ACTIVITY REPORT 2012
ACTIVITY REPORT 2013

ACTIVITY REPORT 2012
ACTIVITY REPORT 2013

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 2012. Activity Report 2013. 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 978-1-78068-359-1
D/2015/7849/144
NUR 823

CONTENTS

LIST OF ABBREVIATIONS

ACOS-IS	Assistant Chief of Staff Intelligence and Security
ACOS-Ops & Trg	Assistant Chief of Staff of Operations and Training
ANS/NVO	National Security Authority *(Nationale Veiligheids-overheid – Autorité nationale de sécurité)*
BELINT	Belgian Intelligence
BENIC	Belgian National Intelligence Cell
BIC	Battle Group Intelligence Cell
CANPAN/CANVEK	Advisory Committee for the Non-Proliferation of Nuclear Weapons *(Commissie van advies voor de niet-verspreiding van kernwapens – Commission d'avis pour la non-prolifération des armes nucléaires)*
CFREU	Charter of Fundamental Rights of the European Union
CGRS	Office of the Commissioner General for Refugees and Stateless Persons *(Commissariaat-generaal voor de vluchtelingen en de staatlozen – Commissariat général aux réfugiés et aux apatrides)*
CHOD	Chief of Defence
CIA	Central Intelligence Agency
Classification Act	Act of 11 December 1998 on classification and security clearances, certificates and advice *(Wet betreffende de classificatie en de veiligheidsmachtigingen, veiligheidsattesten en veiligheidsadviezen – Loi relative à la classification et aux habilitations, attestations et avis de sécurité)*
COMINT	Communications intelligence
CPOE	Comprehensive Preparation of the Operational Environment
CUTA	Coordination Unit for Threat Assessment (*Coördinatieorgaan voor de dreigingsanalyse – Organe de coordination pour l'analyse de la menace*)
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
FPS	Federal public service
FTE	Full-time equivalent
GCCR	Governmental Coordination and Crisis Centre
GCHQ	Government Communications Headquarters
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
ICCPR	International Covenant on Civil and Political Rights
ICT	Information and Communications 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)*
ISAF	International Security Assistance Force
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
KAIA	Kabul International Airport
MAT	Military Assistance Team
MCI&S	Ministerial Committee for Intelligence and Security (*Ministerieel Comité voor inlichting en veiligheid – Comité ministériel du renseignement et de la sécurité*)
NATO	North Atlantic Treaty Organisation
NGO	Non-Governmental Organization
NSA	National Security Agency
OEF	Operation Enduring Freedom
OSCE	Organization for Security and Co-operation in Europe
OSINT	Open source intelligence
Parl. doc	Parliamentary document
Police Function Act	Act of 5 August 1992 governing the missions of the police *services (Wet op het Politieambt – Loi sur la Fonction de police)*
PRT	Provincial Reconstruction Team
RD CUTA	Royal Decree of 28 November 2006 (see the Threat Assessment Act)

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*)
RFI	Request for Information
SEP	Scientific and economic potential
SIGINT	Signal 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
SOP	Standing Operating Procedure
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'Etat*)
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)*
UN	United Nations
US	United States

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 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 documents of the intelligence services are classified in accordance with the

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.).

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 were appointed or renewed by the Senate in 2012 and 2013.[2] 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 2012 and 2013 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 fourth to be published in English by the Standing Committee I, after the *Activity Report 2006-2007,* the *Activity Report 2008-2009* and the *Activity Report 2010-2011* (see www.comiteri.be).

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

1 September 2015

2 Pursuant to the sixth state reform, this competence has recently been transferred to the Chamber of Representatives. 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 2012

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2012

PREFACE – ACTIVITY REPORT 2012

The Standing Committee I has set itself a twofold mission this year.

Firstly, investigations, which remain the *core business*, should be professionalised as much as possible. This can be realised through a relentless quest to improve the quality of investigations and by developing a clear methodology that must allow the work to focus on elements that are essential and relevant to the parliamentary review in which the Committee participates. This means that investigative work should be completed within a reasonable period. Without becoming dogmatic about it, a period of six to twelve months – depending on the investigation and its scope – must be an achievable objective.

Secondly, the Standing Committee I must continue its current projects: active presence at international forums, raising the profile of the Committee in Belgium and of initiatives such as the *Belgian Intelligence Studies Centre* – which aims to bring the intelligence services closer to the academic world – and the 'Analysis Working Group' that is preparing a training programme for the analysts of the two intelligence services.

The challenges are enormous because the Standing Committee I cannot afford to neglect its core tasks, namely carrying out its legal review mission for Parliament and the jurisdictional monitoring of special intelligence methods, for the sake of a representative or reflective role. Nevertheless, in addition to this legal review of the services, the Committee must make its mark both in Belgium and abroad and promote the 'Belgian model' of democratic and parliamentary oversight of the intelligence services.

In terms of its legal tasks, the '2012 harvest' was more than satisfactory. After all, the Standing Committee I initiated eight interesting investigations and completed six, including a joint investigation with the Standing Committee P on the Coordination Unit for Threat Analysis. The completed investigations include the report on how the Belgian intelligence services monitor any activities of foreign services in our territory in relation to their diaspora and the investigation into the manner in which and the circumstances under which State Security investigates and processes requests for information as part of the procedures for obtaining Belgian nationality.

Lastly, we wish to end for once on a more personal note. It is with a sense of pride that I can announce I have been reappointed as chairman for a new six-year mandate. It is indeed an honour to be able to lead an organisation that has resolutely carved a niche for itself in our democratic system. A further personal

source of motivation is the fact that this has given my fellow councillors and me the opportunity, driven by a constant concern to maintain high quality, to continue fulfilling the assignments that Parliament has entrusted to the Committee and to try and promote the 'Belgian model' of democratic and parliamentary oversight of the intelligence services.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2013

CHAPTER II
REVIEW INVESTIGATIONS

Six investigations were completed in 2012, including a joint investigation with the Standing Committee P. Two investigations were at the request of the Monitoring Committee of the Senate, two as the result of complaints and two at the initiative of this Committee alone or jointly with the Standing Committee P. The six final reports are explained below (II.1 to II.6). This will be followed by a summary and a brief description of the background to the ongoing investigations (II.7). The eight investigations opened in 2012 are also referred to in that section. One of these was opened at the initiative of the Monitoring Committee of the Senate, six (of which one jointly with the Standing Committee P) were opened at the Committee's own initiative and one after a complaint by a citizen. The Committee received a total of sixteen complaints or reports. After verifying a number of factual points, the Committee rejected fourteen complaints or reports because they were manifestly unfounded (Article 34 of the Review Act) or because it was not competent for the matter in question.[3] 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.

II.1. STATE SECURITY'S ROLE IN RELATION TO THE PROCEDURES FOR OBTAINING BELGIAN NATIONALITY

Following the discussion of the review report on the Belliraj case, which referred to problems concerning the opinions that State Security issues for the purpose of naturalisation applications[4], the Monitoring Committee of the Senate requested an investigation *'into the manner in which and the circumstances under which State Security investigates and handles requests for information regarding*

[3] A complaint from the end of 2012 led to the official opening of an investigation only at the start of 2013.

[4] STANDING COMMITTEE I, *Activiteitenverslag 2008* (Activity Report 2008), 33–42 and *Activiteitenverslag 2009* (Activity Report 2009), 30–40.

procedures for obtaining Belgian nationality'.[5] In the past, the Committee focused its attention more than once on certain aspects of this issue.[6]

II.1.1. THE LEGAL FRAMEWORK: THE BELGIAN NATIONALITY CODE AND VARIOUS CIRCULARS

Under the then[7] Belgian Nationality Code of 28 June 1984, Belgian nationality could be 'obtained' or 'granted' in different ways. State Security was only explicitly given a role in this regard in four cases:

- grant on the grounds of birth[8];
- obtaining through a nationality declaration;
- obtaining through choice of nationality; and
- obtaining through naturalisation.

The Code explicitly requires State Security to issue an 'opinion' only for naturalisation applications (Article 21 of the Belgian Nationality Code). In the other cases, the service must provide its 'comments' to the competent public prosecutor's office according to the directives[9] that apply at the time of the investigation. The Code does not provide for any explicit intervention here.

---

5 This investigation was opened in December 2010 and closed at the end of March 2012.

6 See, for example, STANDING COMMITTEE I, *Activiteitenverslag 1999* (Activity Report 1999), 66–81 and *Activiteitenverslag 2010* (Activity Report 2010), 33 et seq.

7 The investigation ended at the start of 2012. It thus could not take into account the important amendment that the Act of 4 December 2012 made to the Belgian Nationality Code.

8 In relation to the granting of nationality on the grounds of birth, the Committee asked whether State Security's involvement was necessary in these types of files. Given that the declaration that leads to the granting of Belgian nationality must be made before the child is twelve (at that time Article 11*bis* of the Belgian Nationality Code), State Security's role was extremely limited, if only for the reason that the service normally does not keep any files on minors. Exceptions are minors that are known for serious offences (e.g. participating in terrorist training camps) or in respect of whom another service (such as the police or the Immigration Office) have forwarded information.

9 Circular of 6 August 1984 on the Belgian Nationality Code, *Belgian Official Journal* 14 August 1984; Circular of 8 November 1991 on the amendment of the Belgian National Code, *Belgian Official Journal* 7 December 1991; Circular of 20 July 2000 to supplement the Circular of 25 April 2000 on the Act of 1 March 2000 amending a number of provisions relating to Belgian nationality, *Belgian Official Journal* 27 July 2000; Circular of 25 May 2007 on amendments to the Belgian Nationality Code that were implemented by the Act of 27 December 2006 containing various provisions, *Belgian Official Journal* 4 June 2007. Since the entry into force of the Act of 4 December 2012 amending the Belgian Nationality Code (*Belgian Official Journal* 14 December 2012), these circulars have been replaced by the Circular of 8 March 2013 on certain aspects of the Act of 4 December 2012 amending the Belgian Nationality Code in order to make obtaining Belgian nationality migration-neutral (*Belgian Official Journal* 14 March 2013).

The Committee found that State Security never actually issues an 'opinion' on the opportuneness of granting or not granting Belgian nationality, including in relation to naturalisations. The service limits itself to providing intelligence or information that it deems relevant to the body that must formulate an opinion (the public prosecutor's office) or make a decision (the Chamber of Representatives). The Committee showed understanding for this way of working. After all, the very nature of intelligence work means that clear and definitive answers – in a positive or negative sense – are not always possible. Besides, the work by definition involves many unknown, uncertain or unverifiable elements. The files on naturalisation and nationality declarations and choices also contain advice and opinions from other players, such as prosecutors' offices and the Immigration Office. It can moreover often be inferred from the length of the 'opinion' how the case should be understood. After all, State Security will only issue an extensive memorandum if there is really something relevant to mention. The Standing Committee I has also been able to ascertain that the Chamber of Representatives' Committee for Naturalisations does not question the nature of State Security's 'opinion'. There is accordingly consensus between State Security and the client. The Standing Committee I nevertheless believes that it would be good to formalise this procedure, possibly in the form of a protocol.

However, the more important question is what information must be shared. The Code only refers in this regard to '*important facts, specifically related to the person*'. This description was briefly explained in the aforementioned ministerial circulars. It was clear, for example, that this did not necessarily have to involve criminal convictions and that – conversely – a conviction did not by definition form an obstacle to the granting of Belgian nationality. All in all, these circulars provide little guidance. Very little was documented at State Security itself in this regard. An internal memorandum from 1993 did state that answers are provided (to the public prosecutor's questions) only within the limits of State Security's competence. In practice, therefore, State Security only mentions facts that relate to the interests and threats that the service must monitor under the Intelligence Services Act: extremist or terrorist activities, involvement in arms trafficking and proliferation, membership in a harmful sect, espionage or interference etc. The question that naturally remains is whether what State Security regards as *'serious'*, or at least worth reporting, is also perceived that way by the other parties concerned, and what importance is thus attached to those facts in the file. This question also made it clear that the concept of '*serious facts, specifically related to the person*' required further explanation.

Lastly, the Code states the period within which State Security must send the information in its possession to the 'client'. In the case of a nationality declaration or choice of nationality, the information must arrive at the competent magistrate within two months of the party's application; in case of naturalisation, the service has four months to inform the competent Chamber of Representatives' committee.

II.1.2. PROCESSING OF FILES WITHIN STATE SECURITY

Every process to obtain Belgian nationality starts with the foreign national's application at the registrar of births, marriages and deaths of his/her principal place of residence or at a Belgian foreign mission, or – in the case of naturalisation – at the Chamber of Representatives.

All these applications arrive (normally bundled) at State Security's Security Verification Service – either directly or via the central *Point of Contact*. The service checks whether the applicant appears in State Security's central database. If the answer is negative, the application form is stamped '*unknown to State Security*'. If the applicant's identity is in the database, the file is sent to the Analysis Service. From that moment, there are three possibilities. Either that service is of the opinion that there are no elements that give rise to negative comments.[10] In that case, the file is stamped '*not known unfavourably*'. Or the situation is clear in the sense that something negative is known about the subject. In that case, the relevant information is then incorporated into a '*contextualised memorandum*' and forwarded to the competent authority. However, in a limited number of files, the situation of the subject is unclear – for example, the available information is outdated or comes from only one source. In that case, the analyst can request an investigation by State Security's External Services. The client is told that an '*an investigation is being carried out*' pending the results. After completing this investigation and/or receiving additional data, the Analysis Service draws up its '*contextualised memorandum*', which is then forwarded to the competent authority.

All the various steps will be examined further below.

II.1.2.1. Procedure at the Security Verification Service

From 2009 to 2011, the Security Verification Service processed between 37,000 and 40,000 'nationality files' a year. Around one-quarter of these files related to naturalisations.[11]

In principle, files and documents arrive at and leave State Security via the *Point of Contact*. A fixed date and reference is allocated here to facilitate internal follow-up. However, this was not done systematically for nationality applications: some files arrived directly at the Security Verification Service and were not allocated a number and date. What is more, little or nothing was noted when the files left the Service. This made it almost impossible to properly follow-up

10 This may be the case, for example, if the subject is mentioned in a report, but personally has nothing to do with the threat.

11 However, the work of this service involves more than that. Nationality applications made up around half of the work volume from 2009 to 2011. After all, the service also receives all the applications for which a security advice or certificate must be issued or a security investigation is required.

nationalisation, nationality declaration and choice of nationality applications or to determine their lead times. The Standing Committee I was of the opinion that this situation is problematic. Proper file management requires each file to be separately registered in a central system.

The initial substantive processing at the Security Verification Service involves determining whether or not an applicant is 'known' at State Security. This is done by entering his or her name in the central database. This database has an advanced and effective search system that can take into account phonetic spelling (especially for non-Latin alphabets), alternative spellings, different versions of names or surnames or even multi-barrelled surnames.

Entering and searching all names is very labour-intensive. This involves many different aspects: the correct spelling (of foreign names) must be observed, many details are not digitally available, the composition of the files differs from municipality to municipality, etc.

The Security Verification Service had three FTEs in 2010 for processing the (thousands of) files. The Committee held that the available processing time was sufficient and the workload was feasible.

The Committee further paid attention to supervising the quality of the work delivered. It was able to establish that the head of the Service had performed spot checks. However, as this was not done systematically, the Standing Committee I found this quality control to be inadequate. It also transpired that the head of the Service processed around 5% of the files (namely those cases in which a lack of the required identification data meant there were doubts about a person's identity) himself. This was necessary because, surprisingly enough, he was the only person within the Security Verification Service that had access to the National Register.

Apart from searching for the names in the database, the naturalisation files are essentially processed 'on paper'. It goes without saying, therefore, that there is room for improvement here. Besides the fact that computerisation would facilitate better follow-up of files and enable the electronic transmission of documents[12], IT applications can take over or reduce monotonous routine tasks. An excellent computer system would moreover be able to support quality control.[13]

---

12 This aspect obviously cannot be seen in isolation from the operations of the other players (municipalities, prosecutors' offices and the Chamber of Representatives' Committee for Naturalisations).

13 In association with the ICT Service, the Security Verification Service previously experimented with a system by which a schedule of names, included in the inventory list of naturalisation files sent by the Chamber of Representatives to State Security, was entered in its entirety into the search system. However, the tests showed that the system was not yet fully reliable. The Security Verification Service guaranteed that it has eliminated the problems by the middle of 2012 and that the system was operational. However, this was not the case at the end of 2012.

Computerisation was a little further advanced in the nationality declaration files. This was possible because a number of these files were delivered electronically. Although this obviously yielded benefits, a few qualifying remarks also had to be made: the files were received at specific email addresses and thus not via the central *Point of Contact*, as a result of which these files had a 'separate' electronic existence from that point and the manner in which they were compiled was not uniform.

In view of the two-month or four-month period within which State Security must deliver its completed product to the client (see II.1.1), the Committee believes that the one-month processing deadline specified by the Security Verification Service is feasible. This leaves the Analysis Service (and, if necessary, the External Services) room to promptly process the 'known' files. However, in early 2012 this deadline had not been achieved for the naturalisation applications: the files took two months on average to process.[14] On the other hand, the specified deadline was achieved for the nationality applications and choices.

II.1.2.2. Procedure at the Analysis Service

Around 6% of all candidate Belgians are 'known' to State Security each year. Their files then also end up at the Analysis Service. The Standing Committee I established that this service – just like the Security Verification Service – failed to register and formally follow up incoming files.

The processing of the files starts at the database in which the reports of the External Services and earlier assessments can be efficiently consulted.[15] Searching for the available information in the database therefore costs the analysts little time. However, an assessment sometimes requires consultation of other open sources. The analyst may also instruct the External Services to gather more data in the field.

The number of requests for additional information via 'written orders' was rather limited. It totalled somewhat less than 400 files from 2009 to 2011. This is only 5.5% of the number of 'known' files that the Analysis Service needed to process for the same period. There are no written instructions in order to determine which files must be sent for further investigation to the External Services. Although drawing up general rules is not an obvious solution in this regard, the Standing Committee I believes that certain criteria may be set: the age of the available information, the nature of the material taken into account, State Security's general priorities, the 'seriousness' of the file, etc.

---

14 It may be assumed that the 2010 backlog arose due to the increase in the number of incoming files arising from the Belgian EU Presidency as well as staff cutbacks. The Security Verification Service cleared this backlog by mid 2012.

15 Exceptionally, (older) hard copy paper files also need to be consulted.

After the analyst had completed the investigation, around three-quarters of the files could be stamped as 'not known unfavourably', while a quarter resulted in a 'contextualised memorandum'. This memorandum must obviously be drafted with the necessary care and attention, especially if the analyst is dealing with classified data or information covered by the confidentiality of sources. Although this data must be protected, this concern should not defeat the purpose of the memorandum. Every 'contextualised memorandum' is moreover submitted to the Legal Service before it is sent.

The Committee was able to conclude that attention was also paid to the quality of the files within the Analysis Service. It is true that 'quality' is difficult to measure in terms of analysis work. However, the Committee enquired into the satisfaction of the Chamber of Representatives' Naturalisation Service. This enquiry revealed that no significant problems had been identified in relation to the memorandums issued by State Security. However, the Standing Committee I did not have the impression that the required quality had been discussed at any length, either with State Security or with the clients.

The Analysis Service regards the available period for nationality declarations and choices of nationality as a type of 'deadline' by which the file *must* be completed. It is true that additional information, where present, was also forwarded to the public prosecutor after this deadline. However, there is a chance that the files had already been processed by then at prosecutor's office level.

The Analysis Service has more time for naturalisation applications. On the one hand, State Security's deadline *in casu* is four months. On the other hand, the Chamber of Representatives waits to process a file if the Analysis Service notifies it that an '*investigation is being carried out*'.

The service itself regards the work pressure as manageable. Staffing at the Analysis Service for such files was estimated at 5.7 FTEs (2010), out of a total of 90 employees.

II.1.2.3. Procedure at the External Services

The manner in which the External Services carry out their investigation assignments does not differ from other intelligence assignments except that no specific or exceptional methods may be used. They must limit themselves to the ordinary methods. Article 18(1)(1) limits the use of special methods to State Security's intelligence assignment (Article 7(1) of the Intelligence Services Act). The investigation of 'nationality files' falls under the scope of application of Article 7(4) of the Intelligence Services Act.

The Committee had to conclude that External Services' response time varied from 'quick' (within a week) to 'slow' (several months). In some cases, no answer

was given at all[16] and/or a reminder was necessary. Sometimes the information arrived late, i.e. after the Analysis Service had already sent its memorandum to the competent authority. The Committee therefore held that attention had to be paid to the prompt forwarding of additional information from External Services to the Analysis Service. Stricter follow-up of the response from External Services to the Analysis Service's written orders was necessary.

II.1.2.4. The interaction among the various procedures and the follow-up and updating of processed files

There is interaction between the procedures for nationality declaration and choice of nationality on the one hand and naturalisations on the other hand: if an applicant receives a negative opinion from the public prosecutor in relation to a declaration or choice and does not bring his or her case before the Court of First Instance, the application is officially referred to the Chamber of Representatives and is treated as a naturalisation application.[17] The case is thus automatically 'converted' as it were from one procedure to the other. However, if the Chamber of Representatives sends such files to State Security for an opinion, nothing indicates that they have already been handled at the intelligence service. Since the Security Verification Service also does not keep track of 'unknown' *files*[18], they are in practice investigated twice. The creation of what are known as *consultation lists*, which keep track of the people in respect of whom a search has already been performed, is therefore urgently needed.

However, just because a person was 'unknown to State Security' yesterday does not mean that he or she will still be unknown today or tomorrow. After all, the full nationality process takes several months. It is thus possible that a person who was not on State Security's radar at the time of his or her initial application is subsequently on that radar. A consultation list should not, therefore, result in the Security Verification Service failing to check the applicant's identity again. It is nevertheless useful to register who has already been scanned. In this way, State Security at least knows the subject's 'procedural history' and the service can also refer to the original nationality declaration file.

The second reason why such a list is useful and even necessary relates to updating information. If the Security Validation Service initially sent back the subject's application as 'unknown' and new information subsequently came to light, it would be impossible to still use this data without such a list. The same applies to the files of people who are known and were processed by the Analysis

16 For example, because there was no relevant additional data to report. In that case, External Services should have reported this formally to the Analysis Service.

17 Articles 12*bis* §3 and 15 §3 of the Belgian Nationality Code.

18 The problem only arose in respect of people who were 'unknown'. A trail exists for a 'known' file, namely at the Analysis Service.

Service. New information could also come to light here, in both a positive and a negative sense. If the file was meanwhile processed by the Analysis Service, the new data will no longer reach the prosecutor's office or the Chamber of Representatives. The converse may also apply: if a file is submitted twice – intentionally or unintentionally – within a short space of time, this can lead to two different opinions.

II.1.3. STATE SECURITY'S ROLE IN A WIDER CONTEXT

It is not up to the Standing Committee I to comment on procedures for acquiring nationality in general. The Standing Committee I therefore considers only how these procedures run within State Security. It has become apparent in the course of the investigation, however, that file processing at State Security is dependent on many external factors.

The Committee has been able to establish that the statutory descriptions of precisely what State Security must deliver – the '*opinion*' that relates to '*serious facts, specifically related to the person*' – are not very precise. This goes well beyond the scope of State Security.

It is further evident that the manner in which State Security processes the files is dependent on how the other players fulfil their roles. Two examples make this clear. The manner in which municipalities forward files (paper or electronically) and the composition and accuracy of those files has a significant impact on State Security's further processing of those files. But the fact that State Security has no insight into what happens to the files after its intervention makes it difficult to use any information that subsequently comes to light. It is thus obvious that improving how State Security functions in relation to processing such files can be optimal only if the external factors are also adapted.

A number of proposals to change the procedures were included in the Administrative Simplification Service's report on 'Optimising the administrative processing of naturalisation and nationality declarations' (September 2011) (free translation).[19] A proposal was made to integrate the ICT systems of the various players. Information can be forwarded more efficiently and shared more easily in this way. The individual nature and needs of each body must obviously also be taken into account. Attention must also be paid, for example, to State Security's security and classification issues. The Committee recommended that State Security should already take these plans into consideration when developing its own procedures.

[19] www.vereenvoudiging.be.

II.1.4. CONCLUSION

Two findings emerged in relation to the above-mentioned investigation. Firstly, despite the limited number of staff who are entrusted within State Security with nationality declarations, choice of nationality and naturalisation files, the service was able to manage the significant volume of incoming files. On the other hand, follow-up – particularly administrative follow-up – was not optimal. This was partly due to factors outside State Security; after all, the intelligence service is only one link in a broader procedure. The procedures of other players have an unavoidable influence on how State Security can fulfil its duties in this regard.

II.2. MONITORING OF FOREIGN INTELLIGENCE SERVICES IN RELATION TO THEIR DIASPORA IN BELGIUM

Belgium appears to be a source of attraction for intelligence services from other countries. The presence of the European institutions and NATO on Belgian territory is one of the reasons for this. Foreign intelligence services show great interest moreover in Belgian high-tech research in space programmes and the arms industry. However, some of these services also closely monitor the activities of their own migrants in Belgium, who have left their homeland for a variety of reasons. These expatriates often have no plans to return and sometimes acquire Belgian nationality, but retain links with their country of origin. They belong to what is commonly referred to as the 'diaspora'. Activists, dissidents and political opposition groups are obviously also active within such communities and attract the attention of the respective foreign intelligence services.

At the request of the then President of the Senate, the Standing Committee I opened an investigation '*into the manner in which Belgian intelligence services monitor any activities that are engaged on Belgian territory by intelligence services from major immigration countries outside the European Union*"(free translation).[20]

II.2.1. METHODOLOGY, DEFINING CONCEPTS AND DELINEATING THE INVESTIGATION

The Standing Committee I applied a combination of quantitative and qualitative parameters for selecting 'major immigration countries' from outside the European Union. The Committee based its numerical approach on the statistics

[20] This investigation was opened in mid-July 2011 and officially closed in December 2012.

kept by official bodies. The qualitative parameters that were taken into consideration were the following:

- the setting of priorities[21] within the Belgian intelligence services for the activities of foreign intelligence services that monitor their communities in Belgium;
- how intensely the foreign intelligence services monitor their diaspora on Belgian territory;[22]
- the extent to which the diaspora living in Belgium are important to the country of origin;
- how intensely the Belgian intelligence services themselves monitor the various diaspora groups present on Belgian territory;
- the historical political ties between Belgium and the relevant country;
- the strongest growing diaspora or the largest number in recent asylum applications;
- the extent to which incidents between Belgian and foreign intelligence services at that level are known (according to open sources);
- the setting of priorities of the Belgian intelligence services, by which they monitor the activities that the foreign intelligence services engage in within Belgium, but not necessary in relation to monitoring of their diaspora.

Based on a weighting of the above parameters, it was decided to focus the supervisory investigation on 'monitoring the monitoring' of thirteen specific diaspora groups.[23]

What is meant by 'activities that the foreign intelligence services engage in' also had to be defined. For the Standing Committee I, this means, first, any form of intelligence collecting and processing as also described in Article 7 of the Intelligence Services Act, namely '*collecting, analysing and processing information*'. Open source research showed that intelligence services use many methods to collect, analyse and process information or intelligence when monitoring their diaspora. An often recurring working method is establishing what are known as '*friendship organizations*' or groups of friends. These groups, which mostly bring North African immigrants together, provide the opportunity to meet each other, but at the same time facilitate the political supervision that is organised from within embassies, for example. However, the classic method that intelligence services use to monitor activities within migrant communities remains a network of informants. Certain professional groups such as

21 For example, on the basis of the State Security Action Plans.

22 In this regard, State Security stated that the greater the internal and external dissent relating to a particular regime, the greater the chance that these regimes will try to control and manipulate their diaspora.

23 In view of the classified nature of much of the information from this investigation, the Committee could not list the relevant diaspora groups by name.

journalists, interpreters, students and scientists, businesspeople, police officers, etc. are used more readily for this purpose than 'ordinary citizens'. Infiltrators are also used, while several open sources also mention intercepting telecommunications as a source of intelligence. A last form of intelligence gathering at this level seems to be cross-border cooperation among the different intelligence services.

However, 'engaging in activities' is more than just gathering intelligence. According to the literature, intelligence services, in addition to collecting information and intelligence, are also 'more active' and undertake all types of actions. These vary from organising demonstrations to (diplomatic) influence, openly or otherwise, by which foreign governments make use of their intelligence services to lobby, to secretly influence political and official decision-making or to orchestrate propaganda in the media. On the one hand, this is often to put opponents in a bad light and, on the other hand, to prevent negative attention or to generate positive attention for the relevant foreign interests. The (physical and other) intimidation of opponents of specific regimes on foreign soil is also discussed in open sources. Various degrees of intimidation can be noted: this may range from subtle indications that someone is being watched to physical or other threats made against people or family members that are left behind.

In addition to establishing the methodology and defining the key concepts, the area of investigation had to be clearly delineated at two levels. Initially, the direct monitoring of various diaspora by State Security and GISS was not the subject of the investigations, unless the information gathered as a result of that would be forwarded to the foreign intelligence services (see II.2.2.4). The same applied to the general operation of embassies. After all, every foreign representation is entitled to actively engage with its national community. However, the Committee pointed to the sometimes blurred lines between intelligence work and diplomacy. An embassy must maintain diplomatic relations between two countries but sometimes goes further and monitors or controls the diaspora. Diplomats that went 'too far' in monitoring also fell within the scope of the investigation. Because combating the interference activities of embassies could give rise to a conflict with what State Security describes as one of its powers (i.e. 'protecting Belgium's diplomatic relations' – however see II.2.2.1), it regarded this as a delicate matter.

