertaken to ensure fulfilment of the assignments provided for in this Act.

Art. 3
For the purposes of this Act, the following definitions shall apply:
1° "Police services": in addition to the local police and the federal police, the services that come under the authority of the public authorities and public interest institutions, whose members have been invested with the capacity of judicial police officer or judicial police agent;
2° "Intelligence and security services": State Security and the General Intelligence and Security Service of the Armed Forces;
3° "Coordination Unit for Threat Assessment": the service referred to in the Act of 10 July 2006 on threat assessment;
4° "Other support services": the services other than the police services and the intelligence and security services referred to in this Act, that are required, in accordance with the Act of 10 July 2006 on threat assessment, to pass on information to the Coordination Unit for Threat Assessment;
5° "Threat Assessment Act": the Act of 10 July 2006 on threat assessment;
6° "Ministerial Committee": the Ministerial Committee referred to in Article 3, 1° of the Act of 30 November 1998 governing the intelligence and security services.
Shall be equated to police services for the purposes of this Act, the people who are individually authorised to detect and establish criminal offences.

CHAPTER II – REVIEW OF THE POLICE SERVICES

This chapter that concerns review of the police services by the Standing Committee P is not reproduced.

CHAPTER III – REVIEW OF THE INTELLIGENCE SERVICES

SECTION 1 – THE STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE

Subsection 1 – Composition

Art. 28
The Standing Intelligence Agencies Review Committee, hereinafter referred to as the "Standing Committee I", shall consist of three full members, including a

Chairman. Two substitutes shall be appointed for each of them. They shall all be appointed by the Chamber of Representatives, who may dismiss them if they perform one of the functions or activities or hold one of the positions or mandates referred to in paragraph 4, or for serious reasons.

The Standing Committee I shall be assisted by a registrar. In his absence, the Standing Committee I shall provide for his replacement in accordance with the terms defined in the rules of procedure referred to Article 60.

At the time of their appointment, the members and their substitutes shall satisfy the following conditions:
1° Be Belgian;
2° Enjoy civil and political rights;
3° Have attained the age of 35 years;
4° Reside in Belgium;
5° Hold a Master's degree in Law and demonstrate at least seven years' relevant experience in the field of criminal law or criminology, public law, or management techniques, acquired in positions related to the operation, activities and organisation of the police services or of the intelligence and security services, as well as having held positions requiring a high level of responsibility;
6° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

The members and their substitutes may not hold a public elected office. They may not perform a public or private function or activity that could jeopardise the independence or dignity of the office. They may not be members of the Standing Police Services Review Committee, nor of a police service, an intelligence service, the Coordination Unit for Threat Assessment, or another support service.

The Chairman shall be a magistrate.

The decisions assigned to the Standing Committee I by this Act or other acts shall be taken in plenary session.

Art. 29
The registrar shall be appointed by the Chamber of Representatives, who may dismiss him or terminate his appointment in the cases referred to in Article 28, paragraph 4. At the time of his appointment, the registrar shall satisfy the following conditions:
1° Be Belgian.
2° Enjoy civil and political rights;
3° Have knowledge of the French and Dutch languages;
4° Have attained the age of 30 years;
5° Reside in Belgium;
6° Hold a Master's degree in Law;
7° Have at least two years' relevant experience;

8° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Before taking up his duties, the registrar shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Chamber of Representatives.

Art. 30

The members of the Standing Committee I and their substitutes shall be appointed for a renewable term of six years starting from the time they take their oath. At the end of this term, the members shall remain in office till their successors have taken their oath.

The substitutes shall be appointed for a renewable term of six years starting from the time the member whom they are replacing took his oath.

A member whose mandate ends before the expiry of the term of six years shall be replaced for the remaining period of the mandate by his first substitute or if the latter relinquishes this position, by his second substitute. If a position of substitute member should become vacant, the Chamber of Representatives shall appoint a new substitute member forthwith.

For the appointment of a substitute member, the conditions laid down in Article 28, paragraph 4, shall be verified by the Chamber of Representatives upon taking up his duties.

Before taking up their duties, the members of the Standing Committee I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Chamber of Representatives.