II.2.2. THE LEGAL FRAMEWORK

The issue of monitoring the activities of foreign intelligence services in relation to their respective communities raised various legal questions.

II.2.2.1. Legal basis for the scope of competence of the Belgian intelligence services

Monitoring the activities of foreign intelligence services on Belgian territory is not included *expressis verbis* among the legal duties of State Security or GISS. The Standing Committee I has made several pleas for the explicit inclusion of this power in the Act.[24] The Belgian intelligence services are, after all, best positioned to recognise and assess the activities of foreign partner (or other) intelligence services. The Standing Committee I was able to establish that ample support exists for this recommendation. In addition to the Belgian Senate and the Secretary-General of the Council of Europe[25], the European Parliament was also of the opinion that '*all European countries should have specific national laws to regulate and monitor the activities of third countries' secret services on their national territories, to ensure a better monitoring and supervision of their activities, as well as to sanction illegal acts or activities […]*'.[26]

The lack of such an explicit provision therefore does not mean that there is currently no role for both intelligence services to play.

The competence of State Security is determined by a combination of statutorily defined 'interests to be safeguarded' and a number of specific 'threats' provided for by law. In terms of 'interests', sufficient points of departure can be found for specific actions of foreign intelligence services: '*human rights and fundamental freedoms*'[27], '*the safety and physical and moral protection of persons*' and '*protecting […] the sovereignty […] of the State*'[28] (Article 8, 2° of the Intelligence Services Act). The same applies to 'threats': certain actions of foreign intelligence services can be classified as interference, espionage and even extremism (Article 8, 1° (g), (a) and (c) of the Intelligence Services Act).

The statutory point of departure is less clear for GISS, but not completely non-existent in theory. According to Article 11, 1° of the Intelligence Services

---

24 See Standing Committee I, *Activiteitenverslag 2006* (Activity Report 2006), 132 and *Activiteitenverslag 2008* (Activity Report 2008), 2.

25 *'It would appear that most of Europe is a happy hunting ground for foreign secret services. While most of our member states have mechanisms to supervise the activities of their domestic intelligence agencies as well as the presence of foreign police officers on their territory, hardly any country, with the clear exception of Hungary, has any legal provisions to ensure an effective oversight over the activities of foreign security services on their territory*' (T. DAVIS, in Council of Europe, Speaking notes for the press conference on the report under Article 52 of the ECHR, 1 March 2005 (*www.coe.int/t/e/com/files/events/2006-cia/speaking_notes%20_sg.asp*)).

26 Report on the alleged use of European countries by the CIA for the transportation and illegal detention of prisoners, European Parliament, 2006/2200(INI), 30 January 2007 (among others 48, 188 and 204).

27 This includes the right to privacy or freedom of association that can also be relied on by foreigners opposing their homeland's regime from within Belgium.

28 Under Belgian law, foreign services have no competence on Belgian territory. They may do what ordinary citizens are allowed to do, no more and no less. Certain forms of monitoring may be regarded as an infringement of national sovereignty.

Act, GISS's intelligence tasks include analysing and processing intelligence that relates to:

- any activity which threatens or could threaten the execution of the assignments of the armed forces (in other words any expression of the intent to neutralise, hinder, sabotage, endanger or prevent the preparation, mobilisation and use of the Belgian armed forces, of allied armed forces or of inter-allied defence organisations for missions, actions or operations in a national context, in the context of an alliance or an international or supranational cooperation agreement);
- the safety of Belgian nationals abroad (in other words any expression of intent to endanger the life or physical integrity of Belgians abroad and their family members collectively by destruction, massacre or pillage).

From that perspective, 'monitoring of the monitoring in Belgium' could yield crucial information that may be useful in safeguarding the above interests (e.g. in relation to the *modi operandi* of foreign intelligence services). The Committee therefore did not fully share GISS's view that *'on the basis of the organic law, […] [it is] not authorised to monitor the intelligence activities of these services in relation to their diaspora in Belgium'*(free translation). Notwithstanding this, the Committee was able to conclude that GISS had made efforts in this regard (cf. *infra*).

II.2.2.2. Interference activities versus protecting diplomatic relations

State Security regards 'protecting Belgium's diplomatic relations' as one of its 'competences' (see II.2.1). Although the Committee is aware of the delicate relationships within which State Security must move – including under the Vienna Convention – it emphasised that 'protecting Belgium's diplomatic relations', *as such,* does not fall within the legal scope of competence of this service. State Security must gather intelligence that could constitute a threat to the international relationships of Belgium, among other things. The Standing Committee I wished to point out, insofar as necessary, that any reticence of the service should not result in a failure to inform the Government and the administrative authorities as accurately as possible. It is up to the Government or the competent administrative authority to determine how to make use of the supplied information.

II.2.2.3. Legal instruments of the Belgian intelligence services

As part of monitoring the activities of foreign intelligence services on Belgian soil, State Security and GISS may – insofar as these activities fall within the

scope of their competence – obviously use all the instruments that the legislature has put at their disposal. This includes all forms of intelligence gathering, ranging from consulting open source material to using special intelligence methods.

However, it ought to be noted in relation to such methods that Article 18, 9° of the Intelligence Services Act does not include interference in the list of threats for which State Security may employ exceptional methods. State Security therefore cannot apply such methods in respect of activities in Belgium that can be qualified only as interference. The Committee did not see any convincing arguments for this, especially since exceptional methods are subject to very tight administrative and jurisdictional control. It therefore recommended that the Act be amended in this respect.[29]

II.2.2.4. Cooperation with foreign services that monitor their diaspora

Article 20 §1 of the Intelligence Services Act instructs intelligence and security services to ensure '*that there is cooperation with foreign intelligence and security services*' (free translation). The third section of the same 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 but classified instruction on bilateral cooperation with correspondents. The principles set out in this instruction can certainly be applied to monitoring by foreign services of their diaspora, both as regards any approval of the activities of foreign services on Belgian territory and any cooperation in actions. However, the directive limits the exchange of information to the formal context; there are no precise guidelines on the nature of the information that can be shared with foreign services.

Although the Standing Committee I regarded this State Security directive as valuable, it pointed to the role that the legislature has entrusted to the Ministerial Committee in this regard. The Committee believed that certain options which State Security has included in its directive ought to be endorsed by those who are politically responsible. The Committee therefore again repeated[30] its recommendation to the Ministerial Committee to issue such a directive.

GISS has apparently also worked on a similar memorandum with 'verifiable criteria' for the purpose of potential cooperation with foreign intelligence services (in the broad sense).

---

29 The investigation did not demonstrate that this legal loophole has caused any problems in relation to 'monitoring of the monitoring' to date.

30 See STANDING COMMITTEE I, *Activiteitenverslag 2011* (Activity Report 2011), 5–6 above.

II.2.3. THE MANNER IN WHICH THE INTELLIGENCE SERVICES MONITOR THE MATTER

II.2.3.1. Setting priorities

Interference and espionage activities (in the broad sense and thus not limited to 'monitoring a diaspora') of various foreign intelligence services on Belgian territory are 'permanently monitored' by the General Intelligence and Security Service and also monitored '*actively* (and as a priority)'[31] by State Security. But to what extent do the intelligence services specifically monitor activities that foreign intelligence agencies engage in within Belgium in relation to their communities? What criteria are used to determine whether or not these activities must be monitored and what priority is given to this monitoring?

Around 150 problematic cases in total within the operational section of State Security's annual action plans are listed as 'an active priority' or 'active'. Whether or not the activities of a specific intelligence service with regard to a community are monitored and, if so, with what priority, are documented here. With one exception, State Security has included in the action plans consulted all the countries that the Standing Committee I defined as 'major' immigration countries (see II.2.1) in relation to espionage or interference activities, placing them under the heading 'active' or 'an active priority' for monitoring.

Priorities are generally set on the basis of evaluations by the analysis services and after internal consultation with the operational services. Staffing capacities, current requirements, internal need for intelligence and the information needs of external partners (domestic and foreign) are also taken into account. There are various other criteria that also play a role. The Committee assessed these as valuable and pertinent. However, it seems they have never been included in a directive or instruction, which does not facilitate their uniform application by the various internal services. The Standing Committee I also had to conclude that these criteria were not formally applied within the Analysis service. Different and additional criteria were also sometimes applied. The Committee held the view that the criteria for monitoring a specific 'monitoring of the diaspora' should not differ according to diaspora. The Standing Committee I also recommended that these criteria be recorded in a document. This must allow the various sections to do the testing within their area in a more uniform manner.

Obviously, 'interference and espionage in the military sphere' are areas of interest for GISS with regard to the intelligence services of specific countries or

[31] Active prioritised monitoring means that State Security engages actively and as an absolute priority in activities to acquire, expand or strengthen the information position in relation to these matters. 'Normal' active monitoring means the same thing but without absolute priority being given to the matter.

regions. The link with any 'monitoring of the monitoring' is not evident as far as this competence is concerned. GISS appeared to focus on one specific diaspora in relation to this 'monitoring of the monitoring'. GISS's competence in this regard was also based on its role in safeguarding military interests abroad.

II.2.3.2. Deployment of resources

Human resources are not solely and clearly assigned within the intelligence services to one matter, one problem (such as 'interference by foreign services' and certainly not 'monitoring of the monitoring') or even to one geographical area. The share of 'interference by a foreign intelligence service' in State Security's total workload also fluctuates over time. It was therefore not possible to determine which resources State Security deploys in this regard.

This also applied to GISS in relation to what extent the permanent monitoring of certain intelligence services yields information about how these services gather intelligence about their own diaspora. However, reference also had to be made to the fact that an analyst at GISS focused specifically on the actions of a certain intelligence service in Belgium (including those with regard to its own diaspora) in the wider context of monitoring the relevant diaspora in Belgium. This, notwithstanding the fact that GISS did not assign itself any organic authority in this regard and did not treat this theme as a priority.

The 'monitoring of the monitoring' took place on the basis of all legally permitted methods. There was nothing specific to report at this level. Information was regularly exchanged, for example, between State Security and GISS. However, information was also shared, where possible, with other authorities (e.g. FPS Foreign Affairs). State Security, in particular, relied on special intelligence methods for this purpose. Although these methods are often used as part of the struggle against interference and espionage activities of foreign intelligence services, it was very difficult to determine, let alone quantify, to what extent 'monitoring of the monitoring' was targeted. This related mostly to targets that were followed in relation to espionage and/or interference activities, and for which it could be established in context that they were also focusing on diaspora in Belgium as subjects of interest.

II.2.3.3. Output of the Belgian intelligence services

State Security drew up memoranda on the problem of interference by foreign intelligence services in the diaspora at the request of an authority or at its own initiative if the service deemed it relevant. The latter was the case, for example, if State Security established that the relevant activities could be regarded as 'criminal activities' or if these constituted a danger to public order.

The addressees included the Prime Minister, the Ministers of Foreign Affairs, Justice and Interior, the King's chief of staff, the State Secretary for Asylum,

Immigration and Social Integration, various services within FPS Foreign Affairs, the Belgian ambassadors stationed in various countries, the Commissioner General for Refugees and Stateless Persons, the Immigration Office, as well as GISS, CUTA and the Governmental Crisis Centre.

Information was also sometimes forwarded to foreign intelligence services, even though this seldom happened. State Security bases this on its own legal powers and duties, and not on those of the foreign service.

The Standing Committee I also enquired about the number of reports and analyses that dealt with 'monitoring of the monitoring'. However, State Security only had overall figures on the monitoring of 'espionage' and 'interference' for 2011.[32] Hundreds of reports and analyses were drawn up in that year for some of the countries that the Standing Committee I selected. It was not known how many of those information reports and memoranda related fully or partially to 'monitoring of the monitoring'.

The number or size of the reports are obviously not always an indicator of the relevance of their contents. The activities of an intelligence service are difficult to represent in terms of purely quantitative data. This means that the measurability of the prioritised active handling of certain problems based on quantifiable data, such as the number of reports and analyses, is quite limited. The Committee therefore also made an estimate (marginal testing) of the quality of the output. State Security was requested to submit 10 analyses and 25 information reports in that regard.

Reference was made in respect of documents for internal use to ordinary and operational information reports of State Security's external services, telexes and reports of meetings with partner services.

State Security referred in respect of assessments to the 'Phenomenon Analysis on Interference (December 2009)', which deals with the various forms of interference – thus not only those relating to diaspora groups in Belgium – by foreign intelligence services. This well-documented study constituted a textbook case of an intelligence product for the Standing Committee I, which is very useful for both internal and external use.[33] The Standing Committee I subjected the other submitted analytical memoranda (investigation into interference activities) to marginal testing. With the exception of one memorandum, it could be established that the topics discussed corresponded to State Security's proposed list of priorities. This involved countries that, barring the same exception, also appeared on the Standing Committee I's checklist. The majority

---

32 The figures related to both the Operational Service's information reports and the Analysis Service's memoranda, namely the investigation assignments ('apostilles'), memoranda to domestic authorities, memoranda to foreign partner services and summary memoranda. However, depending on the monitored country, the emphasis focused either on espionage or on interference.

33 Since this phenomenon assessment dates back to 2009, the Standing Committee I felt it appropriate to update it, based on the available material in the specific memoranda, in order to guarantee business continuity. However, State Security – which agreed with this recommendation – pointed out a lack of time and staff to carry out such an update.

of the memoranda that the Committee could look at were drawn up at the services' own initiative.

All of the memoranda concerned were classified as 'CONFIDENTIAL' or 'SECRET'. The Committee could agree that the documents were assigned a classification level. However, it had to conclude that the reason for the difference in classification levels was not always clear. An urgency level was also added to the most recent reports, which enabled the addressee to see how quickly the author wished the information to be processed.

The consulted memoranda were mostly well-structured, adequately detailed, easy to read and substantively relevant. Although the Committee could not place itself in the clients' shoes, it still felt that some of the memoranda could have been more concise. Some memoranda started with a concise summary and this clearly added value. The memoranda were well-documented and represented the chosen topic in a balanced way. However, since they were not differentiated according to the addressee, the Committee could not escape the impression that some of the information would not have been equally relevant for everyone (what is interesting to a minister is not necessarily interesting to a police force and vice versa).[34] The Committee could not give an opinion in this investigation on the 'prompt' nature of the memoranda or the potential 'added value' and direct usefulness thereof for decision makers. This required a different type of investigation.

GISS was also asked to submit analyses and information reports that related to the subject of the supervisory investigation. In view of its own 'declared lack of competence' (see II.2.2.1), it was understandable that GISS only provided a few documents.[35, 36] A report of around ten pages described GISS's activities relating to (the intelligence services of) three countries under the headings of 'Intelligence and Espionage', 'Extremism' and 'Terrorism', among other things. Mention was made here and there to 'monitoring of the monitoring'. Another report was far more extensive and detailed. It related to one country and focused more on the monitoring of the diaspora. Since the Committee only had access to a few documents, it did not wish to make any substantive assessment. It could however conclude that the manner in which 'monitoring of the monitoring' was reported on fell within the scope of GISS's legal assignments.

The Committee concluded that few documents concentrating specifically on 'monitoring of the monitoring' were drawn up by either of the intelligence services. On the other hand, it seemed as though there was definitely knowledge

---

34 State Security also agreed that differentiating the memoranda based on the addressee would indeed mean added value but once again pointed out its limited workforce.

35 The addressees of these documents included the Chief of the King's Military Guard, the Defence Cabinet, the Chief of Defence, various ACOS departments, the local GISS-CI/C, SHAPE and the partners State Security, CUTA and the Federal police. The Standing Committee I found it surprising that FPS Foreign Affairs had not received these documents.

36 GISS advised that it was working on a third document that related specifically to the activities of certain intelligence services in Belgium. However, the document was not yet finalised at the time of the investigation.

about this phenomenon. Generally, however, this knowledge remained a personal asset of the employees, which was seldom documented in the form of analytical memoranda. These were drawn up only at the express request of third parties or when it was necessary to draw policy-makers' attention to specific situations or events. This obviously means that when employees leave their job for any reason, this knowledge leaves with them.

II.2.4. SOME SPECIFIC POINTS OF ATTENTION

II.2.4.1. Methods and resources used by foreign intelligence services to monitor their citizens

Most foreign intelligence services have a network of informants within the diaspora. The main task of such networks (which can be developed and managed by members of the intelligence services operating under diplomatic cover) is to control, manipulate and sabotage *any* form of opposition to the political regime of the country of origin. Relatively classic, 'soft' methods are usually relied on: spreading misinformation, establishing own 'opposition parties' to divide the opposition, bribing opponents, etc. Other techniques are also used: facilitating or hindering the issuing of official documents or return to the homeland, exemption from military service, etc. If this does not yield any or enough results, 'harder' methods are sometimes used (such as putting pressure on or intimidating opposition figures or their family members in the homeland). There were rumours within some diaspora groups about hit teams that would come to Belgium on the regime's instructions in order to eliminate opponents. However, no evidence was ever produced of this. These were probably misinformation campaigns.

Another commonly used method is setting up, financing[37] or manipulating all types of social-cultural 'friendship organisations' that are apparently intended to strengthen ties between the diaspora and the homeland but which actually serve another purpose.

Reference can also be made to the role of political control over the religious convictions of the diaspora. After all, control over a diaspora involves control over the religious convictions and practices that exist within a specific diaspora and the possible political consequences thereof.

II.2.4.2. What difficulties do the Belgian intelligence services face when monitoring foreign services?

As a smaller intelligence service, State Security stated that it does not always have the necessary capacity to properly monitor the interference attempts of foreign intelligence services. In its opinion, this could lead to gaps in the

[37] Financial stimuli moreover form a proven means to ensure the loyalty of certain groups associated with the diaspora.

intelligence. There was moreover the general problem of misinformation and false rumours that hindered intelligence gathering. Lastly, attempts by intelligence services to convince Belgium that everything was peaceful and quiet within their own community were also pointed out.

II.2.4.3. Countermeasures

If foreign intelligence services secretly gather intelligence on Belgian territory, this may be regarded as an infringement of sovereignty or may even constitute a crime. The question arises as to what measures the Belgian intelligence services can or must adopt.

Clearly, it cannot move 'actively' to influence the course of events. The legal framework only allows for limited direct interventions. The head of State Security or GISS can only address oral questions to its foreign counterpart or inform the diaspora of the activities that a foreign intelligence service is undertaking in relation to that community.[38] However, if further action appears necessary, the intelligence service must notify the authorities that are competent in that regard, such as the judicial authorities or FPS Foreign Affairs.[39]

Although judicial measures can be used, Standing Committee I noted that the definition of the threat of 'espionage' under Article 8, 1° (a) of the Intelligence Services Act differs completely from the constituent elements of the crime of 'espionage', and that 'interference' (Article 8, 1° (g) of the Intelligence Services Act) is not even a crime. Some activities of foreign services are punishable (e.g. infringements of the Privacy Act, the Electronic Communication Act, etc.).

Other countermeasures – which can be applied by FPS Foreign Affairs – consist, for example, of declaring diplomats *persona non grata*, not extending their accreditation[40] or even demanding that the head of the foreign intelligence service in Belgium recalls the agent caught involved in clandestine activities.[41]

II.2.5. CONCLUSIONS

Control over the activities of foreign intelligence services on Belgian territory is not explicitly included as such as a legal duty of State Security or the General

---

38 Article 19, §1 of the Intelligence Services Act allows for this: '*The intelligence and security services may only share the intelligence […] with authorities and people that are the subject of a threat as referred to in Articles 7 and 11*' (free translation).

39 Despite the fact that this public service can possibly be regarded as the most important 'client' and is moreover the appropriate service to assist State Security in calling a halt to the activities of foreign intelligence services on Belgian territory, it turned out that there were no documented working arrangements between them.

40 State Security issues opinions to the Chairman of the Management Committee of FPS Foreign Affairs for the purpose of the accreditation of embassy personnel.

41 STANDING COMMITTEE I, *Activiteitenverslag 2001* (Activity Report 2001), 117–118.

Intelligence and Security Service. Despite this lacuna, it is clear that State Security is competent in this regard given the legal 'interests to be safeguarded' by it, combined with a number of specific 'threats' summarised in the Intelligence Services Act. The legal anchor is less clear for GISS, but not completely non-existent in legal theory. Information and intelligence on 'monitoring of the monitoring in Belgium' may yield crucial information that can be useful in the safeguarding of specific interests summarised in Article 11, 1° of the Intelligence Services Act.

The Standing Committee I was able to establish in its supervisory investigation that State Security paid attention to the activities that foreign intelligence services engaged in with regard to their diaspora in Belgium. However, it is very difficult to determine how the intelligence service set and gave shape to its specific priorities in this regard. Although the Committee was informed of valuable and pertinent criteria in this regard, there was no formalisation or formal application thereof. Due to the lack of documented criteria, there is an impending danger of setting pragmatic priorities and a real chance that the priorities defined in the Action Plans will not be implemented.

Barring one exception, all countries defined by the Standing Committee I as 'major' immigration countries were listed in *Action Plan 2012* to be monitored at least 'actively' by State Security under the broader term of espionage and interference activities. The Committee was able to conclude that this was also put into practice.

GISS, in turn, had a more than adequate information position with regard to two specific foreign intelligence services. In that context, and without having to actively search for it, the service also possessed information on the actions of these foreign intelligence services in relation to their diaspora. It further transpired that there was a lot of information within GISS regarding the activities of the intelligence services of a specific country that were active in Belgium, both in general and with regard to their diaspora. GISS worked in a far more 'targeted' manner here despite the fact that the service wrongly regarded itself as unauthorised in this regard.

In general, however, the information gathered by both intelligence services turned out to remain a mainly personal asset of the employees that was only rarely formalised. Memoranda are normally only drawn up either when an express request is made to that effect or when circumstances are of such a nature that it is necessary to draw policy-makers' attention to specific situations or events. This raises questions in relation to business continuity: after all, if employees leave their job for any reason, this knowledge leaves with them. An exception to all of this is a document such as the 'Phenomenon Analysis on Interference (December 2009)' of State Security, which, if regularly updated, is regarded by the Standing Committee I as a textbook case of an intelligence product.

II.3. POSSIBLE MONITORING OF AN INDIVIDUAL DURING AND AFTER HIS DETENTION IN BELGIUM

In July 2010, a British newspaper[42] reported that M.J., who was convicted in relation to the Trabelsi case and detained in a Belgian prison, was purportedly put under pressure by a certain David, who was introduced as an agent of the British intelligence service. David purportedly offered M.J. the opportunity to go and work for his service. After M.J. accepted this proposal, he was allegedly taken unlawfully to Great Britain and detained there in secret. M.J. is said to have been interrogated there for two weeks and more or less forced to work for the British intelligence service. According to M.J.'s lawyer, this operation could not have taken place without the consent, or at least the knowledge, of the Belgian intelligence services, among others. The Standing Committee I then opened an investigation on 28 September 2010.

The final report – of which a summary can be found under II.3.1 – was sent to the Monitoring Committee of the Senate and to the competent ministers in April 2012 and discussed within the Monitoring Committee at the start of May 2012. However, the Committee was informed at the end of May 2012 of a memorandum on this investigation report that State Security had addressed to the Minister of Justice. State Security made substantive comments on the Committee's final report in that memorandum. Some of those reservations related to elements that were not reported to the Committee earlier during the investigation and that gave rise to questions as to the relevance of its conclusions and recommendations. The Standing Committee I therefore felt obliged to investigate these new elements further on the basis of additional questions. The relevant report can be found under II.3.2.[43]

II.3.1. FINDINGS FROM THE INITIAL REPORT

II.3.1.1. Background

M.J. left his country of birth (Morocco) at the age of 16. He lived in various European countries, including Spain, where he was arrested for the first time. After his release, he sought refuge in mosques. After living in Germany and the Netherlands, he travelled to London, where he was received by leaders of the radical mosque of Finsbury Park. M.J. thus became a member of a radical Islamic group that recruited people for military training in the Pakistan/

42 R. VERKAIK, *The Independent*, 23 July 2010 (Uncovered: Britain's Secret Rendition Program).

43 The supplementary report was finalised in mid-October 2012.

Afghanistan region or in Georgia. He supplied false passports to aspiring jihad fighters.

At the end of 2001, M.J. left Great Britain. A judicial inquiry was underway against him there. He was detained by Dutch police in December 2001. He was extradited to Belgium at the start of January 2002 on suspicion of involvement in an Afghan network. After the judicial inquiry, in which State Security cooperated, the Correctional Court sentenced M.J. and seven other accused to prison terms ranging from thirty months to ten years.[44] The main charges were: belonging to a criminal organisation, forgery of documents, falsification or counterfeiting of passports and recruiting people for foreign armies. M.J., who was also found guilty of residing illegally in Belgium and using a false name, was sentenced to four years' detention, with half of the sentence suspended for five years. The judgment refers to the fact that the accused '*demonstrated his religious intolerance and anti-Western radicalism*' (free translation) during his trial.

M.J. was imprisoned. As he was still considered to be illegally resident in Belgium at the end of his sentence, he submitted a regularisation request at the end of December 2003. He did so for fear that he would be repatriated to his country of origin. The request was, however, rejected.

At the end of his sentence, in mid-December 2003, M.J. was therefore in the hands of the Immigration Office. He remained in detention but as an 'administrative detainee' pending his extradition or repatriation. The necessary steps for this were being prepared.

In February 2004, M.J.'s lawyers advised the Immigration Office that his client wished to be repatriated to Great Britain as he had a valid residence permit for that purpose. The Immigration Office then contacted the British authorities, which confirmed the authenticity and validity of this residence permit. M.J. was then visited twice by delegates from the British Consulate in Brussels to prepare for his repatriation to Great Britain. The British authorities agreed to the repatriation in April and he was then transferred.

II.3.1.2. Monitoring of M.J. during and after his detention by State Security

There is no document proving that State Security monitored M.J. after his conviction or during or after his detention. The service was, however, aware of the facts from July 2010 via the newspaper articles, first in the British and then the Belgian press. However, State Security did not have any information based on which it could confirm or refute the story. The service expressly denied any prior knowledge of these facts and emphasised that it had not in any way participated in transferring M.J. to Great Britain. State Security declared that it has not given any information to the foreign intelligence service regarding M.J's

44 One of the other accused in this trial was Nizar Trabelsi, who was convicted of preparing a suicide attack against the US base of Kleine Brogel.

transfer. The Standing Committee I's investigation did not reveal any information that could refute these statements.

According to State Security, M.J. chose to leak his story to the media in order to embarrass the British government, which he held responsible for his problems with the immigration services and public assistance. In August 2010, State Security sent a classified memorandum to the Minister of Justice to notify him of this.

II.3.1.3. Monitoring of M.J. during and after his detention by GISS

M.J. was only known at GISS based on the summary of a court file relating to Nizar Trabelsi and Maaroufi Tarek. This stated that M.J. was sentenced to four years in prison due to his role in recruiting aspiring jihad fighters who wanted to travel to Afghanistan. GISS had received this information from the federal police.

However, no trace was found of any monitoring of M.J. at GISS. Even the articles from the Belgian and British press from July 2010 seemed to have failed to attract GISS's attention. Lastly, there was no trace at GISS of any exchange of information relating to M.J. with foreign counterparts.

II.3.2. CONCLUSIONS OF THE FIRST INVESTIGATION REPORT

The Committee had to conclude that GISS had remained completely irrelevant to this case. State Security also appeared not to have participated in any way in the steps that were taken to repatriate M.J. to Great Britain. The Belgian intelligence services therefore did not infringe the rights that the Constitution and the law granted to this person. The repatriation to the United Kingdom was, moreover, not unlawful.

The Committee arrived at a different conclusion in regard to the coordination and efficiency of both intelligence services. Even though the case related to a person who was convicted of a serious case of terrorism, neither State Security nor GISS had monitored his situation after his conviction. They had likewise not tried to gauge what his position would be after his release. Neither service exchanged even the minimum information in this regard. They remained ignorant both with regard to M.J.'s administrative situation at the end of his sentence and the measures that the Immigration Service had taken to transfer him to the United Kingdom.

Although no cooperation protocol existed at the time that the facts occurred between State Security (and GISS) on the one hand and the Directorate-General

for the Execution of Penalties and Disciplinary Measures[45] or with the Immigration Office and the Commissioner General for Refugees and Stateless Persons[46] on the other hand, Article 14 of the Intelligence Services Act nevertheless provided for the opportunity to request information from these public authorities.

Even after they became aware of the press articles about M.J.'s transfer to Great Britain, neither State Security nor GISS took any initiative to check these facts, more specifically to check the circumstances under which and the intentions with which M.J. had received the visit from embassy representatives shortly before the end of his detention. By not responding to this information, State Security adopted a passive attitude that was inconsistent with the attitude that it had always declared to adopt with regard to friendly foreign intelligence services deemed to be operating in Belgium. That attitude was that these services may operate in Belgium only insofar as they observe Belgian law, have State Security's prior consent and act fully under State Security's control.[47]

II.3.3. FINDINGS FROM THE SUPPLEMENTARY REPORT

II.3.3.1. No monitoring of M.J. during his detention

In its original report, the Committee criticised the fact, among other things, that State Security had failed to monitor the subject (and his situation) during his detention. Although State Security gave various explanations for this in a memorandum to the Minister of Justice, these were not raised in any way during the initial investigation. State Security explained that M.J. was no longer monitored during his detention because it held the view that he could not cause any further harm during his detention and because the service was understaffed and overburdened during that period because of the assistance it had to provide in major terrorism cases. It was also suggested that monitoring was unnecessary because M.J. had been remanded during the judicial inquiry and was thus under

45 Such a protocol was concluded on 20 November 2006, in the wake of the Radicalism Action Plan. The main aim of the protocol agreement was to lay down the conditions for cooperation and the exchange of information between State Security and the Directorate-General for the Execution of Penalties and Disciplinary Measures with regard to detainees convicted of terrorism. According to the Standing Committee I, the application of the measures provided for by this protocol agreement would have allowed State Security (and GISS) to check who had been in contact with M.J. during his detention.