Subsection 2 – Definitions

Art. 31

§1. For the purposes of this chapter, "the competent ministers" shall mean:

1° The minister responsible for National Defence, with regard to the General Intelligence and Security Service;

2° The minister responsible for Justice, with regard to State Security;

3° The minister responsible for a service referred to in Article 3, 2°, in fine;

4° The minister responsible for the Interior, with regard to the assignments of State Security relating to the maintenance of law and order and the protection of people, as well as the organisation and administration of State Security when that organisation and administration have a direct influence on the execution of assignments relating to the maintenance of law and order and the protection of people;

5° The National Security Council, with regard to the Coordination Unit for Threat Assessment or the other support services.

In this chapter, "the competent authority" shall mean the director of the Coordination Unit for Threat Assessment.

Subsection 3 – Assignments

Art. 32
If the investigation concerns an intelligence service, the Standing Committee I shall act either on its own initiative, or at the request of the Chamber of Representatives, the competent minister or the competent authority.

When the Standing Committee I acts on its own initiative, it shall forthwith inform the Chamber of Representatives thereof.

Art. 33
Within the framework of the objectives laid down in Article 1, the Standing Committee I shall investigate the activities and methods of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services, their internal rules and directives, as well as all documents regulating the conduct of the members of these services.

The intelligence services, the Coordination Unit for Threat Assessment, and the other support services shall, on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services. The Standing Committee I and the Investigation Service for the intelligence services shall have the right to be provided with all texts that they consider necessary for the performance of their assignment. The Standing Committee I may, based on a reasoned request of its Chairman, request the administrative authorities to provide it with the regulations, guidelines and documents issued by these authorities which the Committee considers essential for the performance of its assignment. The concerned administrative authority has the right to assess whether it is relevant to communicate the requested regulations, guidelines and documents to the Standing Committee I.

The Standing Committee I shall provide the competent minister or the competent authority, as well as the Chamber of Representatives with a report on each investigation assignment. This report shall be confidential until its communication to the Chamber of Representatives in accordance with Article 35.

This report shall include the conclusions relating to the texts, activities or methods that could jeopardise the objectives laid down in Article 1.

The competent minister or the competent authority may, with regard to the investigation reports, hold an exchange of views with the Standing Committee I. The Standing Committee I may itself propose that such an exchange of views be held.

The competent minister or the competent authority shall inform the Standing Committee I within a reasonable period of time of his/its response to its conclusions.

The Standing Committee I may only advise on a Bill, Royal Decree, Circular Letter, or any documents expressing the political orientations of the competent ministers, at the request of the Chamber of Representatives, or the competent minister.

When the Standing Committee I acts at the request of the competent minister, the report shall only be submitted to the Chamber of Representatives at the end of the term laid down in accordance with Article 35, §1, 3°. The Chairman of the Monitoring Committee concerned referred to in Article 66*bis* shall be informed of the request of the minister to the Standing Committee I and of the content of the report before the end of the term laid down in Article 35, §1, 3°.

Art. 34

Within the framework of the objectives laid down in Article 1, the Standing Committee I deals with the complaints and denunciations it receives with regard to the operation, the intervention, the action or the failure to act of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services and their personnel.

Without prejudice to the provisions of Article 46, the Standing Committee I may decide not to follow up a complaint or a denunciation that is clearly unfounded. It may delegate this responsibility to the Head of the Investigation Service for the intelligence services.

The decision of the Standing Committee I not to follow up a complaint or denunciation and to close the investigation shall be justified and communicated to the party who made the complaint or denunciation.

When the investigation is closed, the results shall be communicated in general terms.

The Standing Committee I shall inform the managing officer of the intelligence service, the director of the Coordination Unit for Threat Assessment, or the managing officer of the other support service, depending on the case, of the conclusions of the investigation.

Art. 35

§1. The Standing Committee I shall report to the Chamber of Representatives and the Senate in the following cases:

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the Chamber of Representatives and the Senate, and to the competent ministers by 1 June at the latest. In this report, the Standing Committee I shall pay special attention to the specific and exceptional methods for gathering information, as referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, as also to the application of

Chapter IV/2 of the same Act and to the implementation of the Act of 10 July 2006 on threat assessment.
2° When the Chamber of Representatives has entrusted it with an investigation.
3° When at the end of a period that it believes to be reasonable, it notes that no action has been taken concerning its conclusions, or that the measures taken are inappropriate or inadequate. This period may not be less than sixty days.

§2. The Standing Committee I shall present a report annually to the Chamber of Representatives regarding the application of Article 16/2 and Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services. A copy of this annual report shall also be provided to the Ministers of Justice and Defence, and to State Security and the General Intelligence and Security Service, who may draw the attention of the Standing Committee I to their remarks.

The report shall contain the number of clearances granted, the duration for which the exceptional methods for gathering information are applicable, the number of persons involved and, if necessary, the results obtained. The report shall also mention the activities of the Standing Committee I.

The elements appearing in the report should not affect the proper functioning of the intelligence and security services or jeopardise the cooperation between Belgian and foreign intelligence and security services.

Art. 36
In order to prepare its conclusions of a general nature, the Chamber of Representatives may request the Standing Committee I to provide each and every investigation dossier, according to the terms and conditions that they determine and which in particular aim to safeguard the confidential nature of these dossiers and to protect the privacy of individuals. If the investigation was initiated at the request of a competent minister, his consent shall be required before handover of the investigation dossier, unless the term laid down in Article 35, §1, 3° has expired.

Art. 37
After acquiring the advisory opinion of the competent ministers or the competent authority, the Standing Committee I shall decide, within a period of one month from the request for advice, to make public all or part of its reports and conclusions, according to the terms and conditions it stipulates.

The reports and conclusions made public shall include the advisory opinion of the competent ministers and the competent authorities.

Art. 38
The Prosecutor-General and the Auditor-General shall ex-officio send to the Chairman of the Standing Committee I a copy of the judgments and judicial

decisions relating to the crimes or offences committed by the members of the intelligence services and the Coordination Unit for Threat Assessment.

The public prosecutor, the labour prosecutor, the federal prosecutor or the prosecutor-general of the Court of Appeal, depending on the case, shall inform the Chairman of the Standing Committee I whenever a criminal or judicial investigation into a crime or offence is initiated against a member of an intelligence service or the Coordination Unit for Threat Assessment.

At the request of the Chairman of the Standing Committee I, the prosecutor-general or the auditor-general may provide a copy of the deeds, documents or information relating to criminal proceedings against members of the intelligence services and the Coordination Unit for Threat Assessment for crimes or offences committed in the execution of their duties.

However, if the deed, document or information concerns an ongoing judicial investigation, it may only be communicated with the consent of the examining magistrate.

The copies shall be delivered without charge.

Art. 39.
The Standing Committee I shall exercise its authority over the Investigation Service for the intelligence services, assign investigations to it, and receive reports on all investigations that are carried out.

However, when they perform a judicial police assignment, the Head and the members of the Investigation Service for the intelligence services shall be subject to review by the prosecutor-general of the Court of Appeal or the federal prosecutor.

SECTION 2 – THE INVESTIGATION SERVICE FOR THE INTELLIGENCE SERVICES

Art. 40
By order of the Standing Committee I or, except with regard to the Coordination Unit for Threat Assessment and the other support services, on its own initiative, in which case it shall immediately inform the Chairman of the Standing Committee I, the Investigation Service for the intelligence services, hereinafter referred to as the "Investigation Service I", shall supervise the operations of the intelligence services, the Coordination Unit for Threat Assessment and the other support services, through investigations, within the limits of Article 1.

It shall examine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another support service. Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them,

as well as by the methods or actions, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

On its own initiative or at the request of the competent public prosecutor, military public prosecutor or examining magistrate, it shall, together with the other officers and agents of the judicial police, and even with a right of priority over them, investigate the crimes and offences which the members of the intelligence services and the Coordination Unit for Threat Assessment are charged with. With regard to the members of the other support services, this provision only applies with respect to the obligation laid down by Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

If the person filing a denunciation so wishes, his anonymity shall be guaranteed. In this event, his identity may only be disclosed within the Service and to the Standing Committee I.

Art. 41

A person may not be appointed Head of the Investigation Service I if he has not been a magistrate or a member of an intelligence or police service for a period of five years, or if he cannot demonstrate at least five years' relevant experience as a public servant in positions relating to the activities of the intelligence or police services. At the time of his appointment he must have attained the age of 35 years. The Head of the Investigation Service I shall be appointed by the Standing Committee I for a renewable term of five years.

Before taking up his duties, the Head of the Investigation Service I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the Chairman of the Standing Committee I.

He must have knowledge of the French and Dutch languages.

He shall retain his right to advancement and salary increase.

He may be dismissed by the Standing Committee I.