46 The Standing Committee I was of the opinion that in light of this protocol agreement, State Security may have been informed of the administrative situation of M.J. after the end of his sentence.

47 See, for example, A. WINANTS, '*Anything you can do I can do better?*', Orde van de Dag, Theme: A public debate on secret methods, J. VANDERBORGHT and B. VANGEEBERGEN (eds.), Kluwer, December 2011, 45.

the control of the judicial authorities. He was once again monitored by the Immigration Office during his administrative detention.

The Committee pointed out first that State Security itself always emphasises – completely correctly – that the judicial authorities pursue a different aim than an intelligence service. It therefore appeared strange to the Committee that the service justified its own inactivity with possible control by the judicial authorities. The same obviously applied to the 'control' by the Immigration Office: this service monitors the residence status of detainees, not the possible threat that they pose to the internal or external security of the State.

But even State Security's first two comments could not convince the Standing Committee I: detention certainly did not rule out the need to monitor the detainee and any contacts.

In response to the Committee's additional questions, State Security specified that the decision not to monitor M.J. was made taking into account the threat at the time, the service's workload, the available resources and priorities. However, the Committee held that this 'decision' was not preceded by any assessment, resulting in a written memorandum drawn up by the analysis services.

The Committee reiterated its finding that the subject was one of the few people convicted of terrorism in Belgium at the time, which phenomenon should logically have been an absolute priority of the service.

The Committee was well aware – in view of the clearly limited resources – that it is impossible for an intelligence service to monitor everyone that constitutes a potential threat (even an intensive one). Choices therefore had to be made, even if the resources had been at full capacity (see also II.3.3.3). But the Committee emphasised, in respect of the threats for which State Security must monitor convicted persons, that there must at least be a prior and real assessment resulting in a reasoned, searchable and verifiable decision. The Committee pointed out that State Security had itself recently acknowledged the necessity of this in its '*Instruction for bilateral cooperation with correspondents*' (free translation). Under the heading '*Transparency and traceability*' (free translation) it calls for an '*administrative trail*' (free translation) for every action, in view of an audit by the Standing Committee I, among other things. The Committee can only welcome such instructions.

II.3.3.2. Protocol with the Immigration Service and CGRS

In its original report, the Committee recommended that the intelligence services enter into a cooperation agreement with the Immigration Service and with the Commissioner General for Refugees and Stateless Persons (CGRS). It later turned out that such an agreement had already been concluded on 27 June 2011, but that State Security had failed to take the initiative to notify the Committee thereof, as provided for in Article 33 of the Review Act.

II.3.3.3. The incomplete resource framework

The Committee wished to know from State Security whether its current resources sufficed to better guarantee the monitoring of specific detainees and the activities of foreign services on Belgian territory. State Security referred to the situation as being '*as problematic as in 2003 and stated that the service thus had to make choices in relation to the persons/activities/phenomena that could be monitored*' (free translation). Although the Committee found that the number of External Services FTEs increased by almost 30% from 2003 to 2012, it regretted that the global staff complement was incomplete and that there had been a percentage increase in understaffing. The Committee understood that choices had to be made as a result of this. However, the Committee was just as convinced that the question of prioritising will remain, even if the staff are at full capacity.

II.4. TRADE UNION ASSISTANCE DURING QUESTIONING ARISING FROM A SECURITY INVESTIGATION

At the end of 2011, a recognised trade union submitted a report to the Standing Committee I. Agents of the GISS Security Division had denied a permanent representative of the trade union access to its premises. The result was that this trade union employee could not be present during questioning between GISS agents and a serviceman as part of his security investigation. According to GISS, the Intelligence and Security Services Act of 30 November 1998 and the Classification Act of 11 December 1998 preclude such presence. However, the trade union was of the opinion that Article 13 of the Act of 11 July 1978 governing relationships between the government and the trade unions of military personnel and – in particular – Article 2 of the Intelligence Services Act entitle it to be present at such interviews in order to safeguard the individual interests of its members. The Committee decided to study the case and extended the investigation to State Security.[48]

The Committee held that the regulations with regard to security investigations (namely the Classification Act of 11 December 1998, the implementation decree of 24 March 2000 and the Ministerial Committee directive of 16 February 2000 that organises security investigations in detail), do not deal with the presence of any third party at an interview or questioning.

[48] Shortly after the start of the investigation at the end of December 2011, the serviceman concerned appealed to the Appeal Body for security clearances, certificates and advice against the withdrawal of his security clearance. Although the report was not made by that serviceman, the Committee still felt it was opportune to apply Article 3 of the Appeal Body Act: the investigation was suspended pending the decision of the Appeal Body. This judgment was delivered in mid-February 2012. The investigation was completed at the end of September 2012.

The Committee also did not read any such rule in Article 2 of the Intelligence Services Act. This provision states that the intelligence services '*when performing their assignments must ensure […] compliance with and [contribute] to the safeguarding of individual rights and freedoms as well as the democratic development of society*' (free translation). The Committee was of the opinion that no precise, subjective rights could be inferred from this provision, regardless of its importance as a general framework for the actions of intelligence services in a democratic society.

Even the declarant's reference to the 'rights of defence' as an administrative legal principle was not relevant in this case, as this concept applies only in disciplinary and criminal cases.[49] A security investigation has a different purpose and its own procedure.

Lastly, the Committee analysed the various laws pertaining to the relationship between trade unions and the government: the Act of 11 July 1978 regulating relationships between the government and the trade unions of military personnel (Article 13), the Act of 19 December 1974 governing relationships between the government and the trade union of its personnel (Article 16) and the Act of 17 March 2004 governing relationships between the government and the trade unions of the personnel of State Security external services (Article 15). No right to be present at interviews for security investigations could be inferred from these provisions.

The Committee therefore decided that there was no obligation to allow trade union representatives for military or non-military personnel.

On the other hand, the Committee questioned whether there are rules that could prohibit it. It referred to the provisions of the Classification Act that form an obstacle to the presence of a representative during an interview if he or she does not have a security clearance. On the one hand, Article 8 of the Classification Act stipulates that classified information may only be examined under a twofold condition: the person involved must have a security clearance and a need to know. It clearly would not be obvious at all under those conditions to allow a trade union representative to attend a meeting if classified information had to be discussed. On the other hand, access to classified zones[50] may also be made subject to restrictive conditions. The Committee stated, however, that the latter may not be used as a specious argument to make the presence of a trade union representative impossible by definition, as an interview can also take place outside such zones.

---

49 See I. OPDEBEEK, 'De hoorplicht' (The obligation to hear), in *Principles of proper administration*, I. OPDEBEEK and M. VANDAMME (eds.), Bruges, die Keure, 2005, 236.

50 A classified zone is *'the site primarily intended for handling and storing classified documents and protected by a security system intended to prevent access by any unauthorised persons*' (free translation) (Article 1, 7° of the Royal Decree on classification and security clearances, certificates and advice).

The Committee therefore concluded that, with the exception of the situation in which classified information were to be discussed, the presence of a 'neutral observer' at the questioning is neither prohibited nor compulsory. When asked, neither intelligence service showed support for a system in which a trade union representative would have a right to assist.

II.5. JOINT INVESTIGATION INTO CUTA'S THREAT ASSESSMENTS RELATING TO FOREIGN VIP VISITS TO BELGIUM

When it became apparent that CUTA regularly carried out threat assessments as a result of visits by foreign VIPs to Belgium, the Standing Committees P and I decided to open an investigation in mid-2010.[51] The intention, among other things, was to determine whether this was a legal task of CUTA, how the service fulfilled this task and how the quality of the assessments is guaranteed.

II.5.1. THE LEGAL BASIS

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 Assessment Act). The threats referred to in Article 3 of the Threat Assessment Act are terrorism and extremism as defined in Article 8, 1° (b) and (c) of the Intelligence Services Act. CUTA is not competent in respect of other threats (e.g. threats relating to a criminal organisation or public order).

II.5.2. THE SPECIFIC PROCEDURE

Ad hoc assessments are performed by experts seconded from the supporting services.[52] These experts (eleven in total in 2012) are both authorised to act in

---

51 The investigation – which was officially opened at the end of June 2010 – could not be finalised earlier (start of February 2012) because of the CUTA's rather long response times and the difficulties that were experienced in arranging meetings with the members or managers of CUTA. The Standing Committees P and I therefore regretted that CUTA was so uncooperative in this investigation.

52 Article 7, 1° of the Threat Assessment Act and the Royal Decree of 23 January 2007 on the personnel of the Coordination Unit for Threat Assessment. The expert's profile and job description were included in detail in Appendix 3 to the Royal Decree of 23 January 2007.

respect of certain countries or regions in the world and for specific aspects. They performed 178 assessments for foreign VIP visits to Belgium in 2010.[53]

In an internal memorandum from 2011, CUTA explained that '*the ad hoc assessment […] always [includes the following]: an account of the event, a description of the context (political situation, historical precedents, etc.), the determination of the threat level and, where applicable, the proposal of specific measures*' (free translation). CUTA further explained that the quality of the competent expert's proposed assessment is checked by means of informal peer counselling. This takes place during the daily meetings with the departmental head and/or director of CUTA and is attended by a second expert who was not involved when the assessment was drawn up.

Although the ad hoc assessments are thus drawn up according to a standardised scheme, the Standing Committees P and I had to conclude that no formalised procedures or assessment criteria were available. CUTA does not make use of checklists or worksheets. It was even of the opinion itself that a formalised procedure was not necessary, relying for this on the individual nature of each case and 'the general principles of assessment'. The Coordination Unit was of the opinion that the only guarantee of uniform control is testing by management in relation to CUTA's general strategy. It argued that similar foreign services apply an identical or very similar procedure. Even so, CUTA did not provide a single specific piece of information to substantiate its views. The Committees referred, on the other hand, to the procedure of the federal police that is authorised to carry out threat assessments other than for terrorism and extremism. It applies a specific method (which involves the weighting of criteria) that was developed on the basis of foreign examples. However, the hierarchy of CUTA stated that it did not believe in a method by which the assessment must follow a specific template.

Lastly, the Committees focused on knowledge development and transfer by the experts. They established that these took a very unstructured form and were often based on personal initiatives. No training plan was presented either.

As far as 'the specific procedure' is concerned, the Standing Committees P and I thus arrived at the conclusion that the assessments were made informally and the experts did not even receive uniform training. This situation could become problematic for CUTA if an incident were to happen and it was called upon to explain its methodology. The Committees emphasised that the expertise, which is certainly present within CUTA, is not inconsistent with the use of a standard method that also takes certain specifics into account.

---

[53] CUTA initially provided the following figures: 665 applications for assessments and 728 completed assessments. It subsequently transpired that only 220 ad hoc assessments of Belgian (42) and foreign (178) VIPs had been completed.

II.5.3. VIEW OF THE GOVERNMENTAL COORDINATION AND CRISIS CENTRE

The most important 'client' with regard to VIP assessments is the Governmental Coordination and Crisis Centre (GCCR). The CGCCR explained that it is routine to request CUTA's opinion when the visit of a foreign VIP is announced. It approaches the police as well only when there are specific elements of a criminal threat.

The Standing Committees P and I established that the CGCCR had positively evaluated the work delivered to it. The management stated that it was very satisfied with the assessments, both in terms of their content and the speed with which they were received. According to the CGCCR, the assessments were very useful for the purpose of adopting the necessary measures.

The CGCCR did, however, emphasise that it was always important to distinguish among (a) the assessment of the threat (CUTA's task), (b) the task of deciding which measures are necessary (CGCCR's task) and (c) implementing those measures (a task for the police or State Security).

II.6. HANDLING OF REQUESTS FOR 'AUTHORISATION FOR ASSIGNMENTS' AT STATE SECURITY

A member of State Security lodged a complaint with the Standing Committee I because his 'authorisation for an assignment in the public interest' was refused. He alleged that he had been discriminated against as other colleagues were granted such authorisation.[54, 55]

There is a clear regulatory framework for this authorisation both for personnel of internal services[56] and external services[57] of State Security. The

---

54 As there was initially talk of other people who might lodge a similar complaint, the Standing Committee I decided to wait with the investigation. However, since no other complainants came forward, the Committee opened its investigation on 8 February 2012. It was finalised in mid-2012.

55 The complainant wished for his identity to be protected under Article 40, last paragraph of the Review Act.

56 Articles 99–112 of the Royal Decree of 19 November 1998 on authorisations and leave granted to government department staff and Circular no. 476 of 28 May 1999 of the Minister of the Civil Service (*Belgian Official Journal* 17 June 1999). The circular states, for example, that '*The Minister of the Civil Service […] will only be able to recognise the public interest nature of the assignment if the Minister to whom the official has to report demonstrates the interest that the country, government or administration has in the performance of the assignment*'(free translation).

57 Articles 184 and 187 of the Royal Decree of 13 December 2006 on the status of the officials of State Security's external services, and State Security's service memoranda of 20 February 2007 and 7 December 2007. These service memoranda state, among other things, that *'there*

granting of this authorisation is sometimes a right, in other cases it is favour where prior 'permission' is required or by which the assignment is 'entrusted'. The criteria within which the competent authority can or cannot grant authorisation, were – certainly as far as external services are concerned – described quite precisely.[58]

Despite the difference in the elucidation of the rules relating to internal services and external services, the Standing Committee I pointed out that the policy pursued in relation to granting authorisation for assignments was based on the same principle for both groups of personnel and thus followed the same rules and philosophy. The procedure for processing leave requests was also identical for both groups, on the understanding that an additional opinion was issued for external services – in addition to the opinion of the HR Service – by the Director of Operations. When issuing opinions, the impact of the assignment on operations of the service where the applicant is employed was taken into account along with the issue of public interest and added value for the service. Furthermore, contract staff could not replace employees who were absent from external services. The impact of absenteeism on the implementation of special intelligence methods was another factor that was taken into consideration.

From 2007 to 2012, 27 people submitted an application for leave in respect of positions within the EU, NATO, UN, OSCE, European Defence Agency and International Criminal Court.[59] It involved a total of three candidates for two assignments within internal services. Two employees were granted the requested leave. In external services, 24 people requested leave for 16 different positions.

Although the Committee had to conclude that the number of State Security personnel that carried out an authorisation for an assignment was relatively higher than in the other federal public services, this still only involved less than 1% of the total workforce. In this way, these employees are given a unique experience to gain useful international experience and expand their networks, which can be an asset for both the employee concerned and State Security. In the Committee's opinion, the existence of such added value is correctly taken into

---

must be a public interest that is adequately demonstrated and that there is also an interest/added value for the service that must be demonstrated'. It is further stated that '*every file [will be] assessed on an ad hoc basis and placed in light of the situation that applies at that moment within State Security, and the consequences of granting authorisation for a public interest assignment on the organisation of State Security's services will be evaluated. This means that the personnel situation within the section/special unit to which the employee belongs and the position held by the employee will be taken into account, among other things*'(free translation).

58 In its ruling of 24 April 2012 (Zinzen, no. 219.010), the Council of State held that the criteria applied by State Security did suffice to decide whether or not to grant authorisation for assignments in the public interest.

59 There are also positions to which State Security employees can be seconded. Examples include Europol, CUTA and the Investigation Service of the Standing Committee I. In all these cases, the person involved continues to be paid by State Security (with possible recovery from the service where he or she is actually employed), while in case of authorisation for an assignment in the public interest, the salaries are paid by the service employing the individual.

consideration when assessing applications for an assignment (or for its extension).

The Committee lastly concluded that State Security processed the applications for authorisation for an assignment in a lawful manner: the criteria applied were established beforehand, the decisions were adequately justified and there were no indications that applications were processed in a discriminatory manner. It ought to be noted, however, that a number of people whose applications (or the extension thereof) were rejected ended up leaving the service. This phenomenon, which was also influenced by a number of external factors – such as the difference in salary between State Security and certain international institutions – was, however, very limited and not problematic in that sense.

II.7. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2012 AND INVESTIGATIONS OPENED IN 2012

This section contains a list and brief description of all investigations opened in 2012 and those investigations that were continued during the operating year 2012 but which have not been completed as yet.

II.7.1. INVESTIGATION WITH REGARD TO THE ACTIVITIES OF GISS IN AFGHANISTAN

In December 2001, Belgium decided to join the ISAF (International Security Assistance Force) in Afghanistan. Belgian service personnel have since been based at the airport of the capital Kabul and in the Northern Afghan province of Kunduz. Belgian F-16 fighter planes have been operating out of Kandahar since 2008.[60]

A briefing of GISS regarding the situation on the ground revealed that the service had applied several intelligence methods (HUMINT, OSINT, IMINT, SIGINT, etc.) and worked closely together with intelligence services of other countries. In order to obtain a complete picture of the situation, the Committee decided to open an investigation into '*the role of GISS in monitoring the situation in Afghanistan*'. This investigation included topics such as the personnel

[60] At the end of 2011, the Belgian government decided to begin the withdrawal of Belgian troops from 2012. The 'security mission' of international troops in Afghanistan will be concluded by the end of 2014. NATO plans a follow-up mission that will focus on training and assistance in rebuilding the country from 2015. Belgium's possible contribution to this mission is as yet undecided.

deployed, intelligence methods used, cooperation with foreign intelligence services as well as the transmission of intelligence.

The Standing Committee I will finalise this supervisory investigation in mid-2013.

II.7.2. ASSESSMENT OF THE MANNER IN WHICH STATE SECURITY PERCEIVES ITS ROLE WITH REGARD TO THE FIGHT AGAINST PROLIFERATION AND THE PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL

The Standing Committee I has already conducted various investigations into the manner in which the intelligence services carry out the fight against proliferation[61] and the protection of the scientific and economic potential (SEP).[62] In both these matters, State Security has an extremely important role to play with respect to the various public services. But the intelligence provided by State Security or the manner in which this intelligence information is used can lead to adverse consequences for legal or natural persons. Moreover, the interests in the fight against proliferation and those related to the protection of the SEP do not necessarily coincide. In this investigation, the Standing Committee I seeks to determine, on the basis of an actual case, whether State Security has worked meticulously in this context. The chosen cases offer the opportunity to carry out an assessment that covers a fairly long period.

Various investigative steps were taken during this supervisory investigation in 2012 (briefings by the intelligence services, company visit, interview with the relevant experts, etc.).

II.7.3. ALLEGED CRIMINAL OFFENCES BY A FOREIGN INTELLIGENCE SERVICE AND STATE SECURITY'S INFORMATION POSITION

At the beginning of December 2011, the Standing Committee I was advised of a complaint including a civil claim for damages before the examining magistrate. The complaint involved the offences of abduction, unlawful detention, assault and battery committed in the Netherlands and Belgium and attributed to intelligence agents of a foreign power.

---

61 See, for example, STANDING COMMITTEE I, *Activiteitenverslag 2005* (Activity Report 2005), 8–27; *Activiteitenverslag 2008* (Activity Report 2008), 42–57 and *Activiteitenverslag 2011* (Activity Report 2011), 37–40.

62 See, for example STANDING COMMITTEE I, *Activiteitenverslag 2005* (Activity Report 2005), 67 and 98–145 and *Activiteitenverslag 2008* (Activity Report 2008), 60–66.

Although it does not have the legal authority to supervise foreign intelligence services, the Committee deemed it appropriate to investigate State Security's information position. After all, the reported offences did allegedly partly take place on Belgian territory.

The supervisory investigation was completed by the beginning of 2013.

II.7.4. MONITORING EXTREMIST ELEMENTS IN THE ARMY

As a result of briefings given by GISS, the Standing Committee I took note of the problem of service personnel moving within extremist circles and service personnel 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 Ardense Jagers Battalion, who apparently drew up combat manuals with the experience gained there. The Committee therefore decided to open an investigation into '*the monitoring by GISS of extremist service personnel within the Armed Forces*' (free translation). The investigation wishes to examine whether GISS is tackling this problem efficiently and also respecting citizens' rights in this regard.

The investigation will be completed during the course of 2013.

II.7.5. HOW THE SPECIAL FUNDS ARE MANAGED, USED AND AUDITED

Two judicial inquiries had previously been opened into the possible misuse of funds intended for the payment of informants. The Investigation Service I was engaged for this purpose. 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 thematic investigation into '*the manner of managing, spending and auditing funds intended for the payment of State Security and GISS informants*' (free translation).

In view of the current criminal investigations, the supervisory investigation was suspended until further notice.

II.7.6. STATE SECURITY AND ITS CLOSE PROTECTION ASSIGNMENTS

Within the framework of the '*joint investigation into CUTA's threat assessments relating to foreign VIP visits to Belgium*' (free translation) (*supra*, II.5), it had to be concluded that there were problems with State Security's availability to carry

out certain close protection assignments. State Security gave the compelling reasons of being overburdened and a lack of resources as the justification for this on several occasions.

The Standing Committee I then decided to open an investigation to examine whether State Security was performing its close protection activities in accordance with the law and/or whether it was working efficiently in this regard.

The investigation is in its final phase.

II.7.7. POSSIBLE REPUTATIONAL DAMAGE BECAUSE OF STATEMENTS MADE BY STATE SECURITY

In July 2012, the Standing Committee I received a complaint about State Security from a private individual. The complainant carried out professional activities in the economic information gathering sector and alleged that State Security had smeared his reputation. This situation purportedly had harmful consequences for his professional relationships.

On 19 September 2012, the Standing Committee I opened an investigation '*into the information that State Security may have disclosed about a private individual*'(free translation). The investigation was completed in April 2013.

II.7.8. JOINT SUPERVISORY 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 introduced at CUTA for the purpose of '*structurally gathering intelligence on entities that are monitored as part of the Radicalism Action Plan*' (free translation).

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).

II.7.9. INTELLIGENCE AGENTS AND SOCIAL MEDIA

At the end of November 2012, the media reported on the profiles of intelligence service employees on social networking sites such as Facebook and LinkedIn. The Monitoring Committee of the Senate then requested that the Standing

Committee I open a supervisory 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. A joint supervisory investigation was opened with the Standing Committee P as regards CUTA employees at the start of 2013.

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS

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 methods for intelligence gathering, as referred to in Article 18, 2° of the Intelligence and Security Services Act of 30 November 1998 [and] to the application of Chapter IV(2) of the same Act*'.[63] 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 on behalf of the Monitoring Committee of the Senate.[64, 65]

III.1. FIGURES WITH REGARD TO THE SPECIFIC AND EXCEPTIONAL METHODS

Between 1 January and 31 December 2012, the two intelligence services combined granted 848 authorisations for the use of special intelligence methods: 757 by State Security (of which 655 were specific and 102 exceptional) and 91 by GISS (of which 67 were specific and 24 exceptional).

The following table draws a comparison with the figures of 2011, being the first full year in which the special intelligence methods could be used.

---

63 For an analysis on the special intelligence methods and on the manner in which they are monitored, please refer to: STANDING COMMITTEE I, *Activiteitenverslag 2010* (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.

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

65 On the presentation of its '*Report on the application of specific and exceptional methods by the intelligence and security services and the monitoring thereof by the Standing Committee I (1 January to 31 December 2011)*'(free translation), the Committee was asked by the Monitoring Committee to prepare two legislative bills for the amendment of the Special Intelligence Methods (SIM) Act. This related firstly to amending the arrangement for identifying users of certain means of communications as a specific method and secondly to amending the emergency procedure for specific and exceptional methods.

	GISS		State Security		TOTAL
	Specific method	**Exceptional method**	**Specific method**	**Exceptional method**	
2011	60	7	731	33	831
2012	67	24	655	102	848

Apart from the qualification that will be made later in this report (see III.1.2.1), the number of methods used has remained quite stable. What is striking, however, is the shift to greater use of exceptional methods: these increased more than threefold in 2012 compared with the previous year for both services.

Three major categories are distinguished for each service below: figures on specific methods, figures on exceptional methods and figures on threats and the interests to be defended that are envisaged by the methods.

III.1.1. AUTHORISATIONS WITH REGARD TO GISS

III.1.1.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2011	NUMBER 2012
Entry into and surveillance of or in places accessible to the public using a technical device	7	8
Entry into and searching of places accessible to the public using a technical device	0	0
Inspection of identification data of postal traffic and requesting the cooperation of a postal operator	0	0
Inspection of identification data of electronic communications, requesting the cooperation of an operator or direct access to data files	23	25
Inspection of call-associated data of electronic communications and requesting the cooperation of an operator	17	30
Inspection of localisation data of electronic communications and requesting the cooperation of an operator	13	4
TOTAL	**60**	**67**[66]

[66] In one case, the authorisation related to one of the protected professional categories, i.e. a lawyer, doctor or professional journalist.

III.1.1.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2011	NUMBER 2012
Entry into and surveillance in places not accessible to the public with or without a technical device	0	1
Entry into and searching of places not accessible to the public with or without a technical device	0	0
Setting up and using a fictitious legal person	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	0	0
Collecting data on bank accounts and banking transactions	5	7
Penetrating an IT system	0	2
Monitoring, intercepting and recording communications	2	14
TOTAL	**7**	**24**[67]

III.1.1.3. Interests and threats justifying the use of special methods[68]

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

- the intelligence task focused on threats against the inviolability of national territories, 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 task 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 2011	NUMBER 2012
Intelligence task	38	63
Military security	8	7
Protection of secrets	19	21

Unlike for State Security, the Act does not lay down which threats GISS may or must pay attention to. Despite this, the service systematically mentions the

67 In one case, the authorisation related to one of the protected professional categories, i.e. a lawyer, doctor or professional journalist.

68 Each authorisation may involve multiple interests and threats.

threat being targeted in its authorisations. Such transparency is to be recommended. The figures show in relation to the use of special methods, that the fight against espionage has remained the first priority of the military intelligence service.

NATURE OF THREAT	NUMBER 2011	NUMBER 2012
Espionage	54	78
Terrorism (and radicalisation process)	10	3
Extremism	3	3
Interference	0	2
Criminal organisation	0	1
Other	0	5

III.1.2. AUTHORISATIONS WITH REGARD TO STATE SECURITY

III.1.2.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2011	NUMBER 2012
Entry into and surveillance of or in places accessible to the public using a technical device	89	75
Entry into and searching of places accessible to the public using a technical device	0	1
Inspection of identification data of postal traffic and requesting the cooperation of a postal operator	4	2
Inspection of identification data of electronic communications, requesting the cooperation of an operator or direct access to data files	355	254
Inspection of call-associated data of electronic communications and requesting the cooperation of an operator	237	147
Inspection of localisation data of electronic communications and requesting the cooperation of an operator	46	176
TOTAL	**731**	**655**[69]

[69] In seventeen cases, the authorisation related to a protected professional category, namely that of a lawyer, doctor or professional journalist. Last year there were nine cases.

The comparison with 2011 for specific methods used by State Security reveals three significant figures: the number of 'Inspections of identification data' and 'Inspections of call-associated data' decreased significantly, while the number of 'Inspections of localisation data' rose sharply. A partial explanation for this may be found in how State Security has responded to a specific decision of the Standing Committee I. The jurisdictional body namely established that State Security had obtained unsolicited localisation data when it requested call-associated or identification data. Since requesting localisation data is a distinctive method, the Committee called for stopping this practice. In all probability, State Security then explicitly requested localisation data because it could produce interesting information.

Another element that warrants attention has to do with the count used. After all, 274 identifications of call-associated data were not included in the count because they were included in the authorisation for 'Inspections of call-associated data'. Last year there were only 116. By taking these figures into account, there is no longer any decrease, but rather an increase, in the number of 'Inspections of identification data'.

III.1.2.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2011	NUMBER 2012
Entry into and surveillance in places not accessible to the public with or without a technical device	2	8
Entry into and searching of places not accessible to the public with or without a technical device	3	6
Setting up and using a fictitious legal person	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	4	12
Collecting data on bank accounts and banking transactions	10	16
Penetrating an IT system	3	10
Monitoring, intercepting and recording communications	11	50
TOTAL	**33**	**102**[70]

The figures – just as for GISS – show a significant increase in the number of tapping measures: 50 in 2012 compared with 11 in 2011. However, the other exceptional measures were also authorised more frequently.

For the first time, the competent minister granted two authorisations because the SIM Commission was unable to convene (also see III.2.2.1).

[70] In five cases, the authorisation related to a protected professional category, namely that of a lawyer, doctor or professional journalist.

III.1.2.3. Interests and threats justifying the use of special methods[71]

State Security may only take action in order to safeguard the following interests:

- the internal security of the State and maintenance of democratic and constitutional order;
- the external security of the State and international relations;
- safeguarding of the key elements of the scientific or economic potential.