Art. 42

Without prejudice to Article 39, second paragraph, the Head of the Investigation Service I shall manage it and set out the tasks, under the collegial authority, direction and supervision of the Standing Committee I.

He shall be responsible for relations with the Standing Committee I, from which he shall receive the assignments and to which he shall send the reports.

He shall be responsible for relations with the judicial authorities, from which he shall receive the requests and to which he shall send the reports referred to in Article 46.

Art. 43

Except for the cases laid down by Articles 40, paragraph 3, and 46, the Head of the Investigation Service I shall inform the competent minister or the competent authority that an investigation is initiated.

He shall send a report to the Standing Committee I at the end of each investigation assignment.

However, in the cases referred to in Articles 40, paragraph 3, and 46, the report shall be limited to the information necessary for the Standing Committee I to perform its assignments.

Art. 44

The members of the Investigation Service I shall be appointed and dismissed by the Standing Committee I on the recommendation of the Head of the Investigation Service I.

At least half of the members, and this for a renewable term of five years, shall be seconded from an intelligence or police service or an administration in which they have acquired at least five years' experience in positions relating to the activities of the intelligence or police services.

The members of the Investigation Service I shall take the same oath as the Head of the Service.

In the service or administration that they have been seconded from, they shall retain their right to advancement and salary increase.

Art. 45

The Head and the members of the Investigation Service I shall have the capacity of judicial police officer, assistant public prosecutor and assistant military public prosecutor.

In order to be appointed, they must hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Art. 46

When a member of the Investigation Service I has knowledge of a crime or offence, he shall produce a formal report that is forthwith sent by the Head of the Investigation Service I to the public prosecutor, to the military public prosecutor, or the examining magistrate, depending on the case.

The person who lodged the complaint or filed the denunciation, or the authority who called upon the Standing Committee I, shall be informed thereof by the Head of the Investigation Service I.

Art. 47

When a member of the Investigation Service I observes facts during an investigation that could constitute a disciplinary offence, the Head of the Investigation Service I shall forthwith inform the competent disciplinary authority thereof.

SECTION 3 – INVESTIGATION PROCEDURES

Art. 48

§1. Without prejudice to the legal provisions relating to the immunity and privilege, the Standing Committee I and the Investigation Service I may summon for hearing any person they believe useful to hear.

The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services which are being heard may testify about facts covered by professional secrecy.

§2. The Chairman of the Standing Committee I may have members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services summoned through the medium of a bailiff. The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services are bound to testify after having taken the oath prescribed by Article 934, paragraph 2 of the Judicial Code.

The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services are bound to disclose to the Standing Committee I the secrets that they know of. If these secrets relate to an ongoing criminal or judicial inquiry, the Standing Committee I shall consult the competent magistrate in advance regarding this.

If the member or former members of the intelligence service, the Coordination Unit for Threat Assessment, or the other support services is of the opinion that he must not disclose the secret he has knowledge of because its disclosure would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule, or, if it concerns a member or former member of the Coordination Unit for Threat Assessment or another support service, the Chairmen of the two Standing Committees, who shall rule jointly.

§3. The Standing Committee I and the Investigation Service I may request the collaboration of interpreters and experts. They shall take the oath in the way used in the Assize Court. The remuneration due to them shall be paid in keeping with the rates for fees in civil cases.

§4. Article 9 of the Act of 3 May 1880 on parliamentary investigations shall apply to the members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services who are heard or summoned by the Standing Committee I as witnesses, and to the experts and interpreters who are called upon.

The formal reports establishing the offences committed before the Standing Committee I shall be drawn up by the Chairman and sent to the prosecutor-general of the Court of Appeal in the district where they were committed.

The members or former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services who refuse to testify before the Standing Committee I, and the experts and interpreters who refuse to collaborate, shall be liable to imprisonment of between one month and one year.

Art. 49
The members of the Investigation Service I may request the assistance of the public power in the performance of their assignments.

Art. 50
Any member of a police service who observes a crime or offence committed by a member of an intelligence service shall draw up an information report and send it to the Head of the Investigation Service I within a period of fifteen days.

Art. 51
The members of the Investigation Service I may make all observations in any location.

They may at all times, in the presence of their Head of Department, or his substitute, and of the chief of police, director or senior civil servant concerned, or his replacement, enter the premises where members of an intelligence service, the Coordination Unit for Threat Assessment or other support service perform their duties, in order to make substantive observations. In these locations, they may confiscate any objects and documents useful to their investigation, except for those relating to an ongoing criminal or judicial investigation. If the chief of police or his substitute is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 November 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule. If the director or the senior civil servant or his replacement is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 threat ass 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairmen of the two Standing Committees, who shall rule jointly. The confiscated objects and documents shall be recorded in a special register kept for this purpose.

CHAPTER IV – JOINT MEETINGS OF THE STANDING POLICE SERVICES AND INTELLIGENCE AGENCIES REVIEW COMMITTEES

Art. 52
The Standing Committees shall exchange information on their activities and send each other the reports and conclusions referred to in Articles 9, 11, 33 and 35.

At least twice a year, they shall hold joint meetings, during which additional information may be exchanged.

Art. 53
During their joint meetings, the Standing Committees shall jointly perform their assignments (laid down in Articles 9, 10, 11, 33, 34 and 35):
1° With regard to the public services that perform both police and intelligence assignments;
2° With regard to the division of the assignments and the coordination of the operation between the police services on the one hand, and the intelligence services on the other;
3° With regard to any question put to them, either by a joint request from the ministers responsible for the Interior, Justice and National Defence, or at the request of the Chamber of Representatives;
4° With regard to any question that each Standing Committee believes does not fall within its exclusive competence;
5° With regard to any question considered by a Standing Committee to be sufficiently important to warrant a joint meeting;
6° With regard to the Coordination Unit for Threat Assessment or another support service.

A report shall be produced jointly by the Standing Committees at each joint meeting. This report may include advisory opinions and recommendations. It shall be sent as stipulated in Articles 9, 11, 33 and 35.

Art. 54
These joint meetings shall be chaired alternately by the Chairmen of the Standing Committees.

The functions of the secretariat of the joint meetings shall be performed by the longest serving registrar or, in the event of equal length of service, by the youngest registrar.

Art. 55
During the joint meetings, the Standing Committees may decide to assign investigation assignments to the two Investigation Services or to either one of them. They shall receive the reports on all the investigations that are carried out.

CHAPTER V – COMMON PROVISIONS

Art. 56
Each Standing Committee shall examine the complaints that are lodged with it by its former members or by former members of the Investigation Services who believe they have been subject to prejudicial measures because of the functions they have carried out in the Standing Committees or in the Investigation Services.

Art. 57
The funds required for the operation of the Standing Committees and the Investigation Services established by this Act shall be imputed to the appropriations budget.

The Chairmen, the members and the registrars of the Standing Committees, as well as the Director-General of the Investigation Service P and the Head of the Investigation Service I shall enjoy exemption from postal charges for official business.

Art. 58
Each Standing Committee shall appoint and dismiss the members of its administrative staff, on its own initiative or at the proposal of the registrar.

Under the collegial authority and supervision of the Standing Committee in question, the registrar shall be responsible for leading and managing the members of the administrative staff and shall distribute the tasks among them.

The Director-General of the Investigation Service P and the Head of the Investigation Service I shall have authority over the members of the administrative staff, where the number of members and their job requirements shall be defined by the Standing Committee in question, which assigns these members to them.

The registrar shall have authority over the members of the Investigation Service P or I, depending on the situation, where the number of members and the job requirements shall be defined by the Standing Committee in question, which assigns these members to him.

The staff members referred to in the third and fourth paragraphs shall retain the rights and obligations specific to the statute applicable to them.

Art. 59
The travel and subsistence expenses of the Chairman, the members and the registrar of each Standing Committee, the Director-General of the Investigation Service P, the Head of the Investigation Service I and the members of these services shall be determined according to the provisions applicable to the public services.

Art. 60
Each Standing Committee shall adopt its rules of procedure. The rules of procedure for the joint meetings shall be adopted jointly by the two Standing Committees.

The rules of procedure of both Standing Committees shall be approved by the Chamber of Representatives.

In accordance with paragraph 2, the Chamber of Representatives may amend the rules of procedure after acquiring the advisory opinion of the Standing Committee concerned. The advisory opinion shall be deemed favourable if it has not been given within sixty days of the request.