NATURE OF INTEREST	NUMBER 2011	NUMBER 2012
Internal security of the State and maintenance of democratic and constitutional order	694	704
External security of the State and international relations	571	693
Safeguarding of the key elements of the scientific or economic potential	24	15

The following table provides an overview of the (potential) threats targeted by State Security when using 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 under its competence (Article 8 of the Intelligence Services Act). Exceptional methods may not be used in the context of extremism and interference. They are allowed, however, in the context of the radicalisation process that precedes terrorism (Article 3, 15° of the Intelligence Services Act).

NATURE OF THREAT	NUMBER 2011	NUMBER 2012
Espionage	193	243
Terrorism (and radicalisation process)	371	288
Extremism	319	177
Proliferation	17	28
Harmful sectarian organisations	4	7
Interference	3	10
Criminal organisations	3	5

These figures are significant in comparison with the count for 2011. As in the case of GISS, significantly fewer special intelligence methods were authorised not only in the fight against 'terrorism' but also against 'extremism'. In 2012, more attention was paid (at least as regards special intelligence methods) to the threat of 'espionage': an increase from 193 to 243.

71 Each authorisation may involve multiple interests and threats.

III.2. THE ACTIVITIES THE OF THE STANDING COMMITTEE I AS A JURISDICTIONAL BODY AND A PRE-JUDICIAL CONSULTING BODY

III.2.1. STATISTICS

A referral may be made in five ways to the Standing Committee I to deliver a decision on the legality of special intelligence methods (Article 43, 4° of the Intelligence Services Act).

- 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 whether or not it is legal to use intelligence acquired by means of specific or exceptional methods, in a criminal case. The decision to ask for the Committee's opinion rests with the examining courts or criminal court judges. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

METHOD OF REFERRAL	NUMBER 2011	NUMBER 2012
1. At its own initiative	13	19
2. Data Protection Commission	0	0
3. Complaint	0	0
4. Suspension by SIM Commission	15	17
5. Authorisation by Minister	0	2
6. Pre-judicial consulting body	0	0
TOTAL	**28**	**38**

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 formal 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 (43, 5°, §1, first to third paragraphs of the Intelligence Services Act);
5. Request for additional information from the relevant intelligence service (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). This section does not refer to the additional information that is often obtained by the Investigation Service I before the actual referral to the Committee and which is, therefore, obtained in a more informal way;
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 judge (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 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 (Article 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 the referral was made to it in this matter (Article 43, 4° of the Intelligence Services Act). This period was respected in all dossiers.

NATURE OF DECISION	2011	FINAL DECISION 2011	2012	FINAL DECISION 2012
1. Invalid complaint	0		0	
2. Manifestly unfounded complaint	1		0	
3. Suspension of method	3		1	
4. Additional information from SIM Commission	4		0	
5. Additional information from intelligence service	9		6	
6. Investigation assignment of the Investigation Service	17		11	
7. Hearing of SIM Commission members	0		0	
8. Hearing of intelligence service members	1		0	
9. Decision regarding investigative secrecy	0		0	
10. Sensitive information during hearing	0		0	
11. Discontinuation of method	12		4	
12. Partial discontinuation of method	7		18	
13. Lifting or partial lifting of ban imposed by SIM Commission	5	**39**	13	**38**
14. No competence	0		0	
15. Lawful authorisation / No discontinuation of method / Unfounded	15		3	
16. Pre-judicial advice	0		0	

Despite the fact that the number of the Committee's final decisions remained almost the same as last year, it is noteworthy that the scope of these decisions differs significantly. While fifteen decisions on the legality of the measures at issue were made in 2011, three times as many decisions were made in 2012. This is most likely because in the first year the Committee still handled certain files in order to take decisions in principle, even if the *prima facie* investigation did not reveal any legality issue; in 2012 the Committee no longer concerned itself with such files.

Another significant fact is that suspensions handed down by the SIM Commission were fully or partially reversed in thirteen cases; this measure was only applied five times in 2011. The higher figure is mainly because the Committee arrived at a different opinion to the SIM Commission in eight identical files (see III.2.2.1.1).

III.2.2. DECISIONS

The 38 final decisions delivered by the Standing Committee I in 2012 are briefly presented below. The summaries have been stripped of all operational information. Only the information that is relevant to the legal question has been included.[72]

The decisions have been grouped into five categories:

- Legal (procedural) requirements and other requirements prior to the implementation of a method;
- Justification for the authorisation;
- Proportionality and subsidiarity requirements;
- Legality of the method in terms of 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 sections.

III.2.2.1. Legal (procedural) requirements prior to the implementation of a method

No special method may be used without prior written authorisation from the head of service. Moreover, in case of an exceptional method, a draft authorisation as well as the assent of the SIM Commission must be presented. If such methods

[72] All decisions of the Committee in this matter are marked for 'limited dissemination' or classified as 'confidential'.

are used without written authorisation or assent, the Committee may obviously intervene.

III.2.2.1.1. Authorisation by the acting head of service

When the official designated by the head of service as his temporary substitute unexpectedly fell ill and was absent himself, another official signed various authorisations for specific methods *'On behalf of the Administrator-general, absent, on behalf of X, absent, Y'* (free translation) (files 2012/1266 to 2012/1273 inclusive). However, as Article 3, 8° of the Intelligence Services Act stipulates that the head of service, who must take responsibility for authorisations, will be replaced if he is unable to act by '*the acting Director-General*' (free translation) of State Security and '*the acting head*' (free translation) of GISS, this raised the question of whether this rule had been observed. The Committee found that the methods had been legitimate under the given circumstances because '*the principles of force majeure and of the continuity of the public service are applicable in this case*' (free translation).

III.2.2.1.2. Authorisation by the competent minister

Because of the holiday period and the fact that substitutes for the regular members had not yet been appointed, the SIM Commission decided to create one opportunity only for handling new files in both July and August. If the intelligence service concerned wishes to use an exceptional method in mid-July, it immediately invokes the procedure under Article 18, 10°, §3, third paragraph of the Intelligence Act (files 2012/1308 and 2012/1309). If the Commission does not issue an opinion within four days of receipt of the draft authorisation, this provision enables the intelligence service to request its minister to authorise the method. In view of the specific circumstances and the need for the service to be able to continue performing its legal assignments, the Committee had no objection to the immediate referral to the minister. The Standing Committee I also notes that Article 18, 10°, §3, third paragraph of the Intelligence Services Act only makes provision for ministerial authorisation '*without setting other requirements such as those provided for in Article 18, 10°, §1; That [the minister] has authorised the exceptional method by placing his signature on the decision*' (free translation). The minister did neglect to state in his authorisation the deadline by which the intelligence service had to report on the progress of the method in accordance with Article 18, 10°, §3, fourth paragraph of the Intelligence Services Act. However, the Committee held '*that this omission does not affect the legality of the decision or the authorisation granted by [the minister]*' (free translation).

III.2.2.1.3. Method not covered by authorisation

During the reference period, the Committee had to make four rulings on files in which an error or force majeure was the reason why the limits of the legal mandate were not observed in practice.

In the first file (2012/902), the head of service had authorised the surveillance of a building for a defined period. The surveillance device was set up at the premises of a person who had cooperated for this purpose. However, the device could not be removed on time due to that person's absence. For a number of days, 'observations' were therefore made beyond the service's control that were not covered by the authorisation. The head of service told the SIM Commission of his own accord that these images had been deleted as soon as the device could be removed. The SIM Commission decided to partially suspend the method, namely in relation to the part that fell outside the scope of the original authorisation. The Committee upheld this decision.

In the second file (2012/1058), the head of service wished to trace the call-associated data of a specific target's mobile phone. The intelligence service demanded the cooperation of another agency to implement the method. Due to an administrative error, however, that agency started telephone tapping. When the error was discovered the next day, the intelligence service immediately requested the discontinuation of the method. The agency involved then deleted all the stored data. The Committee held that '*the communications intercepted in this manner, even though they were not shared [with the intelligence service] and, according to the written report [of the agency concerned], were deleted immediately after the error was established, were obviously obtained unlawfully in the absence of a valid decision*'(free translation). After all, telephone tapping is an exceptional method for which there was no valid decision.

An intelligence service was authorised to monitor two mobile phones for two months (file 2012/1136). The service discovered a material error already on the second day: one of the two intercepted numbers was not the number listed in the authorisation. The head of service ordered immediate discontinuation. He notified the Commission of this, which in turn ordered partial suspension. The Committee acknowledged the material error and likewise ordered partial suspension of the method.

In the last file (2012/1435), the head of service discovered as a result of a legally permitted tapping measure that some information that had been obtained did not relate to the target. This was due to incorrect manipulation by the operator concerned. The SIM Commission partially suspended the method and imposed a ban on using that data. The Standing Committee I confirmed the ban on the use of the data and ordered the destruction of the data concerned but lifted the Commission's ban '*given that the head of service's decision was lawful; that the reason for the legality issue is an error, not of the [intelligence service] but*

of the operator concerned, the method therefore should not be suspended' (free translation).

III.2.2.1.4. An exceptional method without prior authorisation

An intelligence agent had brief access to a digital data carrier. He made immediate use of this opportunity to copy the data before replacing the carrier. However, this amounted to an exceptional method under Article 18, 16°, §1, 1 to 4 of the Intelligence Services Act and thus required prior authorisation. Such authorisation was never granted (file 2012/1371). The head of service relied on the legal concept of emergency for this purpose. He held the view that the legal provisions could not be materially observed within the short period of time that his service had available to it. However, the Committee held that '*the legal concept of force majeure, described erroneously in this case as an emergency, cannot be supported. The legislature emphatically made the most invasive intelligence gathering methods dependent on observing very strict and clearly described conditions, and likewise in the explicit case of extreme urgency. It is accordingly up to the intelligence services to make the necessary arrangements and show the necessary flexibility and innovativeness to be able to operate legally within reasonably foreseeable situations, also and even a fortiori if urgency arises. […] The Standing Committee I is not at all convinced that if these communication devices had been efficiently used, anticipatory scenarios had been available and efforts had been adequately coordinated, it would have been completely impossible to reasonably obtain written authorisation and an assent on time in the specific case [of the method*' (free translation). The Standing Committee I also noted that the head of service neglected to suspend the method and notify the SIM Commission as soon as he discovered the illegality.

III.2.2.1.5. Prior notice to the SIM Commission

A specific method may be used only after notice of the reasoned decision by the head of service is given to the SIM Commission. As the intelligence service concerned had already started to use the method before notice was given, it was decided to partially declare it null and void: after all, the data that was gathered before notice was actually given to the Commission was obtained illegally (file 2012/1662).

III.2.2.2. Justification for the authorisation

III.2.2.2.1. No justification

The head of service took the decision in seven files (2012/1289, 2012/1290, 2012/1293, 2012/1296, 2012/1299, 2012/1300 and 2012/1310) to trace the call-

associated data of mobile phone numbers, to identify the holders of the numbers obtained and to identify the location of all these people. In other words, this involved three separate methods. However, the use of specific methods requires a prior, written and reasoned decision of the head of service. Since '*this provision is not a mere formality, given that it serves to guarantee that the legality of the decision, including the subsidiarity and proportionality of the method to be used, can be verified*'(free translation), the Committee decided to partially discontinue the seven methods because '*no justification at all*' was given in the decisions for the localisation.

III.2.2.2.2. Insufficient justification

The intelligence service concerned wished to trace the incoming and outgoing call-associated data of the communication device of a person who was the 'probable pawn' of a third party, who – despite the fact that he had already been under surveillance for a long period – 'probably' performed intelligence activities, without any concrete evidence of this having being produced (dossier 2011/841). As is the case for every specific method, a potential threat must exist (Article 18, 3°, §1 of the Intelligence Services Act), '*which must be reflected in the decision, given that this must be reasoned*'(free translation). This condition was not satisfied in this file.

The Committee arrived at the same conclusion in file 2011/843. The head of service had formulated '*a mere hypothesis*' in the authorisation '*as well as a truism that can apply to anyone [similar professional]*'. '*According to the Intelligence Services Act, however, there needs to be more, i.e. reasoned potential. In other words, it must be demonstrated that any threat is not a mere figment of the imagination. Evidence must also be produced to reasonably support this possibility*' (free translation). As neither the decision nor the additional information obtained by the Standing Committee I provided any indications that could or would have served as *prima facie* evidence of the assumptions, the method was discontinued.

In two other files (2012/1039 and 2012/1040), the SIM Commission proceeded with suspension on the basis of the file and additional information '*because the seriousness of the potential threat is not sufficiently evident from the file, and it is not clear what threat the target represents and the letter does not provide the requested adequate information*' (free translation). In spite of this, the Committee still asked for additional information from the service concerned. It is certainly clear from this that it '*this is not about a simple lobbying activity; the purpose of the method is to establish whether the target is trying to recruit agents for a foreign intelligence service, as his contacts seem to indicate*' (free translation). As there was definitely a potential threat with regard to the target, the suspension was lifted.

III.2.2.2.3. Ambiguity in the justification

An intelligence service wished to proceed with the surveillance of one person and various locations (files 2011/855). Although the person was not identified, he or she was adequately identifiable. The Committee thus saw no objection to the legality of this method. The surveillance of the entrance of a location known to be that of the extremist movement to which the target belonged, was also not a problem. However, this was not the case with the authorisation to carry out surveillance of the entrance door to the target's domicile, as soon as the address could be established, or the places that he frequented. In the absence of any specific address, the Committee could not determine whether this related to observation of/in private places that were accessible to the public, or to observation in private places that were not accessible to the public (for instance if the location to be observed was in a fenced compound). The latter is an exceptional and not a specific method. As the conditions for using an exceptional method were not satisfied, the authorisation at this level was substantively ambiguous and held to be illegal in this respect.

In another file (2012/1371), an intelligence service wished to inspect computerised data. Since this constitutes an exceptional method, '*the threats, as described in more detail in Article 18, 9° of the Intelligence Services Act, must be of a serious nature*'(free translation). Standing Committee I held that the supposed seriousness of the threat was incompatible with the finding that the service waited 15 days to read the data.

III.2.2.2.4. Enhanced justification for a second extension

Article 18, 10°, §5 of the Intelligence Services Act stipulates that any second and subsequent extension of an exceptional method is possible only if special circumstances necessitate that extension. These special reasons must also be included in the decision itself.

In one file (2012/1230), although the authorisation for the second extension to inspect banking data did refer to the reasons – supported by the Standing Committee I – that justified the use of the method, the special circumstances were hardly explained at all. The reason for the authorisation was almost identical to that of the previous two authorisations. It was evident from an additional investigation that the Standing Committee I carried out pursuant to Article 43, 5° of the Intelligence Services Act that the special circumstances required by law did actually exist and were adequate. The Committee therefore held that '*although the authorisation is valid, its formal compliance with the provisions of Article 18, 10°, §5 of the Intelligence Services Act is very rudimentary. It is therefore preferable to ensure that* all *the special circumstances are included in the decision* ab initio *and do not have to be ascertained only because of intervention by the Standing Committee I*' (free translation).

III.2.2.3. Proportionality and subsidiarity requirements

The Committee ruled four times on whether a permitted method was proportionate to the seriousness of the threat (proportionality) and whether the aim of the method could not have been achieved in a less invasive manner (subsidiarity).

The head of service of an intelligence service granted authorisation for the identification of the communication devices that a person was using (file 2012/1040). There was nothing wrong with that (see III.2.2.2.2 above). However, in the same decision, he also immediately authorised the use of two other methods that were dependent on the results of the first method. The Committee nevertheless held that '*in view of the lack of information obtained by the requested method, namely "the identification of the electronic communication devices on which a specific person is subscribed or that are usually used by a specific person" (Article 18, 7°, §1, 2 of the Intelligence Services Act), it is not possible to rule on compliance with the principles of subsidiarity and proportionality and thus on the legality of the other two requested methods, namely those referred to in Articles 18, 7°, §1, 1 and 18, 8° §1, 1 of the Intelligence Services Act*' (free translation).

The file in which an intelligence service wished to proceed with the surveillance of one person and several locations (file 2011/855) has already been cited above (see III.2.2.2.3). The Committee sanctioned this method in respect of the surveillance of the entrance door to the target's domicile and of all the places that he frequented because, in the absence of any specific address, it could not be determined whether this amounted to specific or exceptional surveillance. The Committee moreover stated that '*the decision likewise does not adequately demonstrate the subsidiarity and proportionality of the method in relation to the unknown locations given that the nature and number of these locations have not been determined at all*' (free translation).

In two files, subsidiarity was the sole problem at issue (files 2012/903 and 2012/904). An intelligence service proceeded to identify a list of landline and mobile telephone numbers. This is a specific method. However, Article 18, 3°, §1 of the Intelligence Services Act stipulates that a specific method can be used only if ordinary methods are deemed inadequate to gather the relevant intelligence. The Committee ruled that some of the landline numbers could be identified by an ordinary method, namely with reference to Belgacom's public 1207 service. The authorisation was therefore illegal as far as the landline (and not the mobile) telephone numbers was concerned.

III.2.2.4. Legality of the method in terms of techniques applied, data collected, duration of the measure and nature of the threat

The intelligence services obviously cannot just apply any method or technique: these must be provided for by law, are sometimes subject to time limits, cannot

always be used for every threat, may not be used outside Belgium, etc. The Standing Committee I has explained these restrictions in some decisions.

III.2.2.4.1. Maximum legal term of a method

The law stipulates that the exceptional method to search private places may not last longer than five days (Article 18, 12°, §1, second paragraph of the Intelligence Services Act). However, authorisation granted by a head of service permitted a search to last for six days (file 2012/972). The Committee decided '*the exceptional method was therefore unlawful for […] the sixth day*' (free translation).

III.2.2.4.2. Legal options and restrictions for third parties that cooperate in the implementation of exceptional methods

In two files (2012/1455 and 2012/1491), an intelligence service wished to proceed with the localisation of a mobile phone. It also requested the possible cooperation of a certain public service. However, the technique used by this public service meant that metadata to and from the mobile phone – or, in other words, signals that must be regarded as communication within the meaning of the Electronic Communication Act of 13 June 2005 – was also intercepted.

The Committee noted that State Security has the power to capture mobile phone signals and can request the cooperation of an electronic communication network operator or an electronic communication service provider for this purpose. However, the specific public service that was requested in this instance did not comply with that qualification. The service in question was also subject to a criminally sanctioned ban on inspecting the existence of communication without the consent of all concerned (Article 124 and 145 of the Act of 13 June 2005). None of the exceptions as set out in Article 125 of this Act applied to it: '*Whereas the exceptions as set out in Article 125 do not provide for requests or claims by [an intelligence service], but this article does explicitly provide for this in relation to the examining magistrate*' (free translation). The Committee therefore held that this method was unlawful to the extent that it provided for any cooperation with the service in question.

The question at issue in another file was the extent to which provision may be made for third-party cooperation (file 2012/1683). The intelligence service concerned wished to search a home. The authorisation stated that this would happen in cooperation with an unnamed member of a specified foreign intelligence service. The Commission made the following decision in principle in this regard: '*Whereas Article 15 of the Constitution nevertheless guarantees the sanctity of the home to the extent that searches may not take place other than in the cases provided for in the Act and in the prescribed form. Whereas the Special Intelligence Methods Act in general and,* in casu*, Article 18, 12° of the Intelligence Services Act, in particular, expressly limit the head of service's right of*

authorisation to the intelligence services. Whereas in accordance with Article 2 of the same Act, these services are only State Security and GISS. That moreover where Article 18, 10°, §2, 6 of the Intelligence Services Act stipulates that the authorisation for exceptional methods must include the name and capacity of the intelligence officers appointed to implement the exceptional method for intelligence gathering, who may in turn arrange to be assisted by members of their service, it is clear that only Belgian intelligence officers and agents may use a method. Whereas in case of any necessary help and assistance, which is not evident in casu *from the authorisation, by a person outside of the service in a criminally sanctioned violation of the home (Article 439 et seq. of the Criminal Code), the procedure laid down in Article 13, 2°, §2, paragraphs 3 and 5 of the Intelligence Services Act must be followed,* in casu quod non. *Whereas there is accordingly no legal basis for the cooperation that is currently authorised with a person outside of the service*' (free translation).

III.2.2.4.3. The use of a non-compliant tactic in a lawful method

The intelligence service obtained authorisation to carry out surveillance in a private place that was not accessible to the public (files 2012/907 and 2012/912). However, when the head of service learnt that a non-compliant tactic was also being used for the purpose of the most efficient possible use of the methods, he suspended the method and notified the SIM Commission of this. The Commission confirmed the suspension. This was because the '*the tactic in question seems to fall under a criminal qualification, albeit of an administrative-technical nature. As this is not an infringement of the Road Code of 1 December 1975, it is therefore only permitted with the prior and explicit authorisation of the SIM Commission. Such permission was not present in this case*' (free translation). The Committee therefore decided that the head of service had correctly applied Article 18, 10°, §5, first paragraph of the Intelligence Services Act that obliges him to suspend an exceptional method if he establishes any unlawfulness. What then had to happen with the gathered intelligence is discussed below (see III.2.2.5).

III.2.2.5. The consequences of an unlawful method or an unlawfully implemented method

Article 43, 6° of the Intelligence Services Act stipulates that the Committee, if it establishes the unlawfulness of decisions relating to specific or exceptional methods, must order the discontinuation of the method concerned if it is still being implemented or, if it has already been suspended by the Commission, it must also order a ban on using the data and the destruction of the data obtained in that way. The Commission delved deeper into the consequences of an unlawful method in a number of decisions.

In the first case (file 2012/902), the head of service had authorised the surveillance of a building for a defined period (also see III.2.2.1.3). The surveillance device could not be removed on time due to the absence of the occupant of the building. For a number of days, further observations were therefore made with the device that were beyond the service's control and not covered by the authorisation. The head of service told the SIM Commission of his own accord that the service had immediately deleted these images. The SIM Commission ordered the partial suspension of the method and the matter was thus referred to the Standing Committee I. The Committee also ruled that the method was unlawful from the end of the original mandate and ordered the destruction of the data gathered as from that date.

In two identical cases (files 2012/907 and 2012/912), the question was what should happen to data that was obtained as a result of a method that was lawful in itself but by means of a tactic that, strictly speaking, was not permitted (see III.2.2.4.3). In view of the precedent value of the decision, the recitals are cited in full below: '*Whereas the question arises, however, to what extent the incompatibility of an aspect of a means of implementation with the rules of the Intelligence Services Act may also affect the lawfulness of the data obtained through duly authorised surveillance. Whereas the data in this case has not been obtained by means of the violation. That this was also not in any way decisive for that purpose. That the offence lay simply in one of the chosen methods of shielding, having been chosen as the most efficient method. That the significance of the envisaged threat and of the gathered data moreover far outweighs the seriousness of the administrative and technical irregularity, that the violation had no repercussions on the reliability of the gathered intelligence, and that the tactic used could also be an additional violation of fundamental rights – such as the right to privacy – of the people targeted by the method concerned. Whereas a distinction also ought to be made here between the possible criminal offence that is committed as a result, which its own punishment, and the punishment of the method itself. Whereas the Standing Committee I is of the opinion that data actually being obtained is not unlawful per se. That the unlawful practical means of implementing the method obviously must or should have been ended'* (free translation).

In another case (file 2012/1371), the question was whether a method that builds on illegally obtained data can itself be authorised. The intelligence service in question wished, namely, to read the data on a data carrier. However, that data had been unlawfully copied (see III.2.2.1.4). The Standing Committee I held that the method that '*aims to inspect and exploit data obtained illegally by the [intelligence service], […] compromises the Intelligence Services Act. After all, Article 43, 6°, §1 of the Intelligence Services Act provides for the destruction of that data*' (free translation).

Another question relating to the possible destruction of data arose in file 2012/1435. The Committee reached the conclusion that the method was

completely legal but due to an error without the intelligence service concerned knowing it, the operator gathered incorrect data (see III.2.2.1.3). The Committee then banned the use of this data and it had to be destroyed.

The intelligence service wanted to search a place in file 2012/1683 in cooperation with a member of a foreign intelligence service. The Committee held that this procedure was inconsistent with the Act (see III.2.2.4.2). It nevertheless did not order the destruction of all the gathered data. Only '*the data obtained and that may still be obtained pertaining to the part of the decision that declares it unlawful, […] may [not] be used and must be destroyed*' (free translation).

III.3. CONCLUSIONS

The following conclusions may be formulated with regard to operating year 2012:

- The number of methods used remained more or less stable in relation to 2011. The conclusion that the Committee formulated last year can therefore be repeated: the intelligence services are applying the opportunities to use special intelligence methods in a balanced manner.
- There is a notable shift, however, towards more exceptional methods for both services. This increase is largely due to the fact that there has been more of an emphasis on monitoring communication.
- A significant number of the authorisations granted in 2012 for using exceptional methods related to the extension of a previously authorised method. In practice, this means that the same target will often be followed far longer than the initial maximum legal period of two months.
- For GISS, the fight against 'espionage' remains the one that requires the most special methods. Attention to this threat (at least as far as special intelligence methods are concerned) is also increasing within State Security. On the other hand, both services authorised fewer methods in the fight against terrorism.
- For the first time, the competent minister granted two authorisations because the SIM Commission was unable to convene.
- 24 specific and exceptional methods were used in relation to a lawyer, doctor or professional journalist. As several such methods can be applied to one person, this figure says nothing about the number of professionals targeted by an special intelligence method.
- Despite the fact that the number of the Committee's final decisions remained almost the same as last year, they differ in scope. While fifteen decisions on the legality of the measures at issue were made in 2011, three times as many decisions were made in 2012. This is because in the first year the Committee still handled files to be able to make decisions in principle, even if the *prima facie* investigation did not reveal any legality issue. It therefore certainly

should not be inferred from this figure that the intelligence services took a harsher approach. The number of fully or partially discontinued methods remained almost the same and the majority of the cases involved the failure to comply with formalities.

CHAPTER IX
RECOMMENDATIONS

Based on the investigations concluded in 2012, the Standing Committee I has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred on 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. REVIEW OF THE ACTIVITIES OF FOREIGN INTELLIGENCE SERVICES[73]

The Committee also repeated its support in 2012 for the Senate's recommendation to include a specific power in the Intelligence and Security Services Act of 30 November 1998 for State Security and GISS to monitor the lawfulness of activities of foreign intelligence services on Belgian territory.[74]

---

73 This recommendation stems from investigations into 'Monitoring of foreign intelligence services in relation to their diaspora in Belgium' and 'Possible monitoring of an individual during and after detention in Belgium' (see II.2 and II.3).

74 STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 132 and *Activiteitenverslag 2008* (Activity Report 2008), 2. In a response to this recommendation, the Minister of Defence supported a legislative initiative that would enable the lawfulness of activities of foreign intelligence services on Belgian territory to be monitored.

IX.1.2. NOTIFYING INDIVIDUALS WHO ARE THE SUBJECT OF A THREAT[75]

Article 19 of the Intelligence Services Act gives State Security and GISS the opportunity to notify not only agencies but also individuals that are the subject of a threat. The Committee recommends that both intelligence services work out the criteria for the application of this provision by the end of 2013.

IX.1.3. UNIFORM CRITERIA FOR 'AUTHORISATION FOR ASSIGNMENTS'[76]

The Standing Committee I recommends drawing up a joint services memorandum for the personnel of State Security's internal and external services on granting authorisation for assignments, obviously within the possibilities of the regulatory framework. This can guarantee – at this level, at least – the most uniform human resource management possible within the service as a whole.

IX.1.4. A 'NEUTRAL OBSERVER' AT SECURITY INVESTIGATIONS

Except when classified information is being discussed, having a 'neutral observer' present at questioning as part of a security investigation is neither prohibited nor compulsory. The intelligence services can determine their own policy in this regard. That is the conclusion of the investigation into 'Trade union assistance during questioning arising from a security investigation'.[77] However, the Committee thinks it would be advisable for the Ministerial Committee for Intelligence and Security to issue an instruction in this regard that would apply to all security investigations, regardless of the service that conducts the investigation and the status of the individual being investigated.

---

75 This recommendation was formulated following the investigation into 'Monitoring of foreign intelligence services in relation to their diaspora in Belgium' (see II.2).

76 See the investigation into 'Handling of requests for 'authorisation for assignments' at State Security' (II.6).

77 See the investigation into the 'Trade union assistance during questioning arising from a security investigation' (II.4).

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

IX.2.1. INCREASED EFFICIENCY IN PROCESSING NATIONALITY APPLICATIONS[78]

Efficiency in processing files relating to nationality legislation could be increased at State Security's Security Verification Service by means of:

- central registration of all developments in a file;
- systematized quality control;
- uniform file compilation;
- wider use of ICT tools *in the broad sense*, ranging from extended access to the National Register to detailed computerisation of activities.

The following measures may contribute to increased efficiency at the Analysis Service and External Services:

- developing a methodical and formal file follow-up system in order to guarantee that time limits are observed (even though that is not currently a problem);
- establishing criteria that are decisive for sending a file to External Services for additional investigation;
- holding a debate with internal partners, external partners and clients on concrete substantive expectations relating to State Security's role.

Drawing up a consultation list of applications that have already been processed would also make it possible for a file to be permanently updated at each stage of the procedure.

The Committee believes that the implementation of these recommendations will be optimal only if work is also done in relation to factors that fall outside State Security's scope of competence. This means:

- integrating the ICT systems of the various parties so information can be shared more efficiently;[79]

---

78 This recommendation arises from the investigation into 'State Security's role in relation to the procedures for obtaining Belgian nationality' (see II.1).

79 The individual nature and needs of all parties involved must obviously also be taken into account. The security and classification issues of State Security, for example, must be

– determining the proper scope of State Security's 'advisory' mandate in relation to naturalisation files, with formalisation, if necessary, in a protocol with the Chamber of Representatives;
– a more detailed description of the concept 'obstacle due to important facts, specifically related to the person'.[80]

IX.2.2. ESTABLISHING AND FORMULATING ACHIEVABLE PRIORITIES[81]

The Committee recommends that both intelligence services establish the criteria in a directive that would enable them to decide what priority to give to 'monitoring the monitoring' by foreign intelligence services of their diaspora in Belgian territory.

As far as the 'espionage and interference' section from the priorities list of State Security's action plans is concerned, it should moreover be noted that the description of priorities is still too often vaguely formulated. Among other things, this means that it is difficult to indicate with certainty whether monitoring the intelligence activities of the various services in relation to their diaspora is or is not regarded a priority. The same comment applies to setting priorities from GISS's steering plans. It is recommended that this be explained and made explicit in future plans.

Around 150 problematic cases within the operational section of State Security's action plans are monitored as 'an active priority' and 'actively' each year. This has led to State Security concluding – in view of its human resources – that it is not possible to assign the necessary agents to each of these problem cases. GISS must also make choices in its steering plans based on limited resources. These choices are too often motivated by pragmatism and thus cannot be given sufficient objective justification. The Standing Committee I believes that action plans/steering plans should be drawn up on the basis of available human, budgetary and technical resources and in accordance with political policy choices. In other words, if there are insufficient *resources* available, the 'priorities list' must be pruned. Otherwise this list inevitably becomes an unachievable summary.

considered. The Committee therefore recommends that State Security should already take these plans into account as far as possible when developing its own procedures.

80 This recommendation has since been implemented.

81 This recommendation was formulated following the investigation into 'Monitoring of foreign intelligence services in relation to their diaspora in Belgium' (see II.2).

IX.2.3. DRAWING UP AND UPDATING PHENOMENON ANALYSES

In reference to structure and content, a document such as State Security's 'Phenomenon Analysis on Interference (December 2009)'[82] is a textbook case of an intelligence service's strategic product. With a view to business continuity, the recommendation is to draw up such documents in the medium term for as many threats or interests to be protected as possible, and to regularly update them. This recommendation is obviously addressed to both intelligence services.

IX.2.4. A MINISTERIAL DIRECTIVE FOR THE IMPLEMENTATION OF ARTICLE 20 OF THE INTELLIGENCE SERVICES ACT[83]

Article 20, §1 of the Intelligence and Security Services Act instructs intelligence and security services to ensure '*that there is cooperation with foreign intelligence and security services*' (free translation). The third section of the same provision instructs the Ministerial Committee for Intelligence and Security (MCI&S) to determine '*the conditions for the cooperation referred to in §1 of this article*' (free translation). In 2011, State Security drew up a detailed instruction on 'bilateral cooperation with correspondents'. Although the Standing Committee I regards this directive as very valuable, it points to the role that the legislature has entrusted to the Ministerial Committee in this regard. The Committee believes that certain options which State Security has included in its directive ought to be endorsed by the policy-makers. The Committee therefore repeats[84] its recommendation for the Ministerial Committee to issue such a directive, paying particular attention to the nature of the information that may be communicated to foreign services. It is recommended that State Security provides this directive to MCI&S.

In relation to GISS, the Standing Committee I recommends the speedy finalisation of the project that also aims to set evaluation criteria for determining how cooperation with foreign services can proceed. This document must also be sent to the Ministerial Committee.

---

82 See II.2.3.3.

83 This recommendation comes from the investigation into 'Monitoring of foreign intelligence services in relation to their diaspora in Belgium' (see II.2).

84 STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 132; *Activiteitenverslag 2007* (Activity Report 2007), 73; *Activiteitenverslag 2008* (Activity Report 2008), 6 and 109–110; *Activiteitenverslag 2009* (Activity Report 2009), 4 and 106–107; *Activiteitenverslag 2010* (Activity Report 2010), 3–4.

IX.2.5. AN AMENDMENT TO ARTICLE 18, 9° OF THE INTELLIGENCE AND SECURITY SERVICES ACT[85]

It ought to be noted in relation to the use of special intelligence methods that Article 18(9) of the Intelligence and Security Services Act does not include 'interference' in the list of threats for which State Security may employ exceptional methods. To the extent that a certain activity of a foreign intelligence service in Belgium can be classified only as 'interference', State Security cannot employ such methods. The Committee does not see any convincing arguments for this, especially since exceptional methods are subject to very tight administrative and jurisdictional control. It therefore recommends amending the Act in this respect.

IX.2.6. DOCUMENTED WORKING ARRANGEMENTS BETWEEN STATE SECURITY AND FPS FOREIGN AFFAIRS[86]

Despite the fact that FPS Foreign Affairs is regarded as State Security's most important client in relation to 'monitoring the monitoring of certain diaspora populations' and is moreover the designated service to assist State Security in countering activities of foreign intelligence services on Belgian territory, the lack of documented working arrangements between the two institutions is striking. The Standing Committee I insists on this.

IX.2.7. STANDARDISED METHODOLOGY AND UNIFORM TRAINING FOR AD HOC THREAT ASSESSMENTS

In the investigation into how CUTA draws up threat assessments for VIP visits to Belgium[87], the Standing Committees P and I had to conclude that these assessments are made informally and that even the experts do not receive standard training. This situation could become problematic for CUTA if there were an incident and it was called upon to explain its methodology. The Standing Committees P and I were therefore of the opinion that the expertise which is definitely present within CUTA is not a reason not to use a standardised methodology, taking into account ad hoc specifics. The Committees specifically recommended that CUTA work out a structured process (formal, substantiated

85 *Idem.*
86 *Idem.*
87 See II.5.

and auditable) for threat assessments for foreign VIP visits to Belgium, which would also ensure that experts receive uniform training. In a response to this recommendation, the Minister of Home Affairs advised that she would oversee CUTA's implementation of it.

IX.2.8. PROTOCOL AGREEMENT WITH THE IMMIGRATION OFFICE AND THE COMMISSIONER GENERAL FOR REFUGEES AND STATELESS PERSONS

As part of the investigation into 'Possible monitoring of an individual during and after detention in Belgium'[88], the Standing Committee I repeated its earlier recommendation for a protocol agreement to be concluded among State Security, the Immigration Office and the Commissioner General for Refugees and Stateless Persons.[89, 90] It also recommends that GISS enters into a protocol agreement with these services.

IX.2.9. PROTOCOL AGREEMENT WITH THE DIRECTORATE-GENERAL FOR THE EXECUTION OF PENALTIES AND DISCIPLINARY MEASURES

As part of the same investigation, the Committee recommended the rigorous application of all provisions of the protocol agreement that was concluded on 20 November 2006 between State Security and the Directorate-General for the Execution of Penalties and Disciplinary Measures. It was also recommended that GISS enter into such a protocol agreement.[91]

---

88 See II.3.

89 STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 134.

90 Such a protocol was already signed with the Immigration Office on 27 June 2011. However, State Security neglected to take the initiative to inform the Committee of this, as provided for in Article 33 of the Review Act.

91 The Minister of Defence informed the Committee that GISS took seriously the recommendation to enter into a protocol agreement with the Immigration Office and the Commissioner General for Refugees and Stateless Persons. However, GISS wondered whether a protocol with the Directorate-General for the Execution of Penalties and Disciplinary Measures would amount to a duplication of the agreement that State Security had signed under the 'Radicalism Action Plan'.

IX.3. RECOMMENDATIONS RELATED TO THE EFFECTIVENESS OF THE REVIEW

IX.3.1. CONTROL OF THE INTERNATIONAL EXCHANGE OF INFORMATION AND THE 'THIRD PARTY RULE'[92]

'In view of the growing globalisation of cooperation among intelligence and security services and the ensuing exchange of information, it is necessary to improve the parliamentary oversight of intelligence and security services.' That conclusion was reached by the 'International Conference of the Parliamentary Committees for the Oversight of Intelligence and Security Services of the European Union Member States, Norway and Switzerland'.[93] The Standing Committee I supports this position but is of the opinion that promoting a form of parliamentary oversight of international cooperation among intelligence services should not preclude an in-depth review of how the application of the 'third party rule' can be monitored.

IX.3.2. REASONED, SEARCHABLE AND VERIFIABLE DECISIONS[94]

The Committee is aware – in view of the clearly limited resources – that it is impossible for an intelligence service to monitor (equally closely) everyone that constitutes a potential threat. Choices therefore have to be made. An investigation has shown that State Security did not monitor a prisoner convicted of terrorism during and after his prison term and that no trace of a real assessment that resulted in a reasoned, searchable and verifiable decision could be found in that regard. The Committee pointed out that State Security has recently acknowledged the necessity of this itself in its '*Instruction for bilateral cooperation with correspondents*' (free translation). Under the heading '*Transparency and traceability*' there must be an '*administrative trail*' for every action, in view of an audit by the Standing Committee I, among other things. The Committee can but welcome such instructions.

---

92 This recommendation stems from the investigation into 'Monitoring of foreign intelligence services in relation to their diaspora in Belgium' (see II.2).

93 Seventh conference of the parliamentary committees for the oversight of intelligence and security services (Berlin, 27–28 October 2011). See STANDING COMMITTEE I, *Activiteitenverslag 2011* (Activity Report 2011), 84–85.

94 See 'Possible monitoring of an individual during and after their detention in Belgium' (II.3).

ACTIVITY REPORT 2013

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2013

PREFACE – ACTIVITY REPORT 2013

For the Standing Committee I, 2013 was dominated by two completely different events, each important in its own way.

The first was the twentieth year of its existence. After all, the Standing Committee I effectively started overseeing the intelligence and security services on 24 May 1993. It could not let this anniversary pass unnoticed. A celebratory 500-page volume of articles entitled '*Inzicht in toezicht*' (Insight into oversight) was compiled, dealing with virtually every aspect of democratic control over the intelligence services, and for which all players, past and present, were given the opportunity to submit their views. The book was appropriately presented to the Senate under the auspices of its Speaker.

If one thing has become clear, it is that the Standing Committee I has carved a permanent niche for itself in our democratic system. It has become an organisation that oversees how the intelligence services operate in practice and which, through its reports and recommendations, makes an essential contribution to the debate on their tasks and powers. This has been possible only thanks to the efforts and expertise of everyone that works or has worked for the Standing Committee I, regardless of their position within the organisation.

The Standing Committee I of today is certainly not the same as the review body that started in 1993. A host of legislative amendments and progressive insights in practice have ensured this. Some of the adjustments have been minor, technical interventions, while others have profoundly altered the form of the Committee and its operating procedures. The Act of 6 January 2014 proves that this evolution is far from over: the reform of the Senate under the sixth constitutional reform has seen the contact point of the Committee in Parliament move, since the elections of 25 May 2014, to a single 'Commission entrusted with monitoring the Standing Committee P and the Standing Committee I' in the House of Representatives, which will monitor both the police and intelligence services. But there is more. The commission is structured differently – the leaders of all political parties now get a seat – and their members are allowed access to classified information.[95] The future will show what influence these changes have on parliamentary review.

[95] In the meantime the situation has changed: the commission is composed of 13 MP's who have no access to classified information.

The other event of 2013, which dominated the second half of the year in particular, was that Edward Snowden, a former employee of an American intelligence service, managed to copy tens of thousands of extremely sensitive documents of the National Security Agency and pass these on to journalists. Unedifying reports about worldwide, massive data capture and economic and political espionage by the American and British intelligence services thus appeared repeatedly in the press. It goes without saying that the international intelligence community was considerably shaken by this. These revelations sounded the starting shot for parliamentary, judicial, and intelligence investigations throughout the world, including Belgium. The Standing Committee I initiated no fewer than four investigations in this regard.

The fact that certain major powers had been in possession of far-reaching resources and programmes for such massive data capture for some time was nothing new. What was new, however, was that this electronic gathering of information was taking place on such a comprehensive and massive scale, with the most advanced hardware and software and an unprecedented deployment of human and financial resources. A second new element was that it became increasingly clear that the major powers did not refrain from economic and political spying on 'friendly countries' through massive or targeted data capture. Government leaders, intelligence services and review bodies will have to draw the necessary lessons from this.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2014

CHAPTER II
REVIEW INVESTIGATIONS

Nine investigations were completed in 2013. An interim report on one of the investigations that followed the Snowden revelations was also completed (see II.10). Six of the ten investigations were held at the request of the Monitoring Committee of the Senate (of which one was also partly the result of an initiative by the Minister of Justice); four investigations were started after a complaint or report. The nine final reports (II.1 to II.9) and the interim report (II.10) will be discussed below. This will be followed by a summary and brief description of the investigations that are still ongoing (II.11).

The ten investigations opened in 2013 are also referred to in this last section. Three of those investigations were held jointly with the Standing Committee P. Of the ten new investigations, four were started at the request of the Senate, five as a result of a complaint, and one at the joint initiative of the Standing Committees I and P.

The Committee received a total of 28 complaints or reports in 2013. After verifying a number of objective points, the Committee rejected 22 of these complaints or reports because they were manifestly unfounded (Article 34 of the Review Act) or because the Committee knew it 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, five complaints from 2013 resulted in the opening of an investigation. One complaint, which was submitted at the end of the year, led to the official opening of an investigation only at the start of 2014. As such, it is not referred to further here.

II.1. THE ROLE OF THE GENERAL INTELLIGENCE AND SECURITY SERVICE IN MONITORING THE CONFLICT IN AFGHANISTAN

In December 2001, Belgium decided to participate in the International Security Assistance Force (ISAF), an international peacekeeping force in Afghanistan,

which was set up within the United Nations. In addition to NATO (and its Member States), twenty other countries participated in this force.

Most of the Belgian contingent was stationed in Kabul and responsible for the protection of the international airport. In the northern province of Kunduz, Belgian teams supported the reconstruction of the country and provided technical assistance to the Afghan army. Lastly, a number of Belgian fighter planes have been operating out of Kandahar since 2008.

In order to be able to form a complete picture of how the military intelligence service was involved in this operation, the Committee decided in January 2010 to open an investigation into '*the role of GISS in monitoring the situation in Afghanistan*'.[96] The Standing Committee I had a clear purpose with this investigation: to identify one of the most important tasks of GISS as fully as possible[97] in order to draw up a frame of reference for future missions and the investigations that can be instituted in reference to them.

The conclusions of the Rwanda Parliamentary Inquiry Committee[98], instituted in 1997 following the tragic death of ten Belgian para-commandos, obviously could not be disregarded in this report. This committee found the following with regard to the collection and analysis of intelligence:

- The Belgian contingent must always have its own solid intelligence network, consisting of intelligence officers who are adequately trained and, to the extent possible, have a command of the language of the country. At the very least, they must have reliable interpreters.
- In order to analyse the information, the military intelligence service must have enough analysts who can assess the content of the information. Systematic feedback must also be given to field units.
- It is necessary to reform the military intelligence service, including by taking into account the Act of 30 November 1998 on the intelligence and security services. The service must, in every respect, become an efficient and coherent instrument in support of those responsible for operations. It is necessary that this analytical capacity is made available to those in charge so they can determine the political options. Steps must also be taken to ensure that

96 As part of that investigation, of which a very comprehensive 'SECRET – Act of 11–12–1998' classified final report was delivered to the Minister of Justice in September 2013, the Standing Committee I could rely on the complete openness of the head and relevant members of GISS. The impeccable organisation of the on-site visits in Afghanistan also deserve mention.
The 'LIMITED DISSEMINATION' version of the report was discussed at the meeting of the Monitoring Committee of the Senate on 12 March 2014. Both during that meeting and afterwards (in a letter of 16 June 2014), GISS and the Minister of Defence wished to add a few clarifications and nuances to report. This report has taken those comments into account.

97 Only the collection of SIGINT in Afghanistan was not explained. This aspect was included in a later investigation (see II.10.12 Four investigations relating to the Snowden revelations).

98 *Parl. Doc.* Senate 1997–1998, no. 1–611/7.

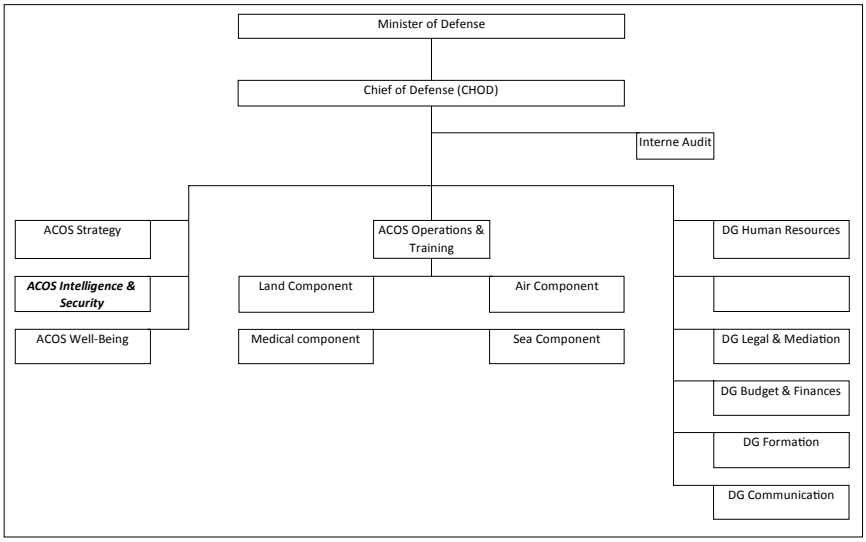
intelligence sources are sufficiently diverse and that the analysis can be contested. This means that information must be continually exchanged between the intelligence service on the one hand and those responsible in the field on the other hand.
– The military intelligence service must reinforce its field units in relation to intelligence, specifically by providing specialised personnel or via technical resources.

II.1.1. THE PLACE, STRUCTURE AND POWERS OF GISS

II.1.1.1. Place and structure of GISS

For a proper understanding, it is important to know how GISS is structured and where its service fits within the Armed Forces (which have other components entrusted with intelligence gathering).

Structure of the Belgian Armed Forces



The General Intelligence and Security Service, also known as the Assistant Chief of Staff Intelligence and Security (ACOS-IS)[99], is one of the staff departments of

[99] As most instructions and permanent orders of this service are in English, the Committee will take over the military terminology in use.

the Armed Forces.[100] At the time of the investigation, the service was made up of four divisions.[101]

The S(ecurity) Division carries out security investigations in relation to specific persons or firms and ensures compliance with the directives on the military security of domains, people, ICT systems, etc.

The (A)ppui Division is responsible for HR and budgetary management, ICT and logistics aspects that are managed within GISS itself.

The C(ounter) (I)ntelligence Division monitors threats against military security or other interests that GISS must defend on Belgian territory. However, this division also has another role to fulfil in the force protection of Belgian units abroad: it provides support to these units to combat specific threats (e.g. infiltration by local groups).

Lastly, the I(ntelligence) Division forms the largest component of GISS. It focuses on phenomena occurring abroad and therefore operates in places where Belgian troops are deployed. The Analysis Services of Division I are mostly organised by geographical region, while there are also offices for Naval and Land Intelligence and cross-border issues. Different services within the Division are actively gathering intelligence: Human Intelligence (HUMINT), Image intelligence (IMINT), Signals Intelligence (SIGINT or COMINT) and Open Sources Intelligence (OSINT). Local intelligence-gathering assignments rest with the I/Ops Department. The I/Ops units that are deployed abroad are called BENIC (Belgian National Intelligence Cell) or BELINT (Belgian Intelligence).

II.1.1.2. GISS's assignments

GISS's four assignments are described in Article 11 of the Intelligence Services Act: the classic intelligence task, ensuring military security, protecting military secrets, and performing security investigations. Each of these tasks may have a link to foreign operations. For example, GISS is entrusted with collecting, analysing and processing information (i.e. its intelligence assignment) that relates to every activity that threatens or could threaten the execution of '*missions, actions or operations in a national context, in the context of an alliance or an international or supranational cooperation agreement*' of the *'Belgian Armed Forces, of allied armed forces or of inter-allied defence organisations*'. Information may also be gathered about collective threats against *'the life or physical integrity of Belgians abroad and their family members*'. The second

100 The Review Act and Intelligence Services Act use the term 'General Intelligence and Security Service of the Armed Forces' (GISS), while the Royal Decree of 21 December 2001 determining the general structure of the Ministry of Defence and the powers of certain authorities (RD Defence) refers, in turn, to the Assistant Chief of Staff Intelligence and Security (ACOS-IS). This is one and the same service.

101 The S(ecurity) and C(ounter) (I)ntelligence Divisions were added in 2013.

assignment – ensuring military security[102] of, for example, '*the personnel under the Minister of Defence*' as well as '*the military installations, weapons, munitions, equipment, plans, texts, documents, computer and communications systems or other military subjects*' – is also important in foreign operations.

II.1.1.3. The powers of GISS and the principle of territoriality

Article 11 of the Intelligence Services Act leaves no doubt that GISS may gather intelligence *about* foreign countries. But can the service also gather intelligence *in* foreign countries? It is not expressly stated anywhere that GISS may act abroad. However, this follows logically from the description of a number of assignments (e.g. the security of operations in the context of an alliance and the security of Belgian nationals abroad), which are impossible to observe only from within Belgium. The same applies to the other assignments. For example, no distinction is made in regard to the protection assignment between personnel or equipment situated within Belgium or abroad.

However, the fact that GISS may act abroad does not mean that all intelligence methods may be used. The use of specific or exceptional intelligence methods under Article 18/1, §2 of the Intelligence Services Act, for example, is permitted only within Belgian territory. The use of these methods as part of an investigation into a possible threat to a foreign mission is thus possible if it occurs within Belgian territory.

GISS was of the opinion that the special intelligence methods may be used abroad. The Committee is of the opinion that this interpretation is contrary to the law. It is however possible, for example, to intercept communications originating abroad, for the security and protection of our troops and those of our allied partners during missions abroad. After all, GISS has a specific legal mandate for this purpose (Article 259*bis* §5 of the Criminal Code, as read together with Article 11 §§2 and 3 of the Intelligence Services Act), which is lacking for the other methods. With a view, among other things, to human rights and operational needs in the field, the Minister of Defence agreed to pay specific attention to this issue during the evaluation of the Special Intelligence Methods Act.

II.1.1.4. Communication of intelligence to third countries

The communication of intelligence to third countries and their possible use thereof is a specific problem. In accordance with Articles 19 and 20 of the Intelligence Services Act, GISS may/must cooperate and exchange intelligence with foreign services. The question is whether such a situation can lead to the

[102] This assignment is limited to drawing up directives and guaranteeing compliance with them, for instance by carrying out on-site inspections.

legal responsibility of the service.[103] The English High Court of Justice had to rule on the claim of a Pakistani citizen. The Pakistani citizen maintained that members of the British GCHQ committed crimes (complicity in murder) by delivering SIGINT that the NSA and CIA then allegedly used to carry out drone attacks that killed his father. The High Court of Justice rejected the claim because the member of the intelligence service in question was unable to determine which intelligence he may or may not pass on to those responsible in the field.[104]

II.1.1.5. Some other players in intelligence gathering

GISS is by far not the only entity within the Belgian Armed Forces that gathers intelligence and may operate abroad.

Within the Land, Sea and Air unit[105] of the Assistant Chief of Staff of Operations and Training (ACOS-Ops & Trg), there are services that gather and process intelligence during operations and the preparation thereof from all types of sources (e.g. via GISS or field commanders). How those services must cooperate with each other was described at the time of the investigation in the Standing Operating Procedure (SOP) Joint Intelligence, Counter-Intelligence and Security Structure of 2008[106], which proceeded from ACOS-Ops & Trg. Among other things, this SOP described the position of GISS in the overall Defence 'intelligence structure'. It was stated, for example, that GISS receives directives from the Minister of Defence and the Chief of Defence (CHOD), must focus on political/strategic and operational intelligence and, if necessary, may deploy an intelligence cell abroad.

In every operational unit of the Armed Forces there is an 'S2-function' that is exercised by the officer that assists the Commanding Officer in providing intelligence about the situation in the field. He provides mostly tactical information.[107]

During operations, the Commanding Officer is assisted by a Battle Group Intelligence Cell (BIC). A reconnaissance battalion called Intelligence, Surveillance, Target Acquisition and Reconnaissance (ISTAR) was also established in 2011. This battalion carries out missions with a view to preparing for action in the field and gathers mostly tactical intelligence in this regard.[108]

---

103 For this purpose, see footnote 111 with regard to the explanation of GISS in the Senate.

104 High Court of Justice, Queen's Bench division, Administrative Court, *R – Noor Khan v Foreign Secretary* – 2012.

105 In Afghanistan, for instance, a division of Air-Intel was active and specialised in the assessment of operational air threats.

106 This Standing Operating Procedure (SOP) was replaced by 'The Belgian Joint Intelligence and Security Structure' SOP of November 2013 (also of ACOS-Ops & Trg).

107 During the parliamentary preparation of the Intelligence Services Act, a distinction was already made between strategic or geopolitical intelligence on the one hand and tactical intelligence that relates to reality in the field and the deployment of a unit on the other hand (*Parl. Doc. House of Representatives* 1996–1997, 49–638/14 22–24 and 38).

108 See also Chapter V.2.

Lastly, there is also the Information Operations Group of the Army under which Psyops and Human Factor Analysis falls. Psyops focus on communicating with the local population and authorities in places where Belgian troops are deployed. The service must also respond to any anti-Belgian propaganda. The Human Factor Analysis studies various human factors that can influence a mission, such as anthropology and human geography.

II.1.2. THE PLACE AND POWERS OF GISS WITHIN THE ISAF

II.1.2.1. The ISAF operation

Three days after the 9/11 attacks, the US Congress adopted a resolution which authorised the use of armed force against those responsible for the attacks and those that offered them refuge. On 15 September 2001, the North Atlantic Council of NATO met and declared Article 5 of the North Atlantic Treaty applicable at the request of the United States: this relates to the right of assistance from NATO Member States to a Member State that has been the victim of an armed attack.[109]

On 20 September 2011, the United States named Osama Bin Laden and his organisation, Al Qaeda, as those responsible for the 9/11 attacks. Bin Laden was living in Afghanistan at the time, where the Taliban regime protected and refused to extradite him.

In October 2001, American, British, French, and Australian troops engaged in action with local opposition groups and formed what became known as the Northern Alliance. This was called Operation Enduring Freedom (OEF).

Belgium – and thus also GISS – do not operate within this framework.[110] The activities of the Belgian Armed Forces form part of a UN mandate. This mandate originated in the Bonn Agreement of 5 November 2001, which proposed the establishment of an International Security Assistance Force (ISAF). The Afghan signatories of this agreement requested the Security Council of the United Nations '*to consider authorizing the early deployment to Afghanistan of a United Nations mandated force. This force will assist in the maintenance of security for Kabul and its surroundings. Such a force could, as appropriate, be progressively expanded to other urban centres and other areas*'.

The UN Security Council complied with this request by adopting Resolution 1386(2001) on 20 December 2001. This resolution gave the mandate for the

109 This was the only time since the creation of NATO that this article had been applied.

110 Belgium only took part in Operation Enduring Freedom in the form of support operations outside Afghan territory (including by deploying C-130 transport planes for humanitarian aid, stationing a frigate in the Mediterranean Sea, and providing crew for the AWACS aircraft in addition to the United States).

deployment of an ISAF '*to assist the Afghan Interim Authority in the maintenance of security for Kabul and its surrounding areas, so that the Afghan Interim Authority as well as the personnel of the United Nations can operate in a secure environment*'.

The Belgian government already decided to participate in this mission on 21 December 2001. A first transport plane was deployed at the end of January 2002, while the deployment of troops in the field followed around a year later.

The ISAF mission initially fell under a command that rotated every six months. NATO took over the command of ISAF in March 2003. Twenty other forces are present in addition to NATO members.

It is important to emphasise that the aim of the ISAF forces is to guarantee the safety of the population and support the legitimate Afghan authorities so they, along with the UN authorities, can perform their civil duties. From a military perspective, this means that ISAF troops must secure the field by countering and weakening adversaries so they are no longer able to destabilise the country. Nonetheless, this military task does not form the essence of the ISAF mission. The mission focuses mainly on what is called counterinsurgency, by trying to reduce and over time eradicate the support (passive or otherwise) that the insurgents enjoy among the population. After all, it is this breeding ground that enables the insurgents to continue their opposition. The operation is thus actually a battle to win over the hearts and minds of the population. The military presence can only facilitate this task by creating a security situation in which the civil authorities can perform their duties.

ISAF is not only not a pure military operation, it is – unlike Operation Enduring Freedom – also not a fight against terrorism. In this regard, reference must be made to the *CHOD OPORDER for Bel contribution to ISAF* (see further under II.1.3.3.4), which states that Belgian troops will not participate in Counterterrorist operations. However, in relation to passing on intelligence, it cannot be excluded that intelligence which is shared as part of the ISAF operation with members of this coalition via the allies that also form part of the US-led coalition finds its way to the OEF, even if that is not the intention.[111] The close connection in the field between both missions is also evident from the fact that the command of ISAF and that of US forces in Afghanistan coincides (USFOR-A).