Art. 61
§1. The members of the Standing Committees shall enjoy the same status as the councillors of the Court of Audit. The rules governing the financial statute of the councillors of the Court of Audit, contained in the Act of 21 March 1964 on the remuneration of the members of the Court of Audit, as amended by the Acts of 14 March 1975 and 5 August 1992, shall apply to the members of the Standing Committees.

The members of the Standing Committees shall enjoy the pension scheme applicable to the civil servants of the General Administration. The following special conditions shall also apply.

The pension may be granted as soon as the person concerned has attained the age of fifty-five years. It shall be calculated on the basis of the average remuneration of the last five years, in proportion to one twentieth per year of service as a member of the Standing Committee.

A member who is no longer able to perform his duties due to illness or infirmity, but who has not attained the age of fifty-five years, may retire irrespective of his age. The pension shall be calculated according to the method laid down in the preceding paragraph.

The services that do not fall under the regulations referred to in paragraphs two to four and that qualify for the calculation of a state pension, shall be taken into account in application of the laws governing the calculation of the pensions for these services.

§2. Unless he has been dismissed, the member of a Standing Committee shall, when his duties are terminated or if his term of office is not renewed, receive a fixed severance grant equivalent to the gross monthly salary of the last eighteen months.

If this severance grant is granted before expiry of the first period of five years, it shall be reduced accordingly.

The following are excluded from this allowance:
1° The members to which Article 65 applies.

2° The members who were members of a police service or an intelligence and security service before their appointment to the Standing Committee and who rejoin this service.

§3. The registrars of the Standing Committees shall enjoy the same statute and pension scheme as the registrars of the Court of Audit.

Article 365, §2, a), of the Judicial Code shall apply to the registrars of the Standing Committees.

Art. 61*bis*

The Chairman of each Standing Committee shall, in accordance with the principle of collective responsibility, preside the meetings of that Committee and assume the day-to-day management of its activities. He shall ensure the application of the rules of procedure, the proper functioning of the Committee, as well as the proper performance of its assignments. He shall also ensure that the performance of the judicial police assignments does not impede the performance of the investigations. To this end, he shall hold the necessary consultations with the competent judicial authorities.

For the implementation of the authorities entrusted to him, the Chairman of each Standing Committee shall be assisted by the registrar and, respectively, by either the Director-General of the Investigation Service P or the Head of the Investigation Service I.

Art. 62

Without prejudice to Article 58, the registrar shall act under the collegial authority and the supervision of the Standing Committee in question, the registrar of each Committee shall among others manage the following:
the administrative staff;
the infrastructure and equipment of the Committee;
the secretariat of the Committee meetings and the minutes of the meetings;
the sending of documents;
the preservation and protection of the secrecy of the documentation and archives.

He shall prepare the budget of the Committee and keep the accounts.

Art. 63

The members of the Standing Committees are prohibited from attending the deliberations on affairs in which they have a direct or personal interest, or in which relatives by blood or marriage to the fourth degree inclusive, have a direct or personal interest.

Art. 64

The members of the Standing Committees, the registrars, the members of the Investigation Services, and the administrative staff shall be obliged to preserve the secrecy of the information that comes to their attention in the performance of

their duties. The obligation of confidentiality shall also apply after they leave office.

Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment of between eight days to one year, and a fine between one hundred francs and four thousand francs, or only one of these penalties, if they divulge these secrets in circumstances other than those stipulated by law or by the rules of procedure.

Art. 65

§1. Articles 1, 6, 1 and 12 of the Act of 18 September 1986 instituting political leave for the members of staff of the public service shall apply, where appropriate and with the necessary adaptations, to members of the Standing Committees.

§2. Members of the judiciary may be appointed as members of the Standing Police Services Review Committee and as members of the Standing Intelligence Agencies Review Committee, and as Director-General of the Investigation Service P or Head of the Investigation Service I.

Article 323*bis*, paragraph 3, of the Judicial Code shall apply if a magistrate from the public prosecutor's office is a chief of police.

Art. 66

Excluding its Chairman, each Standing Committee shall have as many French-speaking members as Dutch-speaking members.

The Chairman of one of the Standing Committees shall be French-speaking, the Chairman of the other Dutch-speaking.

Art. 66*bis*

§1. The Chamber of Representatives shall create a permanent committee responsible for monitoring the Standing Committee P and the Standing Committee I.

The Chamber of Representatives shall stipulate in its regulation, the rules relating to the composition and functioning of the monitoring committee.