---

111 GISS verbally stated the following before the Foreign Operations Parliamentary Committee of 19 April 2012: *'In conclusion, we can assure you that under no circumstances neither the collected information nor the analyses supplied aim at targeting. All our products definitely serve for the purposes of protection, prevention and contextualization of the decision process. However we cannot deny that other practices apply within the Four Eyes (UK/US) or Five Eyes (US/UK/CAN/NZ/AUS) community'* (free translation).

II.1.2.2. The Belgian presence in Afghanistan focusing on GISS

Until 30 September 2012, most of the Belgian contingent (320 people) was responsible for protecting the Kabul international airport (KAIA). Belgium also played a role within the general staff of the ISAF in Kabul and stationed a national support unit in Kabul International Airport. Belgium sent around 25 service personnel as support in Kunduz to the provincial reconstruction teams (PRTs) with the task of securing the environment, coordinating reconstruction projects, and providing support in the areas of health, education and NGOs.

Belgium also had a Military Assistance Team (MAT) of around 60 service personnel in the north of Afghanistan whose task was to provide technical advice to the general staff of a brigade and a battalion of the Afghan national army.

There were also Belgian F-16 fighter jets at the base in Kandahar and Belgium participated from 2008 in Operation Guardian Falcon and trained Afghan pilots and medical personnel in Kandahar.

Lastly, a number of service personnel were also deployed in Mazar-E-Sharif.

In relation to GISS, Divisions I, CI and S participated in assignments in Afghanistan. The composition and numbers of GISS personnel obviously varied based on demand and availability. The strategic situation was monitored by people who were assigned to the Belgian National Intelligence Cell (BENIC). GISS also deployed personnel who were responsible, for example, for exchanging information between the locally deployed Belgian units and the foreign military allies and passing on that intelligence to the Battle Group Intelligence Cell (BIC), the S2, and any other partners. Analysts of Division I were also sent on an *ad hoc* basis to Afghanistan. The Committee found that their assignments were not always clearly described. Division CI was present, among other things, to detect any security problems for the Belgian units, to monitor the local personnel that worked for the Belgian units[112] and to assess the degree of appreciation that the Belgians enjoyed among the Afghans working with the ISAF, and others. Lastly, ADIV-S sent a team if a security audit was requested. Where relevant, this team audited the enforcement of security rules with regard to the personnel, equipment and infrastructure.

GISS obviously did not monitor the local situation within Afghanistan alone. An 'Afghanistan Bureau' was established in Brussels and staffed by analysts. It answers Requests for Information (RFI) from ACOS-IS, NATO, the EU and so-called 'friendly services' and analyses the information originating from the different intelligence-gathering bodies (HUMINT, IMINT, SIGINT, etc.). The bureau also gives briefings to the general staff for the units that have been called up for deployment to the field, for BENIC, and for external partners (e.g. ambassadors).

112 NATO's vetting bureau screened these Local Employed Personnel.

The majority of RFIs received by the analysts relate to questions of an operational or tactical nature (mostly from ACOS-Ops & Trg), while strategic questions only make up a minority.

The Committee found that the analysts of the Afghanistan bureau did not always know exactly what intelligence their partners from the intelligence and military world expected. Conversely, the questions that the latter ask are often not very specific because they do not know what GISS can provide. The presence of analysts in the field proved important for better coordination of supply and demand.

II.1.3. REGULATORY FRAMEWORK APPLICABLE TO GISS IN AFGHANISTAN

II.1.3.1. The national framework

Reference must obviously be made first of all to Article 11 of the Intelligence Services Act, which provides a general description of GISS's four assignments (see II.1.1.2 above). It must be emphasised in relation to the classic intelligence task that the law makes no distinction among political/strategic, operational or tactical intelligence.[113] Although it is clear from the preparatory work of the Act that gathering purely tactical intelligence was not really viewed as an GISS assignment (see II.1.1.5 above), the service is active in the three fields of intelligence. After all, monitoring activities that may constitute a threat to the completion of missions by armed forces may involve all forms of intelligence.

Article 23 of the Royal Decree of 21 December 2001 determining the general structure of the Ministry of Defence and the powers of certain authorities stipulates that the Assistant Chief of Staff Intelligence and Security (ACOS-IS) is entrusted, among other things with '*organising intelligence and security support to operations*'.

Pursuant to the Intelligence Services Act, the Ministerial Committee for Intelligence and Security (MCI&S) may issue additional directives on the functioning of the military intelligence service in case of foreign operations. This has not been used yet. The Ministerial Committee has also not yet issued any directives for the exchange of intelligence with foreign services. The Standing Committee I has already pointed out this shortcoming several times.[114]

---

113 Strategic intelligence is intended to support political/military decision-makers. Operational intelligence, on the other hand, is intelligence that is useful for preparing and implementing campaigns in the field (for instance: what are the troop levels of the adversary in a region and what are conditions like in the field?). Lastly, tactical intelligence is very concrete intelligence that relates to very specific situations that are immediately helpful to personnel in the field.

114 See STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 132; *Activiteitenverslag 2007* (Activity Report 2007), 73; *Activiteitenverslag 2008* (Activity Report

GISS's priorities are described in the Intelligence Steering Plan (of Division I) and the Security Intelligence Steering Plan (of Division CI). According to the Intelligence Steering Plans, Afghanistan has merited a permanent and intensive analysis, based on continuous and thorough tracking of intelligence by the intelligence-gathering bodies, since 2001. This was not previously the case. We see the same evolution in the Security Intelligence Steering Plans.

The *CHOD Operations Order for Bel Contribution to ISAF* (2012) is also important. This directive describes GISS's contribution to the military intervention in Afghanistan in general terms: the service gets involved from an intelligence perspective in the preparation and execution of the foreign operation. The directive also stipulates that the Belgian intelligence capacity (BELINT) remains under its own command. BELINT's tasks extend to strategic as well as operational and tactical intelligence gathering and/or dissemination.

GISS moreover issues directives itself containing the more practical details of all important organisational and operational aspects of assigning personnel abroad and deals in greater detail with the force protection assignment.

Lastly, there are also a number of Fragmentary Orders (FragO) relating to specific missions, for instance a particular team within a certain period. A FragO is in fact an elaboration of a general Operations Order for a specific assignment.

II.1.3.2. The international framework

Particular attention must be paid at international level to the *SACEUR Operational Plan for ISAF* that provides a framework for the intelligence services of the nations that cooperate in ISAF operations.[115] In principle, the local GISS elements do not fall under ISAF/NATO command, contrary to the operational Belgian units. BELINT therefore cannot receive specific instructions to perform certain acts. Obviously, this does not prevent BELINT from cooperating with the ISAF institutions (e.g. in the form of exchanging intelligence). Quite the

2008), 6 and 109–110; *Activiteitenverslag 2009* (Activity Report 2009), 4 and 106–107; *Activiteitenverslag 2010* (Activity Report 2010), 3–4 and *Activiteitenverslag 2012* (Activity Report 2012), 95.

115 A number of internal NATO rules are also applicable, firstly because Belgium is a member of NATO and secondly because ISAF operates under NATO command. The *NATO Human Intelligence (HUMINT) Policy IMSTAM(INT)-0157–2011(SD1)*, for example, contains the NATO policy on HUMINT. This document, which is not specifically intended for the ISAF operation, deals with various topics, including the need for the different Member States to exchange intelligence and the interoperability of the systems used for this purpose. Reference can also be made to the *NATO STANAG 2578 – Allied Intelligence Publication – AIntP-5 – Doctrine for Human Intelligence Procedures*. Among other things, this directive describes the conditions that a HUMINT operator must satisfy, the best way to gather data, and how to draw up a report. The organisation and structure of HUMINT are also discussed. This instruction is intended to establish a uniform approach among the different Member States and guarantee a certain level of quality.

contrary. The *SACEUR Operational Plan for ISAF* assumes, for instance, that countries participating in the operation will be prepared to receive and process Requests for Information from ISAF. BELINT will also subscribe, as far as possible, to the setting of priorities by ISAF so its intelligence-gathering contributes to the intelligence objectives determined by the Operational Plan.

II.1.3.3. Some points for improvement[116]

II.1.3.3.1. Integrated rules, a common conceptual framework, and precise intelligence objectives

The Standing Committee I is of the opinion that more attention could have been paid in the above documents and rules to mutual coordination, even if they were not contradictory to each other. There is little or no integration between the international rules and Belgian rules. While it is true that this involves different authority levels that are independent from each other, this provides no guidance to those in the field.

The Committee is further of the opinion that a type of common conceptual framework should perhaps be used for Belgian rules, which could cover all assignments and tasks of the military intelligence service. This conceptual framework would have to be based on the threats described in the Intelligence Services Act. Following on from this, there would need to be a description of what this means exactly for GISS, the bureaus, and each member of the personnel. In other words, the aim must be to translate the remit into intelligence needs and resources to be deployed so all personnel are aware of the precise intelligence objectives.[117] This determination applies both before and during an operation.

Until shortly before that, little or nothing had been determined about GISS's precise role in preparing for the international intervention. This meant, for example, that the 'intelligence effort' with regard to the situation in Afghanistan remained very limited after the government decided to participate in the international intervention there in 2002.

II.1.3.3.2. Documented methodology in preparing for a mission

The Committee concluded that no documented methodology was used prior to the mission. This has now changed. For the past two years, ACOS-Ops & Trg has used the *Comprehensive Preparation of the Operational Environment* method

---

116 During the course of the investigation, GISS already anticipated a number of formulated comments and implemented a number of changes.

117 The lack of such a structured approach was also established during GISS audit of 2011 (STANDING COMMITTEE I, *Activiteitenverslag 2011* (Activity Report 2011), 7–14 and 104–107).

(CPOE) to prepare for missions. It seems as though there is an important, although not exclusive, role for GISS with regard to the intelligence function. The Committee is of the opinion that further elaboration and following of such a doctrine and methodology must be encouraged.

II.1.3.3.3. Documented methodology during a mission

Even during the execution of the Afghan operation, the precise information and intelligence objectives of GISS were not always well defined. Ideally, the information and intelligence needs and resources for deployment would be determined on the basis of the objectives and threats set out in the Intelligence Services Act.

II.1.3.3.4. Integrated approach for all divisions

The investigation has shown that until the end of 2012, there was no document that included Divisions I, CI and S together in an integrated manner. Although the *CHOD OPORDER for Bel Contribution to ISAF* did include a number of provisions on the intelligence assignment, it was silent on the contribution of Divisions CI and S. This was remedied with regard to Division CI in January 2013.[118]

II.1.3.3.5. Lack of clarity regarding the intelligence to be gathered

The Standing Committee I found a lack of clarity regarding the nature of the intelligence that GISS had to mainly focus on: strategic, operational and/or tactical. According to the SOP OPS *Joint Intelligence, Counter-Intelligence and Security Structure* of ACOS-Ops & Trg (see II.1.1.5), GISS must mainly provide political/strategic and operational intelligence. However, in the CHOD OPORDER on Afghanistan (see II.1.3.3.4), GISS was also given a tactical intelligence assignment.

It appears in practice that GISS's analysis services are rather focused on strategic intelligence but that in the field it is mostly operational/tactical intelligence that is needed.

The Standing Committee I finds that this lack of clarity has already existed for some time. This question is important for how GISS organises its intelligence-gathering and processing. Mixing different types of intelligence without making a distinction can adversely affect efficiency. There is also an effect on the knowledge domains that are necessary for gathering and analysis: the more 'political/civil approach' for strategic intelligence as opposed to the 'military facts and figures' for tactical and operational intelligence.

[118] The joint use of the divisions in the field has been a fact since that date.

II.1.4. VIEW OF GISS's CLIENTS

The Standing Committee I held a survey among GISS's main clients: FPS Foreign Affairs (involving particularly its Crisis Centre for the protection of Belgian nationals abroad and the Security Service for security in foreign diplomatic posts), ACOS-Ops & Trg whose duties within Defence include the operational command of the intervention troops, and the Cabinet of the Minister of Defence.

Generally speaking, these 'clients' appeared to be relatively satisfied with the cooperation with GISS. The service appears, on the one hand, to respond quickly and flexibly to the questions posed to it, and on the other hand the relevance and accuracy of the products are emphasised. GISS moreover has an outstanding reputation with regard to the reliability of its products.

GISS has both formal and structured contact with its partners and simultaneously has many informal contacts that facilitate the flexibility and adaptability of its actions.

GISS's products cover mainly security themes on an operational, tactical and strategic level and fewer political themes. Nevertheless, GISS's task is also to deal with economic, social and media-related domains as provided for in the *Comprehensive Preparation of the Operational Environment* (CPOE). According to GISS, these domains are only partially covered due to a lack of personnel. It was therefore recently agreed that Defence would concentrate on security problems and Foreign Affairs on the above domains.

ACOS-Ops & Trg has indicated that it expects greater involvement from GISS, particularly in relation to the CPOE. In view of the importance of this assignment for both the military authorities and the Minister's staff, it is up to GISS to consider its capacity to meet this demand.

Lastly, the Committee concluded that the clients are not sufficiently aware of what GISS can produce and – even though they are satisfied with GISS's contribution – they consequently do not ask all possible questions. From its side, GISS's analysis service regrets the lack of feedback on its products.

II.1.5. CONCLUSIONS

II.1.5.1. The legality test and other regulatory aspects

The Committee was of the opinion that GISS performed its assignments in Afghanistan in accordance with national and international regulations, notwithstanding the fact that these rules are not only numerous but also poorly integrated.

However, the Committee regretted the fact that GISS did not dedicate any study to its possible responsibility for providing information or intelligence to a

foreign service or institution. The fact that the Ministerial Committee for Intelligence and Security had not yet drawn up any directives in this regard did not change this.

Lastly, the Committee drew attention to the need to redefine the concepts of 'operational', 'tactical' and 'strategic' intelligence. Most international and national rules apply these concepts to demarcate the areas of competence of the various players (BENIC, intelligence officer, S2, BIC, etc.). However, the Act of 30 November 1998 does not use this terminology; it determines GISS's powers on the basis of the threats that must be monitored. In order to perform this assignment, GISS must gather all available intelligence. The Committee also established that these concepts are not decisive in practice for gathering or disseminating intelligence. The Committee therefore felt that it would be useful to consider the connection between these concepts and GISS's legal assignments. This seems to be all the more necessary given the existence of the ISTAR battalion (see *supra*).

II.1.5.2. The need to estimate the risk for personnel in conflict zones

The Committee has been able to establish on several occasions that GISS personnel run risks in certain situations. This is why it placed such a strong emphasis on the quality of training prior to deployment and the need to have adequate equipment and logistical resources.

More specifically, the Committee established that GISS has still not made a general estimate of the risks inherent in deploying military or civilian personnel in conflict zones. Such an estimate must, for example, enable one to assess whether a deployment of civilian personnel (analysts) can be contemplated and, if so, to determine the needs for training and equipment. In addition, the role analysts can play in an environment in which intelligence-gathering is done should be set out, specifically to guarantee the objectivity of the assessment function and to avoid any influence. This reflection on risks must obviously also apply to GISS's service personnel. The Committee considered this still to be insufficient.

II.1.5.3. The need for a more systematic approach to deploying GISS in a conflict zone

The Committee was of the opinion that the deployment of GISS in Afghanistan had been done pragmatically. Such an approach is not necessarily incorrect, but there is a risk that a number of other conceptual aspects are overlooked. An integrated approach, which takes the threats to be monitored as its starting point, provides the opportunity to make coherent connections among the Intelligence Services Act, GISS's mission statement, the integrated strategic plan of I, CI and S, the Intelligence and Security Information Steering Plans, the

intelligence-gathering plan and, in particular, the human and material resources that must be used to achieve the intelligence objectives. In general, only an integrated approach allows one to objectively determine whether GISS has adequate personnel and equipment to perform its legal assignments.

II.1.5.4. The need for adequate equipment

The Committee concluded that the physical integrity of GISS's personnel could be at risk. It is therefore necessary that they have adequate material resources. This is generally also the case. However, the means of communication that are provided to BENIC can be improved.

II.1.5.5. Recommendations of the Rwanda Committee

II.1.5.5.1. Clear rules with regard to deployability and the translation thereof into understandable directives.

The Committee highlighted the plurality of national and international rules that apply to the deployment of the Belgian army in Afghanistan. These rules are moreover very complex, on the one hand because there is a lack of integration (and no available Code) and, on the other hand, because there is a lack of 'translation' of the rules into understandable directives. Such complexity may lead to ignorance of the rules or their incorrect interpretation. The Committee therefore called for an integrated presentation of the prevailing rules.

As far as national rules are concerned, the Committee was moreover of the opinion that these should be better harmonised, for instance by taking GISS's legal assignments as their starting point.

II.1.5.5.2. Adequate preparation for an assignment

The Committee was able to establish that GISS members undergo specific preparation before their departure. This preparation involves various aspects such as local behaviour, the situation in the country, and a practical explanation of the rules on deployability. With the exception of this last aspect, the Committee could identify recent important improvements in this regard.

II.1.5.5.3. A solid intelligence network

The Rwanda Committee insisted that GISS must have its own intelligence network in future as well as educated and trained intelligence officials that have a command of the language or can rely on interpreters. Although the Committee could establish that this objective had been achieved, it did see two areas for improvement.

Firstly, the training of the deployed GISS personnel could be improved. GISS must make a significant and continued effort in this regard. Recent adaptations have undoubtedly added value but have not been adequate in the Committee's opinion. The training must be practical and flexible and may not be dependent on the availability of instructors.

Secondly, GISS's role in the preparation of an international assignment must be reinforced. GISS must subscribe to the methodology of the *Comprehensive Preparation of the Operational Environment* (CPOE), adapt to the needs of partners within the army and act proactively in this regard. Among other things, this requires GISS to perform analyses in the domains under its authority.

II.1.5.5.4. Adequate and competent analysts

The Rwanda Committee insisted on the reform of GISS so the service would form an efficient and coherent instrument for those bearing responsibility for an assignment. It also suggested improving the assessment capacity and making this available so political options can be worked out for those responsible.

The Committee found that these objectives had been largely achieved. GISS has indeed become an indispensable and important partner in gathering and utilising intelligence for the troops in the field and, in particular, for the purpose of force protection. Its role as adviser to those who are hierarchically and politically responsible and its actions in preparing for or during operations were also confirmed.

The Committee is nevertheless of the opinion that it has not yet been possible to fully play the role of adviser to those who are hierarchically and politically responsible. This is possibly and partly as a result of a shortage of analysts within GISS. However, this shortage could be made up if analysts were used more on the basis of clear intelligence objectives.

GISS's clients confirmed they were satisfied with GISS's products, yet conceded they were not really aware of what products could actually be supplied. From their side, the analysts felt that clients gave them insufficient feedback on their products. These findings call for a more proactive approach by GISS towards its clients. Specifically, this means that GISS must actively question the needs and requirements of both the internal and external clients of Defence in order to be able to optimise the efficiency of their products. The Committee did however recognise that the clients also need to contribute towards this optimisation.

II.1.5.5.5. The need to deploy specialised teams

During its mission in Afghanistan, the Committee was able to conclude that the teams deployed by GISS worked very professionally and to the satisfaction of Belgian and foreign authorities. The commanders of the local Belgian units recognised there was a systematic return to field units.

II.2. CONFIDENTIAL MEMORANDA ABOUT THE CHURCH OF SCIENTOLOGY IN THE PRESS

On 17 January 2013, the press cited passages from the State Security memorandum *'Church of Scientology – Infiltration in the Congolese community or in the community of people of Congelese origin in Belgium, Settlement in the Democratic Republic of Congo*' (free translation).[119] The service had disseminated this confidential and classified memorandum of 11 December 2012 among certain authorities shortly before this date. The articles alleged that the Church of Scientology was trying to expand its activities in Africa and looking for middlemen for that purpose in the Belgian Congolese community. A number of politicians were also mentioned by name[120]: Bertin Mampaka, the incumbent deputy president of the Brussels Capital Parliament and municipal executive member in Brussels[121]; Justine Kasa-Vubu, former minister in the first government of Laurent-Désiré Kabila and subsequent ambassador in Brussels; Gisèle Mandaila, an incumbent Brussels MP and, in 2004, Secretary of State for Families and Disabled People and a municipal executive member in Etterbeek and, lastly, Pierre Migisha, an incumbent Brussels MP and municipal executive member in Anderlecht at the time of the leak.

At the request of the Monitoring Committee, an investigation was opened to study both the drafting and distribution of the memorandum.

Almost fourteen days later, another State Security memorandum was reported in the media.[122] This time it was the '*Phenomenon analysis – Interference activities not directed by a State*' (free translation). This secret report also allegedly cited numerous politicians because of their relationships with the Church of Scientology, among others. The Minister of Justice then entrusted the Committee to carry out an investigation. It firstly had to investigate whether the ministerial directive of 25 May 2009, according to which the Minister of Justice has to be advised whenever the name of a federal Member of Parliament is mentioned in a report, had been correctly applied and/or whether or not it was appropriate for Members of Parliament to be mentioned by name in a phenomenon analysis. One day later, the Monitoring Committee gave instructions for its first investigation to be extended to the creation and publication of this phenomenon analysis and the question of whether the

---

119 A. CLEVERS, *La Dernière Heure*, 17 January 2013 (La Scientologie infiltre les milieux belgo-congolais); K. VAN EYCKEN and H. ADRIAEN, *Het Laatste Nieuws*, 17 January 2013, *Scientology infiltreert in Congolese gemeenschap in Brussel* (Scientology infiltrates Congolese community in Brussels).

120 The names of these politicians were discussed extensively in the media.

121 The party involved was later appointed as Senator by the Parliament of the French-speaking Community.

122 M. BUXANT and S. SAMYN, *De Morgen*, 2 February 2013, *Staatsveiligheid houdt Wetstraat in de gaten* (State Security keeps an eye on Wetstraat).

Belgian intelligence services had correctly applied the need-to-know principle.[123]

The assignments that the Monitoring Committee and the Minister of Justice entrusted to the Committee largely related to the same issue. The Committee therefore decided to bring all those aspects under the umbrella of a single investigation, which was entitled '*Investigation into how State Security drafted and distributed the memorandum on the infiltration of the Congolese community in Brussels by the Scientology movement and the 'Phenomenon analysis – Interference activities not directed by the State' report, including studying the problem of mentioning the names of political representatives and the lists of addressees and their 'need-to-know'* (free translation).[124]

II.2.1. THE CONFIDENTIAL MEMORANDUM OF 12 DECEMBER 2012 ON THE CHURCH OF SCIENTOLOGY

II.2.1.1. Content of the memorandum

State Security must monitor activities that threaten (or could threaten) the security of the State and the maintenance of democratic and constitutional order. In carrying out this assignment, State Security came across the names of political representatives who could be connected to the Church of Scientology. This gave rise to the drafting of various memoranda, including the leaked memorandum of 11 December 2012 that dealt with the relationship of the four aforementioned politicians with the Church of Scientology. The memorandum can be summarised as follows:

– one of the four persons involved was approached by the Church of Scientology;

---

123 The Committee was also entrusted with a 'transversal analysis' of how the intelligence services gathered information about political representatives (II.4).

124 It was not only The Standing Committee I that opened an investigation. As a result of the various leaks, State Security filed a civil complaint at the start of February 2013 against unknown parties due to an infringement of Article 11 of the Act of 11 December 1998 on classification and security clearances, security certificates, and security advice (Classification Act). The Committee was not given any insight into the judicial investigation. The National Security Authority (ANS/NVO) also opened an investigation into the addressees of both the first memorandum and the phenomenon analysis. The Standing Committee I was also not advised of the results thereof. Lastly, on 20 March 2013, a complaint was filed at the Standing Committee I in the name of *Scientologykerk van België vzw*. The resultant investigation was completed at the start of 2014 (II.11.8). A 'Proposal to establish a parliamentary inquiry committee entrusted with an investigation into cases where State Security 'shadows' politicians was also tabled in Parliament. (*Parl. Doc*. House of Representatives 2012–2013, no. 53K2652/001 and *Parl. Doc*. Senate 2012–13, no. 5–2034/1).

– a second maintains a relationship with the Church of Scientology;
– State Security alleges on the basis of facts stated by the external services that the other two have very close ties with or are even members of the Church of Scientology.

According to the Committee, State Security was acting within the scope of its statutory powers as described in the Act of 30 November 1998 in drafting this first memorandum. The Committee referred more specifically to Article 8(1)(e) and (g) which relates to 'harmful sectarian organisations' and 'interference'. The Committee had no indication of any irregularities in the gathering of the intelligence that formed the basis of the memorandum. The memorandum was moreover balanced in its wording.

II.2.1.2. Addressees of the memorandum and their 'need to know'

The memorandum in question was sent to six addressees, namely the Minister of Justice, the Minister of Foreign Affairs, the Ambassador of Belgium in Congo, and the Chairman, Head of Security, and Africa Director of FPS Foreign Affairs. They all held the required security clearance. Furthermore, their respective roles as minister, high-ranking official or diplomat and their responsibility for diplomacy and international relations meant that the need-to-know requirement had been met. The memorandum namely related to the infiltration of the Congolese or of Congolese origin community in Belgium by the Church of Scientology and its branch in the Democratic Republic of Congo. The Committee felt that this intelligence was important for the authorities entrusted with Belgian foreign policy. This intelligence had therefore to be given to the authorities concerned in accordance with Article 19 of the Intelligence Services Act.[125]

II.2.1.3. Notification requirement

During the period to which the investigation related, there were two directives that obliged State Security to notify the Minister of Justice if politicians were the subject of intelligence activities: a ministerial directive of 25 May 2009 – drawn up in response to recommendations of the Standing Committee I as part of an earlier investigation[126] – and an internal instruction of 27 March 2012.[127]

---

125 *'The intelligence and security services shall communicate the information referred to in Article 13, second paragraph, only to the relevant ministers and the relevant judicial and administrative authorities, to the police services and to any competent bodies and persons in accordance with the objectives of their assignments and to bodies and persons who are the subject of a threat as referred to in Articles 7 and 11.'*

126 STANDING COMMITTEE I, *Activity Report 2008*, 22–33 (II.2 'Reserved dossiers at State Security).

127 See also II.4.2.1.3 in this regard.

The directive of 25 May 2009 stipulates that the Minister of Justice must be informed whenever the name of a current federal Member of Parliament is mentioned in a report. None of the four parties involved held such a mandate at the time. Notice was therefore unnecessary.

The scope of the internal instruction of 27 March 2012 is both narrower and broader than that of the ministerial directive: on the one hand, it relates only to any reference made in the reports of State Security's external services but, on the other hand, it relates to all ministers and political representatives, including those of the Communities and Regions.

There was also no need to give any notice under this directive in respect of Justine Kasa-Vubu as she was not a Belgian political representative.

The minister should have been informed about the other three parties. State Security sent a first memorandum in relation to Bertin Mampaka to the Minister of Justice in July 2012, referring to his contacts with the Church of Scientology. The memorandum can thus be regarded as notice. Only the memorandum of 11 December 2012 can be regarded as the required notice with regard to Pierre Migisha and Gisèle Mandaila. State Security should thus have notified the Minister sooner about these two latter individuals.

II.2.2. THE PHENOMENON ANALYSIS ON INTERFERENCE ACTIVITIES NOT DIRECTED BY THE STATE[128]

II.2.2.1. Content of the phenomenon analysis

The report in question was the fourth phenomenon analysis that State Security had drawn up. The Standing Committee I again emphasised[129] the usefulness of this type of report that *'explains a topical issue being a matter of interest and competence of an intelligence service and that constitutes a major political and social challenge, be it now or for the years to come. It endeavours to describe this issue with regard to its historical origins, ideology, organisation, structures and related activities. It contextualizes the challenges and risks, makes a 'risk assessment' for our politicians, for the administrative authorities concerned and for the judicial authorities that are also confronted with this issue*' (free translation).[130]

However, the Committee found that State Security management had not given the authors clear guidelines and had failed to define the objectives and methodology. The purpose of this phenomenon analysis was only briefly

[128] The issue of notifying the Minister of Justice in case of intelligence activities relating to political representatives was included in the 'transversal investigation' (II.4).

[129] STANDING COMMITTEE I, *Activiteitenverslag 2012* (Activity Report 2012), 14–28 (II.2 Monitoring of foreign intelligence services in relation to their diaspora in Belgium).

[130] From 'Extrémisme islamique en Belgique, Analyse du phénomène' by State Security.

described in the introduction. '*With this phenomenon analysis, State Security is trying to sketch a picture of the interference activities of groups and/or organisations in political and economic centres*' (free translation). State Security also pointed out that every organisation has the right to lobby in order to promote its objectives. However, according to State Security, if contact is made with people who hold positions of responsibility in order to influence decision-making processes or exercise an influence, the grey area of lobbying is exceeded and there may be 'interference' within the meaning of Article 8(1)(g) of the Intelligence Services Act.

The Committee also criticised the fact that the report failed to clearly[131] describe the strategy used by the Church of Scientology to 'influence decision-making processes with unlawful, fraudulent or clandestine means' (Article 8(1)(g) of the Intelligence Services Act). Likewise, neither the actual objectives of the organisation nor the way in which it made and maintained contact was examined. The Committee therefore found it worthwhile to recommend explaining in such an analysis, by way of example, how recruitment can occur: initial contact(s) by a middleman, approach of Members of Parliament, approach via organisations that do not disclose their relationship with the Church of Scientology, offering benefits or assistance (e.g. participation in courses or financial aid for projects), etc.

However, the Committee was particularly critical about how names of current and former political representatives and their employees were so widely mentioned.[132] Even if some names appeared several times and the involvement of some people was explained in further detail, the impression was nonetheless created that all persons mentioned had to be placed on the same level and had the same intelligence value. The Committee pointed out that being mentioned by name in a State Security report had a 'stigmatising effect', even if this report were distributed on a limited scale.

The Committee emphasised that if the summary of names was meant to demonstrate the scope of the contacts of the Church of Scientology and its activities, it was essential to specify the correct connection between a certain person and that church: whether there were one or more attempts at making contact, were these attempts successful, in which context did they occur, did the party involved participate passively or actively in activities (e.g. by giving a speech at a conference), was the party involved aware that the activities were organised by the Church of Scientology, etc. In other words, if State Security considers it necessary to mention names – and that is its responsibility – it must indicate the degree of involvement of each person in the report.

---

131 It is sometimes implicitly clear which strategy is being followed. The authors of the analysis possibly relied too much on the hypothesis that this was evident to the reader.

132 The Committee found that the authors of the analysis had decided to mention names without any involvement from management. The Standing Committee I questions this decision.

However, if the intention is to demonstrate the development of the Church of Scientology's activities and illustrate in detail that a well-defined strategy of making contact and recruitment is being followed (i.e. if they wish to describe a phenomenon), it is not necessary to mention names. In that case, abstract examples showing how and where the Church of Scientology is recruiting members and expanding networks will suffice.

II.2.2.2. Addressees of the phenomenon analysis and their 'need to know'

Besides internal distribution within State Security itself, the phenomenon analysis was sent to 33 people.

Prior to the distribution, State Security contacted the National Security Authority to check whether the addressees had security clearance at the required level. This turned out to be the case, with one exception.[133] State Security had each addressee or his security officer sign for receipt as required. In the cover letter to the phenomenon analysis, State Security also stressed the need to strictly observe the Classification Act and the serious prejudice that could follow from the inappropriate use of the report.

The Standing Committee I found that there was no existing list of the addressees for this type of analysis: it was left up to the discretion of the authors to decide who would and would not receive a report. The hierarchical authority did add a few names in this case.

It goes without saying that the wide distribution resulting from this increased the chances of a leak. However, the Standing Committee I emphasised that person(s) at the source of the leak is/are chiefly responsible (obviously on the assumption that the leak was intentional or that information reached the press due to negligence) for the adverse consequences of this for State Security and the political representatives mentioned.

The Committee felt that the list of the addressees had not been carefully thought out. In other words, State Security referred in general terms to the 'statutory power' of certain people (particularly the Prime Minister, the Deputy Prime Ministers or the ministers that are part of the Ministerial Committee for intelligence and security) or, more specifically, to their assumed 'need to know'. However, the problem with this is that the question of who has a 'need to know' depends on the purpose of the product being distributed. In other words, is the aim to inform people about a general phenomenon of interference, or is the aim to focus attention on precise risks that a person or institution may be confronted with in relation to their position? The Committee held that it was not necessary to provide the entire report in the latter case. On the contrary, it was appropriate at that time to limit the information to what is useful for a particular addressee.

[133] One addressee did not have security clearance and thus did not receive a copy of the phenomenon analysis.

However, if the report is intended to inform people about a general phenomenon, sending the full report is justified. The question which then arises is whether State Security is entitled to send such a report to fourteen officials/diplomats of FPS Foreign Affairs. The Committee questioned whether it would not have been more appropriate to send reports to a single addressee who, as the point of contact within that department, could determine the 'need to know' status of each of his colleagues.[134]

In specific reference to the interference phenomenon analysis, the Committee held that it would have been more appropriate to distribute the report in a more focused manner, based on the needs of each addressee. This would have probably limited the adverse consequences of the leak.

II.3. AN INFORMANT WITHIN THE VLAAMS BELANG?

At the start of 2013, two secret State Security reports were made public (see II.2). In the ensuing parliamentary debates, the Minister of Justice explained that '*it is not the task [of State Security] to monitor individual Members of Parliament. That is not the assignment of that service and also does not happen in practice*' (free translation).[135] Bart Debie, the former police commissioner of Antwerp and former security adviser of Filip Dewinter (Vlaams Belang), felt he needed to contradict this. He stated in a newspaper article[136]: '*I am not aware of what they do with other politicians. However, State Security has followed Vlaams Belang with great interest for years. And I am in a position to know this, because I was involved in it myself*'(free translation). Debie revealed that he had been a State Security informant from 2007 to 2010 – the period during which he was a spokesman/security adviser for Vlaams Belang. This evoked strong reactions from Filip Dewinter, the Minister of Justice and administrator-general of State Security.

Shortly before this, the Standing Committee I had started a general themed investigation into the monitoring of political representatives.[137] Nevertheless, the Committee decided to focus on this specific case and conduct a 'sub-investigation' into State Security's contacts with Bart Debie and the resulting information, especially with regard to Filip Dewinter. The existence and extent of any monitoring of Vlaams Blok/Belang through the years is examined first.

---

134 State Security is reported to have recently decided to work via one point of contact in future.

135 *Annals* House of Representatives 2012–13, 7 February 2013, CRIV53COM666, 9 *et seq.* Further: '*[…] I repeat it does not fall under State Security's remit to monitor Members of Parliament by reason of their position*' (free translation).

136 J. VAN DER AA and T. LE BACQ, *De Standaard*, 11 February 2013, I*k was de mol binnen Vlaams Belang* (I was the mole within Vlaams Belang).

137 See *infra* 'II.4. The monitoring of political representatives by the intelligence services'.

II.3.1. MONITORING OF VLAAMS BLOK, LATER VLAAMS BELANG

Pursuant to Articles 7 and 8 of the Intelligence Services Act, State Security is authorised to monitor extremism[138] when it constitutes or could constitute a threat for the internal or external security of the country. Monitoring politicians or political parties is therefore possible from this perspective. However, any such monitoring must obviously comply with Constitution, the ECHR, and the case law of the European Court of Human Rights in relation to freedom of expression and freedom of association.

Until the mid-nineties, the Vlaams Blok was systematically included in the 'list of subjects'. It no longer appeared on the lists of 1996 and 1999.[139] There should therefore have been no further monitoring during that period.

That situation changed when the incumbent Minister of Justice in 2001 gave instructions to State Security to regard Vlaams Blok as a subject again in accordance with the Act of 30 November 1998, except for the activities of political representatives in the ~~context~~ of their parliamentary mandate. The exercise of such a mandate was defined as '*expressing an opinion, parliamentary questions and hearings, submitting a legislative bill, in short whatever happens in the parliamentary context'* (free translation). In an internal directive of July 2001, State Security defined the parameters of this ministerial directive: the intelligence gathered and processed about Vlaams Blok had to relate to all individual and group activities that related directly to extremism, as defined in Article 8(1) of the Intelligence Services Act. Activities that were not extremist in nature were therefore not monitored as such. The focus needed to be on active, extremist militants.

In 2003, State Security – in a particularly well-reasoned memorandum – asked the Prime Minister in his capacity as the chairman of the Ministerial Committee for intelligence and security to remove Vlaams Blok from the list of subjects to be monitored. This request went unanswered. In 2004, Vlaams Blok became Vlaams Belang. Even so, this did not give cause for State Security to ask the competent authorities again about their position on whether or not to monitor the party. Vlaams Blok (*sic*) therefore still appeared on the 'List of subjects' for 2006.

State Security stopped making a 'list of subjects' in 2009. An annual 'action plan' has been drawn up since, which must be approved by the Minister of

---

138 Extremism is defined as '*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 other basic aspects of the constitutional state* (Article 8(1)(c) of the Intelligence Services Act).'

139 It was not necessary at the time to draw up a new list every year.

Justice. The phenomena and groups to be monitored[140] are listed in that plan and subdivided into 'active monitoring'[141], 'reactive monitoring'[142] or 'no monitoring'.[143] Under the heading of 'reactive handing' in the 2010 Action Plan, for example, reference is made to *Extreme Right Nationalist and/or identity movements (…) Dutch-speaking: Vlaams Belang'*. The 2011 and 2012 Action Plans refer to '*Vlaams Belang – internal party functioning and national positions*' (free translation), but under the 'no monitoring' heading. The party is no longer mentioned in the 2013 Action Plan. The heading 'no monitoring' is no longer included.

II.3.2. CONTACT BETWEEN BART DEBIE AND STATE SECURITY

The first contact between Bart Debie and State Security was at Debie's own initiative. In mid-August 2010[144] he sent an e-mail to State Security offering his services because he '*had received instructions from a very well-known politician that far exceeded the boundaries of criminal law*' with which he '*did not and could no longer ethically reconcile himself*' (free translation). Five subsequent meetings took place and e-mails were repeatedly exchanged until July 2012.

Bart Debie provided information about foreign contacts and planned trips of Filip Dewinter; about his position within Vlaams Belang and the power relationships within the party; about his 'sponsors' and those of Vlaams Belang; about an international conference for which Vlaams Belang took care of the practical organisation; about the connections between Vlaams Belang and a number of other extreme right organisations; about the terrorist attack of the

140 But never individuals as such.

141 This means that State Security actively develops activities to acquire, expand or strengthen the intelligence position.

142 'Reactive monitoring' means that State Security develops activities to acquire, expand or strengthen the intelligence position, but only in response to an express request for that purpose.

143 'No monitoring' means that State Security does not guarantee monitoring or, if requested, cannot comply with an external request for intelligence. It relates to those problems where the service is aware of the need for monitoring and/or investment, but there is an inadequate intelligence position and no actions can be planned because of a lack of capacity. This does not mean, therefore, that State Security cannot receive, gather or save intelligence about these themes, but that State Security does not explore these in further depth and the monitoring thereof is merely occasional.

144 It was initially reported in the press that Bart Debie was already in contact with State Security in 2007. However that is not what the Standing Committee I's investigation revealed. Perhaps there was a misunderstanding: during his contact with the press, Debie referred to things that had happened in 2007, but which he only reported in 2010. The journalists have also since acknowledged that they might have been inaccurate (T. NAEGELS, *De Standaard*, 27 February 2013 (Welles-nietes-nieuws).

Norwegian Anders Breivik in 2011[145] and about the visit of American businessmen and senators to Europe, whose delegation Filip Dewinter received in Antwerp. Obviously the facts that formed the basis for the contacts (alleged illegal activities) were also discussed.

Sporadic e-mail traffic was also exchanged in which Bart Debie mentioned nothing of significance. After some time, neither party pushed for further meetings. Lastly, Bart Debie mentioned in July 2012 that he had information about 'a leak at the public prosecutor's office'. A meeting was arranged but he did not attend it. There was no further contact after that date.

The Standing Committee I held that State Security had remained within the confines of its annual action plans with these contacts. The 2010 Action Plan provided for 'reactive' monitoring of the extreme right and Vlaams Belang, which meant that State Security could develop activities to respond to a specific event or development. The Standing Committee I was of the opinion that the information that it initially seemed Bart Debie would give – about '*instructions that far exceeded the boundaries of criminal law*' (free translation) – therefore justified taking him up on his offer. Furthermore, given his status within Vlaams Belang and his knowledge of extremism, such a source could not simply be ignored. Vlaams Belang was included under the 'no monitoring' category in the 2011 Action Plan. However, this did not mean that State Security could not receive any further intelligence regarding this theme. Since very little information was recorded that year relating to Vlaams Belang, this monitoring was also in accordance with the action plan. Contact with Bart Debie came to an end in 2012. Vlaams Belang was still included under the 'no monitoring' heading in the action plan of that year.

The Committee also found that State Security had complied with the instruction of 15 May 2001 in its relationship with Bart Debie: it had not gathered any intelligence related to the exercise of the parliamentary mandate as such (expressing an opinion and activities in Parliament) of Filip Dewinter or other parliamentarians.

The Standing Committee I was generally of the opinion that the manner in which State Security prepared for and had contact with Bart Debie could not or could hardly be criticised. For example, the objectives of the intelligence-gathering (such as the intentions of Bart Debie, the alleged illegal activities of Filip Dewinter and the 'covert' financing channels of his party) were clearly explained by the Analysis Service and followed up by External Services. There were several express reminders that the intelligence gathered had to be in connection with activities related to, or that could relate to, extremism. The

[145] Reference was made in Breivik's manifest to Belgian individuals and the document was also sent to a number of Belgians, including a Vlaams Belang Member of Parliament. State Security wanted to know whether there were any links between the Norwegian perpetrator and the cited Belgian names.

information had to be able to contribute, for example, to detecting and analysing extremist (xenophobic or racist) tendencies within Vlaams Belang and not to the exercise of the parliamentary mandate as such of Filip Dewinter or other parliamentarians. This was also made clear on several occasions to the source. Although the reports do mention the names of Vlaams Belang Members of Parliament, this is not in relation to their parliamentary activities. Reference is seldom or never made to the capacity of Member of Parliament. However, the Committee did conclude that the employees of State Security could not always adequately describe the limits of their actions in relation to political representatives, even if they did have a good intuitive feel for those actions. The boundaries set in the directive with respect to the information to be gathered in relation to a politician were not very clear.

Lastly, the Committee also concluded that the actual circumstances under which the source was met were normal. He was not given any financial benefits, only a small gift. Bert Debie also raised personal problems during the discussions. He could not obtain accreditation to give courses to paramedics and asked early on whether he could be considered eligible for rehabilitation for a previous conviction. The relevant commissioner of State Security let his source know that according to the person he contacted no exceptions would be made. He furthermore only gave him information that was also accessible to the public.

II.3.3. FILIP DEWINTER IN STATE SECURITY'S DATABASE[146]

State Security obviously already had information relating to Filip Dewinter before its contact with Bart Debie.[147] His name was in State Security's data system, which has been operational since 2001[148], linked 214 times to specific topics such as 'extreme right', but also 'salafism' or 'radical Islam'.[149] The reports that were drafted following contact with Bart Debie[150], were also included in the database and linked in this case to 'Extremism' and 'Extreme Right Dutch-

146 A large dossier could be seen on the desk of the administrator-general of State Security during a media interview of 11 February 2013. The name 'Dewinter Philip' was on the cover. The Committee found that this related only to a folder with procedural documents, correspondence, and memoranda relating to the many proceedings that Dewinter had conducted to gain access to his file at State Security.

147 GISS also had information and intelligence relating to Filip Dewinter, but to a far lesser extent than State Security. The Dewinter 'dossier' at GISS was old, not kept in very systematic order, and mainly comprised information from open sources.

148 In the IT system that was operational before 2001, Filip Dewinter's name appeared in 459 documents. The Committee did not include these documents in its investigation, partly because the information in them was outdated.

149 A link could mean that one is involved in a phenomenon or that one is a victim.

150 Because this relates to a human source and given the delicate nature of the case, the information arising from the contacts was included in a so-called 'operation'. In this way,

speaking'. 156 of those cases involved a 'pertinent link'; 55 cases were a link 'for info'; three links were 'to be determined'. The Committee asked questions about the correct meaning of these concepts[151] and their specific application in the field.

In addition to linking a name to a certain topic, there are also what are known as operational links, by which a link is made between two names and the relationship between them is classified as 'friends with', 'opponent of', 'acquaintance of', 'sympathiser of', etc.

The Committee did not feel it had to deduce from its analysis that State Security had an exaggerated focus on the subject. From the relatively small number of operational links that were made between Filip Dewinter and third parties – a total of 50 in twelve years – it appears that State Security worked very prudently and did not expand any significant 'intelligence position' with regard to the subject. The Standing Committee I was of the opinion that State Security had acted timidly in this regard in the past.

II.3.4. REPORTING TO THE MINISTER OF JUSTICE

Two directives were important with regard to reporting to the Minister of Justice whenever political representatives were monitored by State Security.[152] Firstly, there was the instruction of the Minister of Justice of 25 May 2009 on referring reports of federal Members of Parliament. Secondly, there was the internal instruction of 27 March 2012 relating to ministers, Secretaries of State, and elected persons at federal, community, and regional level. On 8 July 2010, the subject became Community Senator, which meant that both directives applied to the information that arose from the contacts with Bart Debie. However, with one exception, they were not followed with regard to information about Filip Dewinter.

II.4. MONITORING OF POLITICAL REPRESENTATIVES BY THE INTELLIGENCE SERVICES

Just like the investigation into '*Confidential memoranda about Scientology in the press*' (II.2) and '*An informant within Vlaams Belang?*' (II.3.), this investigation was also the result of the same two classified memoranda of State Security

only people who are expressly authorised to know of a specific operation have access to State Security's database.

151 Also see II.4.2.3.

152 Also see Chapters II.2.1.3 and II.4.2.1.3.

distributed in the press. In the parliamentary debates that followed the publication, the question that was repeatedly asked was whether, and to what extent, Belgian intelligence services may monitor political representatives and which rules they must observe in that regard. The Committee then decided to open a themed investigation '*into how the intelligence services gather information about political representatives, how they deal with and analyse this information, and how they report thereon to the competent authorities*' (free translation).

It was moreover not the first time that the Standing Committee I had investigated the activities of the intelligence services in relation to political representatives.

In 1997, an investigation was opened into '*how the intelligence services distinguish between the activities of MPs as environmental pacifists and as Members of Parliament*' (free translation).[153] The investigation followed a question by an Ecolo Member of Parliament and focused on the intelligence that State Security and GISS possibly gathered about political representatives of Ecolo or Agalev (now *Ecolo-Groen*). The Committee reached the conclusion that the services had dossiers in the name of a number of Members of Parliament of these parties, but that the activities of these people had not been specifically monitored since 1988.

A year later, in 1998, the Standing Committee I started a more general inquiry, as a corollary of that investigation, on '*the gathering of information about Members of Parliament by the intelligence services*' (free translation).[154] This investigation related to the representatives of *all* political parties. The Committee reached the conclusion that '*neither State Security nor GISS initiated any investigation into actions performed within the framework of the actual exercise of the parliamentary mandate*' (free translation).

Lastly, in 2006, the so-called 'reserved dossiers' at State Security came up for discussion.[155] Apparently, the 'General Affairs' department of State Security, had kept a number of dossiers with information about elected persons outside the 'normal circuit' since the end of the eighties. Some of these dossiers were even kept exclusively at the secretariat of the incumbent administrator-director-general of Public Safety. The Committee decided in this investigation that '*the current presence of political representatives and prominent persons in the now digitised reports of an intelligence service remains an extremely delicate issue. However, the Committee was of the opinion that the capacity of a prominent person or politician must not be an obstacle to adequate monitoring and a corresponding availability of the relevant reports in the light of the performance of the legal assignments of an intelligence service. After all, this activity must take place 'irrespective of the persons*' (free translation).[156] As a corollary of this, the

153 STANDING COMMITTEE I, *Activiteitenverslag 1998* (Activity Report 1998), 67 *et seq.*
154 STANDING COMMITTEE I, *Activiteitenverslag 1999* (Activity Report 1999), 12 *et seq.*
155 STANDING COMMITTEE I, *Activiteitenverslag 2008* (Activity Report 2008), 23 *et seq.*
156 STANDING COMMITTEE I, *Activiteitenverslag 2008* (Activity Report 2008), 30 *et seq.*

Committee made the following recommendation: *'More generally speaking, the Standing Committee I wants State Security to develop clear and unambiguous guidelines with regard to the collection, processing, consultation (including the internal compartmentalization, if any), storage, and archiving of data regarding certain categories of persons who have or had special responsibilities. For the development of these guidelines and the actual monitoring of (former) political representatives, State Security must take into consideration the guidelines outlined in the judgement of the European Court for Human Rights in the case Segerstedt-Wiberg and Others v. Sweden'* (free translation).[157]

II.4.1. SOME FIGURES FROM THE NEW INVESTIGATION

On 1 March 2013 – not including double mandates – there were 479 people who were either ministers in the federal or regional governments or elected as a Member of Parliament of a regional or federal legislative authority. In its investigation, the Committee asked both intelligence services to check whether and to what extent the names of these people appeared in their paper dossiers and databases.

It came to light that the External Services of State Security had drawn up 727 documents from June 2010 (in other words, the start of the current federal legislature) until the start of 2013 in which at least one of the 479 political representatives were mentioned each time. A total of 142 political representatives were mentioned.[158]

The Analysis Service of State Security counted 423 documents over the same period in which 93 different political representatives were mentioned. A little more than half of these documents came from external sources (e.g. CUTA, the police or other correspondents); the other half were 'produced internally'. These were documents for internal use (summary memoranda with a status report in a specific dossier and minutes of meetings), documents intended for external parties (memoranda addressed to Belgian authorities and – just a few – to foreign

---

157 STANDING COMMITTEE I, *Activiteitenverslag 2008* (Activity Report 2008), 110–111. In the case of *Segerstedt-Wiberg and Others v. Sweden* of 6 June 2006, the Court questioned the acquisition and storage of data relating to political opinion, affiliations and membership of people, in light of Article 8 ECHR. The fact that such information, even though it concerns publicly known facts, is being collected or stored is a serious violation of privacy. According to the European Court of Human Rights (ECHR), this violation can be justified only if it is proportionate from the perspective of national security. In assessing this proportionality, the ECHR attached great importance to whether or not a political party was violent by nature. The assessment of such a violent nature may not be inferred solely on the basis of the political programme; it must also translate itself into the actions of the party leaders and the positions they adopt.

158 Some appeared in multiple documents: 37% of the political representatives were mentioned once, 35% were mentioned two to five times. Four political representatives appeared in more than 21 documents. One elected person was mentioned in 91 documents.

authorities) and 'written orders' in which the Analysis Service posed specific questions to External Services.

The Committee carried out a random check of these documents[159] and studied them to gain insight into the collection and analysis work of State Security with regard to political representatives (*infra*).

From its side, GISS[160] had information both on paper and digital carriers. For example, 115 sheets were available that corresponded to a paper dossier of a political representative. However, most of the accompanying dossiers were already destroyed. There were only 36 dossiers in the so-called 'live' archive and a further 12 in the 'dead' archive (meaning these had not been consulted for fifteen years).

The names of 109 political representatives were found in GISS's database. The Standing Committee I examined one-quarter of these dossiers. This showed, for example, that it was never stated whether or not a person was a Member of Parliament.

GISS did not draw up any assessment memoranda during the reference period that related specifically to ministers or parliamentary representatives.

II.4.2. MONITORING OF POLITICIANS THROUGH THE INTELLIGENCE CYCLE

The Committee went through all aspects of the intelligence cycle in its analysis of the selected dossiers, starting at 'managing the intelligence activities' to 'collection', 'organisation of the information' and 'analysis' until 'distribution of the intelligence'.

II.4.2.1. Managing the intelligence activities

The activities of the Belgian intelligence services are managed at various levels. The most general level is that of legislation – namely laws, decrees and general instructions – that stipulates what intelligence activities may be performed and how this may occur. Under this is the level of the annual action or intelligence plans which – on the recommendation of the services and approved by the competent minister – specifically stipulate which topics may or must be covered in the next year. Lastly, there is *ad hoc* management in specific dossiers by the head of service or competent minister. These three levels are discussed below.

---

159 One in every four dossiers was studied. An exception was made in this regard: the memoranda intended for foreign authorities were all included in the analysis.

160 More specifically, the C(ounter) (I)ntelligence Division which is authorised in respect of internal threats.

II.4.2.1.1. Rules applicable to intelligence gathering on political representatives

The Act of 30 November 1998 governing the intelligence and security service (Intelligence Services Act) does not contain any provision conferring a special status on a Member of Parliament. The Act moreover makes no reference to political representatives. The same applies to the Special Intelligence Methods Act of 4 February 2010, which does not provide for special protection for politicians, even though it does afford this to professional journalists, lawyers and doctors. From that perspective, the Committee repeated its statement from 2008, namely that the position of politician cannot preclude adequate monitoring and reporting. After all, intelligence work must take place 'irrespective of the persons'. However, any such monitoring must take into account the case law of the European Court of Human Rights in relation to freedom of expression and freedom of association. Interference in these fundamental rights in relation to political parties and representatives (even extreme ones) must be dealt with extremely carefully.

Because one realised that the monitoring of political parties or representatives is particularly sensitive, a special restriction was introduced in 2001 for the monitoring of the parliamentary representatives of what was then the Vlaams Blok party[161]: the ministerial directive of 15 May 2001, which gave the instruction to monitor the party, stipulated that this must be done to the exclusion of the activities that representatives performed as part of their parliamentary mandate. State Security defined this restriction further as follows: '*a parliamentary mandate*' is '*expressing an opinion, parliamentary questions and hearings, submitting a legislative bill, in short whatever happens in the parliamentary context*' (free translation).

Since then, this definition – in respect of which one may ask whether it was (still) sufficiently known, applicable outside the representatives of the party concerned and/or adequately pertinent and clear – has not been explicitly repeated, refined or qualified. The Minister of Justice returned to this in 2013 in her answers to several parliamentary questions: activities of a Member of Parliament '*within Parliament itself*', within the context of their '*parliamentary function*' or '*in their actions as a Member of Parliament*' may not be monitored by an intelligence service.[162] However, according to the Committee, even this 'specification', dated after the start of this investigation, does not eliminate all queries. After all, the distinction between the activities of a political representative within or outside of his or her mandate is difficult to uphold in practice. Certain aspects moreover fall outside the scope of this limitation (e.g. the role of a Member of Parliament in the internal functioning of the party and

161 See Chapter II.3 in this regard.

162 *Annals* Senate, 21 February 2013, no. 5–92, 16–18 and *Annals* Senate, 14 March 2013, no. 5–95, 17–19.

in determining party strategy), while these are a lot more 'sensitive' than simply asking a parliamentary question or submitting a legislative bill (while this information is public by definition).

The Committee therefore repeated the recommendation from its 'reserved dossiers' investigation[163] to develop ready and unambiguous directives for intelligence activities of specific categories of persons that bear or have borne special responsibilities.

The need for a comprehensive clear directive obviously also applies to GISS. After all, this service was at the time of the investigation still applying an instruction that dated from before the Act of 30 November 1998. A memorandum of 25 June 1998 explains that political representatives may not be monitored because of their mandate but that they, like any other citizen, may attract GISS's attention if they are part of an organisation that constitutes a threat to the assignments of Defence, or if they try to enter a military domain or obstruct the activities of Defence.

II.4.2.1.2. Inclusion of political parties in the annual action or intelligence plans

In 2013, none of the political parties represented in Parliament appeared any longer in the annual action or intelligence plans of State Security and GISS. Previously, certain parties were systematically mentioned as targets, in relation to State Security, sometimes at the express request of the competent minister (see II.4.2.1.1).

In 2013, none of the political parties represented in Parliament were monitored as such, although the Standing Committee I was of the opinion that ready and unambiguous directives needed to be developed.

II.4.2.1.3. *Ad hoc* management by the Minister of Justice: a means of applying the directive of 25 May 2009

On 2 May 2009, the incumbent Minister of Justice announced in Parliament that '*State Security will send the Minister of Justice a warning notice […], by way of information, each time that an active federal Member of Parliament is named or linked to specific material in a dossier, if he is the subject of threats towards his person, or if a foreign intelligence service shows interest in him*' (free translation).[164] Pursuant to this, the Minister approved an instruction on 25 May 2009 that was based on a State Security draft. This directive entailed the Minister receiving a '*warning notice*' '*if any current federal Member of Parliament is mentioned in a report* '*for information purposes*' *or is linked to a specific topic*

163 STANDING COMMITTEE I, *Activiteitenverslag 2008* (Activity Report 2008), 110–111.
164 STANDING COMMITTEE I, *Activiteitenverslag 2009* (Activity Report 2009), 3.

mentioned in a report, as an informative element, or is the subject of State Security attention, as a threatened individual or as the target of a foreign intelligence agent. These reports or connections must be made as part of exercising the powers of State Security. The notice will be sent to the Minister of Justice in the form of a 'SECRET – Act of 11.12.1998' classified memorandum for every federal Member of Parliament that is cited or linked in a report drawn up by State Security. […] State Security will continue its monitoring activity as normal (silent procedure), unless the Minister of Justice decides otherwise' (free translation).

In 2013, the incumbent administrator-general of State Security stated the following in this regard: '*The directive broadly covers three aspects. The most important new development is the immediate notice given to the Minister of Justice every time the name of an active federal Member of Parliament appears in a State Security report. By doing this, State Security and the Minister of Justice have alleviated the concern that arose among some federal Members of Parliament following the Standing Committee I's investigation into the so-called 'reserved dossiers*'' (free translation).[165] The administrator-general pointed out that this procedure also allows the Minister to assume responsibility by giving additional, punctual orders to State Security, if required. He can also supervise the intelligence investigation, if necessary, via the Standing Committee I. Lastly, receiving notice enables the Minister of Justice to answer questions from Members of Parliament that make use of their constitutional right of examination. According to the administrator-general, this meets the requirements of a parliamentary, democratic and constitutional state to be met.

In the opinion of the Standing Committee I, the administrator-general summed up the importance of the 2009 directive very well. The Committee had already given this instruction a positive response. In its Activity Report 2009, it stated that '*the concerns of the Standing Committee I expressed as part of the 'reserved dossiers' investigation have already been partly appeased in that way*' (free translation).[166]

However, since June 2010 (in other words, when the instruction had been in force for around one year), around 350[167] reports and memoranda have been drafted within State Security containing the names of then active federal Members of Parliament, while this was only reported in the prescribed form by way of exception. The fact that the instruction was hardly observed was also apparently never noted, reported, checked and/or seen as problematic within the service. The Standing Committee I also pointed out in its investigation that the

---

165 A. WINANTS, '*Control in the circus*. Internal control at State Security' in *Inzicht in toezicht. Twintig jaar democratische controle op de inlichtingendiensten*, (Insight into monitoring. Twenty years of democratic monitoring of the intelligence services) W. VAN LAETHEM and J. VANDERBORGHT (eds.), Antwerp, Intersentia 2013, 137.