§2. The monitoring committee shall supervise the operation of the Standing Committees, and ensure observance of the provisions of this Act and the rules of procedure.

The monitoring committee shall also perform the assignments assigned to the Chamber of Representatives by Articles 8, 9, 11, 1°bis, 2° and 3°, 12, 32, 33, 35, §1, 2° and 3°, 36 and 60.

§3. The monitoring committee shall meet at least once per quarter with the President or the members of each Standing Committee. The monitoring committee can also meet at the request of the majority of its members, at the request of the Chairman of one Standing Committee, or at the request of the majority of the members of a Standing Committee.

Every denunciation by a member of a Standing Committee relating to the inadequate functioning of that Standing Committee, the non-observance of this Act, or the rules of procedure, may be brought before the monitoring committee.

The monitoring committee may issue recommendations to each Standing Committee, or to each of its members, relating to the functioning of the Standing Committee, the observance of this Act, or the rules of procedure.

§4. The members of the monitoring committee shall take the necessary measures to safeguard the confidential nature of the facts, acts or intelligence that they have knowledge of by virtue of their position, and shall be subject to an obligation of confidentiality. They shall be obliged to preserve the secrecy of any information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Any violation of this obligation of confidentiality shall be penalised in accordance with the rules of the Chamber of Representatives.

APPENDIX

30 NOVEMBER 1998 ACT GOVERNING THE INTELLIGENCE AND SECURITY SERVICES

(extract)
[Amendments brought until 08/12/2016]

TITLE I
GENERAL PROVISIONS

(…)

[TITLE IV/2
A POSTERIORI CONTROL OF THE SPECIFIC AND EXCEPTIONAL METHODS FOR THE GATHERING OF INTELLIGENCE BY THE INTELLIGENCE AND SECURITY SERVICES

Article 43/2
Without prejudice to the competences defined in Article 1 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment and in Article 44*ter* of the Act of 30 November 1998 on the intelligence and security services, the Standing Committee I is also called on to conduct a posteriori control of the specific and exceptional intelligence gathering methods used by the intelligence and security services as referred to in Article 18/2.

The Standing Committee I shall rule on the legality of decisions made regarding these methods, as well as on compliance with the principles of proportionality and subsidiarity, set out in Articles 18/3, §1, first paragraph, and 18/9, §§2 and 3.

Article 43/3
The lists referred to in Article 18/3, §3, shall be reported immediately by the competent authority to the Standing Committee I, in accordance with the procedures to be determined by the King.

All decisions, opinions and authorisations concerning the specific and exceptional intelligence gathering methods shall be reported immediately by the competent authority to the Standing Committee I, in accordance with further rules to be determined by the King.

Article 43/4
The Standing Committee I shall operate:

- either on its own initiative;
- or at the request of the Privacy Commission, in accordance with further rules to be defined by the King, in a decree deliberated in the Council of Ministers, following the opinions of that Commission and of the Standing Committee I;
- or as the result of a complaint, which must be submitted in writing on pain of invalidity, stating the grievance, from anyone who can show a personal and legitimate interest, unless the complaint is clearly unfounded;
- on any occasions where the Commission has suspended use of a specific or exceptional method on the grounds of illegality or not permitted the use of intelligence on the grounds of the unlawful use of a specific or exceptional method;
- whenever the competent minister has taken a decision on the basis of Article 18/10, §3.

The Standing Committee I shall rule within one month following the day on which the case was referred to it in accordance with the first paragraph.

A decision by the Standing Committee I not to follow up a complaint shall be justified and the complainant shall be notified.

Unless the Standing Committee I rules otherwise, its control shall not have suspensive effect.

Article 43/5
§1. Control of the exceptional intelligence gathering methods is conducted inter alia on the basis of the documents provided by the Commission in accordance with Article 18/10, §7, and of the special register referred to in Article 18/17, §6, which is kept continuously available to the Standing Committee I, and on the basis of any other relevant document provided by the Commission or for which the Standing Committee I is required to be consulted.

Control of the specific intelligence gathering methods is conducted inter alia on the basis of the lists referred to in Article 18/3, §3, and of any other relevant

document provided by the Commission or for which the Standing Committee I is required to be consulted.

The Standing Committee I shall have access to the complete dossier compiled by the intelligence and security service involved, as well as to that of the Commission and may require the intelligence and security service involved and the Commission to provide any additional information which it deems useful for the control to which it is authorised. The intelligence and security service involved and the Commission are required to follow up this request immediately.

§2. The Standing Committee I may entrust investigation assignments to the Investigation Service of the Standing Committee I. In this context this service may employ all the powers granted to it under the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

§3. The complainant and his lawyer may consult the dossier at the secretariat of the Standing Committee I, for a period of five working days, on the days and times notified by the Committee. This dossier shall contain all information and intelligence relevant to this case, except for those which would breach the protection of sources, the protection of the privacy of third parties, the classification rules set out in the Act of 11 December 1998 on classification and security clearances, certificates and advice, or which would prevent the execution of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11.

The intelligence and security service involved shall be given the opportunity to voice its opinion on the information included in the dossier provided for consultation.

The dossier made available to the complainant and his lawyer shall in any event include the following:
1° the legal basis justifying use of the specific or exceptional intelligence gathering method;
2° the nature of the threat and its degree of gravity which justified use of the specific or exceptional intelligence gathering method;
3° the type of personal data collected in the course of the use of the specific or exceptional method to the extent that this personal data only relates to the complainant.

§4. The Standing Committee I can hear the members of the Commission, as well as the head of service of the service involved and the members of the intelligence and security services who used the specific or exceptional intelligence gathering methods. They shall be heard in the absence of the complainant or his lawyer.

The members of the intelligence services are required to disclose the secrets that they know to the Standing Committee I. If these secrets relate to an ongoing criminal investigation or judicial inquiry, the Standing Committee I shall discuss this beforehand with the competent magistrate.

If the member of the intelligence and security service considers it necessary not to reveal a secret which he holds because its disclosure would prejudice the protection of sources, the protection of the privacy of third parties or the execution of the assignments of the intelligence and security services as referred to in Articles 7, 8 and 11, the matter shall be submitted to the chairman of the Standing Committee I who shall rule after hearing the head of service.

The complainant and his lawyer may be heard by the Standing Committee I at their request.

Article 43/6

§1. When the Standing Committee I establishes that decisions concerning specific or exceptional intelligence gathering methods have been unlawful, it shall order the use of the method to cease if it is still in progress or if it was suspended by the Commission, and shall order that the intelligence acquired by this method cannot be used and is to be destroyed, in accordance with further rules to be determined by the King on the basis of opinions from the Privacy Commission and the Standing Committee I.

The reasoned decision shall be sent immediately to the head of service, to the minister involved, to the Commission and, where relevant, to the Privacy Commission.

If the Standing Committee I considers that a specific or exceptional intelligence gathering method has been used in compliance with the provisions of this Act, while the Commission had forbidden the use of the intelligence gathered with this method, or had suspended the use of this method, the Standing Committee I shall lift this prohibition and this suspension by means of a reasoned decision and shall immediately inform the head of service, the competent minister and the Commission.

§2. In the event of a complaint the complainant shall be informed of the decision under the following conditions: any information which could have an adverse impact on the protection of the inviolability of the national territory, the military defence plans, the execution of the assignments of the armed forces, the safety of Belgian nationals abroad, the internal security of the State, including aspects relating to nuclear energy, the maintenance of democratic and constitutional order, the external security of the State and international relations, the operations of the decision-making bodies of the State, the protection of sources or the protection of the privacy of third parties, shall, with reference to this legal provision, be omitted from the transcript of the decision revealed to the complainant.

The same procedure shall be followed if the decision includes information which could compromise the secrecy of the criminal investigation or inquiry, if information relates to an ongoing criminal investigation or judicial inquiry.

Article 43/7
§1. Where the Standing Committee I operates in the context of this Title, the functions of the secretariat shall be performed by the secretary of the Standing Committee I or by a level 1 staff member appointed by him.
§2. The members of the Standing Committee I, the secretaries, the members of the Investigation Service, and the administrative staff are required to maintain secrecy concerning the facts, actions or information that come to their attention as a result of their cooperation in the application of this Act. They may however use the data and information that they acquire in this context for the execution of their assignment, as set out in Article 1 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment of between eight days to one year, and a fine of between one hundred euro and four thousand euro, or only one of these penalties, if they divulge these secrets in circumstances other than those stipulated in this Act.

Article 43/8
No appeal is possible against the decisions of the Standing Committee I.]

(…)