166 STANDING COMMITTEE I, *Activiteitenverslag 2009* (Activity Report 2009), 3.

167 The 727 documents referred to in II.4.1 relate to representatives of both federal and regional governments and assemblies, while in this instance only federal representatives are involved.

directive *could* not be fully observed simply because State Security did not have a permanently updated list of all political representatives. It was therefore unavoidable that reports were sometimes drawn up about Members of Parliament without State Security necessarily being aware of their status.

In the course of the investigation, State Security introduced a number of changes to its work procedures, including notification of the inclusion of Members of Parliament in its reports. In its working document, State Security recommended that the Minister be informed monthly (and thus no longer immediately) if Members of Parliament were mentioned in Analysis Service (and thus no longer External Service) documents. These working documents resulted in a new instruction after the completion of the Committee's investigation (see Chapter I.1.3).

II.4.2.2. Collection

The Standing Committee I emphasised that most references to Members of Parliament in State Security collection reports were prompted either by the fact that the representative was the subject of a possible threat himself or that he had (by happenstance) been in contact with a person or group that is being monitored. The Committee did not find any indications that State Security targeted political representatives for reasons other than the interests and threats summed up by law.

The same conclusion could be drawn as far as GISS is concerned: the service showed no interest in political representatives as such. If GISS exceptionally paid attention to representatives, it was in relation to a military interest or military matter. Most of the GISS dossiers were moreover opened long before the politician concerned took up office. This also demonstrated that the 'political mandate' was not relevant for GISS's attention.

During its random check, the Standing Committee I only found one dossier at State Security from which it could be deduced that information was gathered about elements that possibly 'formed part of the parliamentary mandate' as described in the above-mentioned directive of 25 May 2001 and that occurred 'within Parliament itself' (albeit, in this case, in the Parliament of a Region). This relates to information that State Security had received about a meeting that a political party had organised with a foreign political movement that could have constituted a threat. This example showed the Committee again that the criteria summarised in the directive were unhelpful and impracticable. After all, firstly, political activities are not limited to Parliament itself and, secondly, there does not seem to be any good reason not to monitor threats that are prepared from within Parliament. The Standing Committee I was therefore of the opinion that these criteria needed to be reassessed.

However, the fact that the Committee did not find any elements that pointed to the illegal monitoring of Members of Parliament does not mean that the usefulness of all collected data was proved. The Committee could not ignore the fact that part of the information was rather 'trite': politician A first greets politician B before leaving; politician C attends a gathering at which thousands of people are present; politician D participates in a demonstration, but only joins at the end, etc. The link with one of the statutorily described interests and threats is therefore sometimes unclear at first.

The Committee is very much aware that it is not always immediately evident when intelligence is gathered what information will or will not turn out to be relevant. However, that does not negate the fact that the applicable requirements – such as those set out in the Intelligence Services Act and the Privacy Act (purpose limitation principle, adequacy, accuracy, etc.) – must be observed. Whether and to what extent specific information must be included in a collection report therefore forms a crucial fact. The Committee was of the opinion that the manner of the input should be a topic of permanent training as well as real quality monitoring. The Committee emphasised in the same context that it must be evident from a report whether a person is a 'victim', 'actor' or 'passer-by' in relation to a specific threat.

II.4.2.3. Organisation of information

State Security's database obviously contains a host of data about people, groups, places and events (entities). In order to facilitate the use of this data, it is linked to one or more of the statutory threats to be monitored, such as extremism, proliferation, interference, etc. This is called 'motivation'. Four types of links are possible: 'For info', 'To be determined', 'Pertinent link' or 'Operational link'. A 'Pertinent link' indicates that the connection with one of the threat topics is specific and abundantly clear.[168] The 'To be determined' link is when it is not yet clear whether or not there is a pertinent link. However, the precise scope of the other two links is less clear. 'For info' is described as a *'link for entities that have no connection with one of the topics or threats dealt with by State Security'* as well as *'a link that indicates an involvement that is passive or not yet classified (for example as the subject of the threat)'* (free translation). The Committee therefore

[168] In accordance with the directive of 27 March 2012, ministers and political representatives in office may be the subject of a 'pertinent link' only if the information from the report shows that they are actively involved in a threat against the continued existence of the democratic and constitutional order. They may be the subject of a 'link for info' if it is clear from the information in the report that they are the subject of a threat or actively involved in a threat against one of the other matters on which State Security is gathering intelligence. When the author of a report believes on the basis of the information in that report that a pertinent link or for info link must be made for a minister or a political representative, he must consult in this regard with the head of his section.

concluded that these concepts are not described and applied unambiguously. Intelligence work is thus at risk of losing efficiency and effectiveness. After all, there is a risk that not all the correct reports will 'come to the surface' when this is necessary for the purpose of assessment work. Incorrect conclusions may thus be drawn. The Standing Committee I was therefore of the opinion that State Security urgently needs to reassess these concepts. The service should also incorporate the possibility of indicating the role or assumed role of a person mentioned in the report in relation to the threat as being a 'passer-by', 'potential victim', 'key figure', or 'actor', etc.

II.4.2.4. Analysis

The Standing Committee I found no indications that the analysis services of either intelligence service had unlawfully paid attention to ministers and parliamentarians.[169] It had already been shown in two previous investigations (see II.2 and II.3) that State Security was aware of the delicate nature of the intelligence work in relation to political representatives. The same applied to the Analysis Service of GISS-CI.

The Committee did however note that the Analysis Services should pay the necessary attention in their reporting to the 'position' of a person mentioned in the report in relation to the threat ('victim', 'actor', 'passer-by', etc.)

II.4.2.5. Dissemination of intelligence

The Committee found that GISS had not disseminated any documents in the reference period to the other services in which the name of a minister or parliamentarian was mentioned.

In contrast, State Security did send such memoranda to Belgian authorities. However, the Committee pointed out that it was indeed a core task of this service to notify competent authorities whenever someone was the subject of a threat or cooperated in a threat themselves (Article 19 of the Intelligence Services Act), even if that person was a Belgian politician. The need to know and requirements of the aforementioned Article 19 of the Intelligence Services Act must provide guidance in the dissemination of this intelligence. The Standing Committee I already stated this in an earlier investigation.[170] This principle and this statutory provision apply regardless of the addressee: public prosecutor's office, federal

[169] The Committee found a report that contained information relating to 'parliamentary activities in Parliament' in only one dossier. The information was recorded by a State Security employee who was invited to attend a closed meeting of Parliament. The report was intended for the Minister of Justice. The Committee again asked whether it could be that such reporting should not be permitted. The Committee found that it was up to the competent minister to make a decision in this regard.

[170] See Chapter II.2. 'Confidential memoranda on the Church of Scientology in the press'.

public services, Prime Minister and portfolio ministers, ministers from the regional governments, the King as Head of State, etc., but also obviously if a foreign service is the addressee. The Committee was able to conclude in this regard that State Security showed the necessary restraint when it came to sharing these reports with foreign services. This restraint manifested itself in various ways: the limited number of communications, the nature of the information, and the countries with which this information was shared. Even so, the Committee emphasised that there must always be a careful assessment of whether the names of Belgian political representatives (as well as ordinary citizens) can be mentioned in documents intended for foreign services. The principle of need to know and the requirements of Article 19 also provide guidance in this regard. However, other requirements, such as those in the Privacy Act, also play a role in passing on personal data abroad. The Standing Committee I again emphasised the need in this regard for the Ministerial Committee for intelligence and security to further define the scope of Article 19 of the Intelligence Services Act.

II.5. THE INTELLIGENCE POSITION OF STATE SECURITY IN RELATION TO AN INTERNATIONAL TRANSACTION OF A BELGIAN COMPANY

II.5.1. COMPLAINT ABOUT A REFUSED EXPORT PERMIT

At the end of 2011, the representatives of a firm incorporated under Belgian law that was specialised in the production of highly technical equipment complained about the refusal of the competent minister to grant them an export permit for isostatic hot presses.[171] However, the destination country was a party to the non-proliferation treaty.[172] The complainants also stressed that the firm had previously been granted an export permit for the same product to the same country. They alleged the refusal was the result of pressure that a foreign country was putting on the Belgian authorities. According to the complainants, this constituted interference and had an adverse effect on their economic interests.

At the start of 2012, the Standing Committee I decided to open an investigation into State Security's intelligence position relating to this transaction

171 An isostatic hot press is a machine that reinforces the resistance and durability of some materials by placing them in their heated state under very high pressure. These presses are used in the aircraft industry but can also be used in the production of rockets and nuclear weapons. It is a dual use product, i.e. it can be used for civil and/or military purposes, whose export is subject to the control measures provided for in Directives 1334/2000 and 428/2009 of the Council of the European Union.

172 'Treaty on the non-proliferation of nuclear weapons'
see: www.un.org/disarmament/WMD/Nuclear/pdf/NPTEnglishText.pdf.

both with regard to combating proliferation and protecting the scientific and economic potential of the country.[173]

It was also the third investigation of the Committee involving this firm. An investigation was already held in 2005 into how State Security had processed information from a foreign service relating to the export of isostatic hot presses to Iran.[174] The Standing Committee I concluded on that occasion that State Security had been rather nonchalant in its handling, assessment and dissemination of this information.

A second investigation into how the firm was monitored by State Security was completed in 2011.[175] It was concluded that while the service had attentively monitored some transactions with one or more sensitive countries, this monitoring had been mainly reactive and *ad hoc*, based solely on information provided by foreign intelligence services. It was, however, positive that State Security did not focus solely on security interests relating to the development of chemical, biological or nuclear weapons, but also the issues of competition and identifying signs of possible foreign interference.[176] In this regard, the Committee, just like State Security, was of the opinion that security interests must take precedence over the economic interests of a company when combating proliferation.

II.5.2. FINDINGS

State Security was notified about the planned export of an isostatic hot press by the secretariat of the Advisory Committee for the Non-Proliferation of Nuclear Weapons (CANVEK)[177] on 1 February 2011. After all, the dossier was already on the agenda of CANVEK's next meeting, to be attended by a State Security analyst. State Security wondered why the firm itself had not informed it about the planned export earlier. The service had already had contact twice with an executive of the firm in January 2011 for the purpose of exchanging information

---

173 The Committee questioned not only State Security for this purpose but also two important actors in relation to Belgian non-proliferation policy, namely Théo Van Rentergem, chairman of the Advisory Committee for the Non-Proliferation of Nuclear Weapons (CANVEK) and Werner Bauwens, FPS Foreign Affairs special envoy for disarmament and non-proliferation. The final report was approved in November 2013.

174 STANDING COMMITTEE I, *Activiteitenverslag 2005* (Activity Report 2005), 8–27.

175 STANDING COMMITTEE I, *Activiteitenverslag 2011* (Activity Report 2011), 37–40.

176 State Security's analyses usually relate to the protection of scientific and economic potential as well as proliferation. However, it is not CANVEK's duty to consider the economic aspects related to the dossiers that are submitted to it.

177 See more about the composition and powers of this Committee: Royal Decree of 12 May 1989 on the transfer of nuclear materials, nuclear equipment, technological nuclear information and derivatives thereof to non-nuclear states (Belgian Official Journal of 15 June 1989) and the Internal Regulations of the Advisory Committee for the Non-Proliferation of Nuclear Weapons (Belgian Official Journal of 8 February 2010).

about any sensitive dossiers that would be submitted to CANVEK. According to the Committee, these contacts indicated that State Security had meanwhile adopted a more proactive approach towards the firm concerned. However, since the firm had failed to notify State Security in this case, the monitoring in this dossier was reactive again.

Immediately after State Security was informed of the planned transaction, a few verifications were carried out at foreign partner services. The information of these correspondents as well as the contextual elements from an open source analysis resulted in a summary memorandum about the situation at the firm. This memorandum was sent to the Minister of Justice at the start of 2011.

In March 2011, State Security also sent two classified memoranda to CANVEK and FPS Economy. In these memoranda, the service set out the information which indicated that the end user of the hot presses could be connected to an entity that had previously been involved in a military nuclear programme.

State Security pointed out to CANVEK in the meetings that this was a sensitive export dossier. In the absence of more accurate information, its careful and balanced analysis was based mainly on hypotheses and assumptions.[178] It appeared from information presented by other committee members that the authorities of the destination country were reticent about providing additional information and about allowing an on-site inspection of the isostatic press after its delivery.

Given the doubts concerning the definitive recipient of the hot presses and control over their use, CANVEK did give a favourable export opinion on 16 June 2011, but on condition that the client provide additional clarification and that the authorities of the country concerned could give guarantees regarding an inspection visit.

As he was also of the opinion that the foreign authorities concerned were offering inadequate guarantees for the on-site visit, the competent minister refused the export permit. He returned the dossier – including the opinion that he had received from a foreign authority – to CANVEK.

State Security asked the relevant correspondent to provide additional information about the opinion sent to the competent minister by the foreign authority.[179] However, the answer received by the service was very 'minimalistic'. It did not enable State Security to supplement or refine its original analysis.

---

178 According to the director of CANVEK, the memoranda that State Security sent to CANVEK usually included hypotheses and assumptions and seldom established facts. It is therefore rather difficult to find the essence of the formal grounds for its advice. There are many reasons as to why nothing certain can normally be stated. State Security refers to the very technical nature of the topic, the complexity of the supply networks, the difficulty of obtaining precise and updated information about current programmes, the lack of access to the financial data of these networks, and this in view of the limited human resources that it can assign to this case.

179 State Security later referred to this opinion as '*laconic and negative*'.

In August 2011, the foreign client apparently agreed to an unconditional right of access to the hot press. But since not one Belgian authority could commit to the on-site inspection visit, CANVEK issued an unfavourable opinion on the export on 17 October 2011.

State Security explained that the information sent by the foreign authority directly to the competent minister had played a decisive role in the review of CANVEK's opinion. Although State Security never excludes the possibility of a protectionist reflex from a foreign country if that country has competing companies or industries, it did not see any attempt in this case to influence economic competition. The negative opinion was rather prompted by a general distrust of this foreign government in relation to certain export transactions to that country and by the fact that the Belgian authorities could not exercise any effective control over the end user. State Security also emphasised that it had no option but to rely on the foreign intelligence service concerned, more specifically for the purpose of investigating a foreign company in a reputable high-technology sector. Moreover, the foreign authority concerned appears on the Entity List of the US Department of Commerce. This means, for this administration, that exports to the entity concerned must be subject to stricter conditions.

The Standing Committee I therefore concluded that State Security could not be blamed for any dysfunction or unlawfulness in this dossier.

The Committee did however ask whether and how the introduction of an on-site inspection system at end users abroad could strengthen analysis and control capacities in relation to the proliferation of weapons of mass destruction in an international context. Regardless of the jurisdiction that this control system is brought under (regional, federal or even European), such an assignment may not be confused with promoting the economic interests of the country.

II.6. ALLEGED CRIMINAL OFFENCES BY A FOREIGN INTELLIGENCE SERVICE AND STATE SECURITY'S INTELLIGENCE POSITION

The Standing Committee I received a short e-mail in January 2010. The author – a foreign national – alleged that a foreign government had organised the abduction of his family in foreign territory. The Committee stated that it did not have jurisdiction because there appeared to be no link to its powers. It did however send a copy of the e-mail to the judicial authorities and State Security.

The man submitted a new complaint in early December 2011. He also lodged a civil complaint with the examining magistrate. The Committee then decided to open an investigation '*into State Security's intelligence position relating to facts stated in a complaint from a foreign national to the Belgian judicial authorities*

against agents of a foreign intelligence services'. After all, new information pointed to a link with its assignments. This investigation was opened in January 2012 and closed at the start of February 2013.

The complainant was employed at an embassy abroad. He stated that in 2003 he noticed those responsible at the embassy and others who worked for foreign intelligence services were in regular contact with individuals who defended an extremist, even violent, Islam. Since his superiors would not listen to him, he decided to inform the media. He also asked immediately for political asylum and obtained a residence permit.

In October 2006, he alleges that he brought his family under threat to Brussels and then put them on a flight to his homeland.

State Security had been made aware of the alleged facts since mid-January 2010 by the Committee (*supra*). At the end of January, the service also received a report from the Belgian ambassador in the complainant's country, who had been in recent contact with him. The ambassador did not comment on the merits of the case, but indicated that it would be useful for the security services to institute an investigation. After all, the ambassador did not completely rule out that there had been an attempt to compromise the embassy. State Security carried out a number of investigative acts[180] that resulted in a concise intelligence report. It drew no conclusions about the veracity of the story. It also did not analyse whether the case might have been fabricated to cause harm to Belgian diplomacy. State Security did not deem it necessary to draw up an evaluation memorandum for third parties '*given the poorness and non-relevance – in terms of intelligence – of the information collected*' (free translation). The ambassador in question was not kept advised of the follow-up by State Security to his letter. According to State Security, this was because it never received an 'official' enquiry from FPS Foreign Affairs about this.

In mid-August 2011, the complainant and his family managed to flee the country.

At the end of October 2011, he submitted a complaint to the examining magistrate based on the offences of abduction, unlawful deprivation of liberty, aggravated assault committed abroad against persons that were probably part of a foreign intelligence service. He repeated his complaint later, but then to the Standing Committee I.

During February 2012 and only after having been informed by the Committee of the opening of an investigation and the complaint lodged with the examining magistrate, State Security contacted the competent public prosecutor's office. The public prosecutor's office was not yet aware of the complaint.

---

180 Consulting open sources, a request for information to a corresponding foreign service, a verification (that proved to be negative because the person involved was not yet known to State Security in 2010), etc.

State Security proceeded with new verifications in April 2012, but these did not produce any evidence.

State Security regarded all aspects of this case as implausible. The documents and information provided by the complainant, as well as the formulation and manner in which it was sent, gave rise to serious doubts about their veracity. This was also because the information obtained from the foreign correspondent did not produce any relevant information, according to State Security, that would have justified an in-depth analysis and sharing of information with a Belgian or foreign partner.

State Security consequently decided that this case was not relevant in the context of intelligence work: *"After all, denouncing an abduction or lodging a complaint to a court has a judicial or police character. It does not fall within the legal competence of the VSSE"* (free translation).

The Standing Committee I shared State Security's position in the sense that the handling of a judicial or political dossier obviously does not fall under the service's jurisdiction. However, if the offences complained of relate to a threat that must be monitored by law (in this case interference), the monitoring thereof is pertinent in relation to the intelligence assignment. The Committee was also of the opinion that State Security should have documented the conclusions – even if interim – of its analyses in writing, in the context of the real or potential threat of which they became aware, regardless of how or from whom.

II.7. POSSIBLE REPUTATIONAL DAMAGE BECAUSE OF STATEMENTS MADE BY STATE SECURITY

In July 2012, the Standing Committee I received a complaint about State Security from a private individual working in the economic intelligence-gathering sector.[181] He alleged that State Security was smearing his reputation in the sector he worked in and that this had adverse consequences for the growth of his professional relationships. In September 2012, the Standing Committee I decided to open an investigation '*into the information that State Security may have disclosed about a private individual*'.[182]

The Committee found that the complainant and his trading companies were known to State Security as part of a general investigation into private investigation companies. The investigation was conducted by the department within State Security that is responsible for the scientific and economic potential of the country (SEP). The Committee held that State Security's interest in the complainant's intelligence-gathering activities was legitimate. The Committee

[181] In accordance with Article 40 of the Review Act, the complainant asked for his anonymity to be guaranteed.

[182] The final report was approved in April 2013.

itself has moreover previously recommended to State Security to study such activities.[183]

The information in State Security's possession did not give cause for any analysis in order to demonstrate what threat the complainant's activities allegedly held for the SEP. The information obtained was therefore kept in the context of general information that is gathered about private investigation companies operating in Belgium. No intelligence report or analysis of the complainant's activities was provided to third parties.

The Committee further held that the information underlying the complaint could not be proved in any way.

II.8. ALLEGED UNLAWFUL DISSEMINATION OF PERSONAL DATA BY STATE SECURITY

II.8.1. CAUSE

In mid-October 2012, a private individual filed a complaint with the Standing Committee I. The content of various newspaper articles[184] led him to suspect that State Security had a 'secret dossier' on him and he wondered how journalists had come into possession of it. The complainant asked the Committee for a copy of all information that State Security had gathered about him as well as an investigation into the members of State Security that in his opinion had committed a criminal offence by passing classified information to the media.

As a result, the Committee decided in April 2013 to open an investigation that was completed at the start of September 2013.

The Standing Committee I was obviously not authorised to give the complainant any information in State Security's possession. The Committee referred for this purpose to the different options as provided for in the Freedom of Information Act of 11 April 1994 and the Privacy Act of 8 December 1992.

What could be checked was whether State Security had actually created a dossier on the complainant and/or whether the press had become aware of that information[185]; whether State Security thereby compromised the rights that the Constitution and law confer on the complainant (more specifically the right to

183 STANDING COMMITTEE I, *Activiteitenverslag 2003* (Activity Report 2003), 24 to 115.

184 PLA, LVDK and GVV, *Het Laatste Nieuws*, 22 September 2012, *Niet te temmen* (Not tameable); JDB and JVC, *Het Nieuwsblad*, 24 September 2012, *Kopstuk Sharia4Belgium werkte even op Vlaams Kabinet* (Leader of Sharia4Belgium worked at Flemish Cabinet).

185 This could be done, for example, pursuant to Article 19(2) of the Intelligence Services Act that lays down the conditions regarding communication of information to the press by the administrator-general of State Security or by an inappropriate communication that would be contrary to the classification rules (Classification Act).

privacy) and/or whether the publication of the alleged information adversely affected the efficient functioning of State Security.

II.8.2. INVESTIGATION FINDINGS

The investigation showed that State Security indeed gathered and kept mostly 'confidential' classified intelligence on the complainant. He was known to State Security because he had attracted the attention in February 2006. The complainant also shared his extremist views and involvement on his blog. He made no secret of the fact that he was active within *Sharia4Belgium* and presented himself as its spokesman. State Security was therefore of the opinion that the complainant's very disturbing behaviour needed to be monitored.

The Committee found this monitoring to be justified from the perspective of the service's legal assignment that consists, more specifically, of the collection, analysis and processing of information relating to any activity which threatens or could threaten the internal security of the State and the survival of the democratic and constitutional order.[186]

State Security confirmed that it has not disclosed any information about the complainant to the press. Besides the complainant's statements, the Committee could not find any indication on the basis of which it could be proven or assumed that such a disclosure had taken place. As the complainant himself was vocal in the media and on social networks, it was not difficult for the press to find indications of his involvement within *Sharia4Belgium*. In the absence of evidence of any unlawful distribution of personal data, the Standing Committee I therefore held that State Security had not in any way impaired the rights conferred by the Constitution and law on the complainant.

II.9. COMPLAINT ABOUT THE THEFT OF A LAPTOP

At the start of 2013, the Speaker of the Senate received an e-mail from someone who stated that his laptop had been stolen during the course of 2007. He wished to know whether the theft had perhaps been committed at the time by a Belgian intelligence service. In response to this, the President asked the Standing Committee I to open an investigation.

The complainant, who worked as a journalist, wrote a number of articles about the situation in Congo during the period 2006–2007. He stated that those

[186] In this regard, the Standing Committee I also remarked that the complainant was placed under a warrant of arrest on 29 August 2013 for making 'written threats' with regard to several people. He was convicted in early January 2014 by the Antwerp Correctional Court.

publications had not been appreciated and alleged that various politicians had taken him to task over them. When his computer – and that of one of the people mentioned in his articles – disappeared, he reported the matter to the police.[187] However he did not suspect any possible perpetrator(s) at the time. It was only later that he became convinced that a Belgian intelligence service was possibly behind the theft: this was prompted by a statement of his lawyer and of a third party whom he suspected had strong ties with a foreign intelligence service. When the press began to refer to the monitoring of political representatives by State Security at the start of 2013 (see Chapter II.2), he did not rule out that journalists may also be the target of special attention from the intelligence services.

The Standing Committee I obviously did not have jurisdiction to look at the criminal side of the case. However, it is its task to deal with complaints and reports concerning the functioning, behaviour, acts or omissions of the intelligence services. This is why the Committee questioned GISS and State Security.

GISS knew the complainant only as the author of the above press articles.

State Security also had the press articles because they dealt with a topic that fell under its statutory competence and that it monitored. However, the complainant himself was never the target of special attention by this service. State Security did know about the theft of the laptop. A short report about this was even drafted without any further analysis and/or comment.

The Committee concluded that the complainant had received limited passive attention from both intelligence services at the end of 2007. No information was found that could point to any involvement by GISS or State Security in this offence.[188]

II.10. INTERIM REPORTS IN THE INVESTIGATIONS FOLLOWING THE SNOWDEN REVELATIONS

The revelations of the American whistleblower Edward Snowden sounded the starting shot for various investigations (see II.11.11). In view of the complexity and impact of the revelations, the Standing Committee I could not complete these investigations in 2013.

However an extensive interim report '*into the intelligence position of the Belgian intelligence services regarding the capacity of certain states to carry out massive data collection and mining and the manner in which these states would engage in political espionage in so-called* '*friendly countries*" (free translation) was completed and sent to the competent authorities. The interim report

187 This criminal investigation was most likely dropped.

188 The investigation was completed in October 2013.

essentially contains the open source analysis of Mathias Vermeulen[189], who was engaged as an expert by the Standing Committee I on the basis of Article 48 §3 of the Review Act. His work resulted in the study '*The Snowden revelations, massive data collection and political espionage*' (free translation). The expert report was preceded by an introduction of the Standing Committee I in which the Snowden revelations were placed in a broader context. This was to facilitate a better understanding of the expert's report.

A second investigation[190] following the Snowden revelations deals, among other things, with the international and national 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, companies or institutions based in Belgium (or that have any link to Belgium). The Standing Committee I also relied on contributions from an expert in relation to this investigation (Prof. Annemie Schaus, Université Libre de Bruxelles). Her '*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, companies or institutions based in Belgium (or that have any link to Belgium)*' has also been included as an appendix to this activity report.

II.11. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2013 AND INVESTIGATIONS THAT WERE OPENED IN 2013

This section contains a list and brief description of all investigations opened in 2013 and those investigations that were continued during the operating year 2013 but which have not been completed as yet.

II.11.1. MONITORING EXTREMIST ELEMENTS IN THE ARMY

As a result of briefings given by GISS during 2012, the Standing Committee I took note of the problem of service personnel moving within extremist circles and

189 *Research Fellow* at the European University Institute (EUI) in Florence and the Centre for Law, Science and Technology Studies at VU Brussel.

190 Investigation '*into 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, companies or institutions based in Belgium (or that have any link to Belgium)*'. The results of this investigation were submitted to the Monitoring Committee of the Senate and the competent ministers in mid-February 2014.

service personnel 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 Ardense Jagers Battalion, who apparently drew up combat manuals with the experience gained there. The Committee therefore decided to open an investigation into '*the detection and monitoring by GISS of extremist elements among the personnel of Defence and the Armed Forces*' (free translation). The investigation wishes to examine whether GISS is tackling this problem efficiently and whether the service is also respecting citizens' rights in this regard.

The regulations on 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 cover that material so the focus would be on two processes: the screening process during the recruitment phase and the detection process and monitoring of radical or extreme elements that have already been recruited.

II.11.2. STATE SECURITY AND ITS CLOSE PROTECTION ASSIGNMENTS

Within the framework of the '*joint supervisory investigation into CUTA's threat assessments relating to foreign VIP visits to Belgium*'[191] (free translation), questions were asked about State Security's availability to carry out certain close protection assignments. State Security on several occasions invoked compelling reasons of being overburdened and a lack of resources.

The Standing Committee I then decided to open an investigation to examine whether State Security was performing its close protection activities in accordance with the law and/or whether it was working efficiently in this regard.

The 'SECRET – Act of 11.12.1998' classified version of the final report was sent at the end of December 2013 to the administrator-general of State Security. This was to allow for comments and additions to be made that would benefit the completeness and clarity of the report. The investigation was completed in early 2014 and discussed in the Monitoring Committee of the Senate.

II.11.3. 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 (see Chapter VI). As the information in the Standing Committee I's possession pointed to possible

191 STANDING COMMITTEE I, *Activiteitenverslag 2012* (Activity Report 2012), 35–37.

structural problems, it was decided at the beginning of September 2012 to open a themed investigation into '*the manner of managing, using and auditing funds intended for the payment of State Security and GISS informants*' (free translation).

In view of the current criminal investigations, the investigation was immediately suspended. It was decided that the investigation could resume again at the end of March 2014.

II.11.4. 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 introduced at CUTA for the purpose of '*structurally gathering intelligence on entities that are monitored as part of the Radicalism Action Plan*' (free translation).

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 disseminates the information contained in the Joint Information Box (JIB), in accordance with the implementation of the Radicalism Action Plan*' (free translation).

In 2013, both Investigation Services P and I carried out investigative acts and drafted an initial summary report.

II.11.5. INTELLIGENCE AGENTS AND SOCIAL MEDIA

At the end of November 2012, the media reported on the profiles of intelligence service employees on social networking sites such as Facebook and LinkedIn. The Monitoring Committee of the Senate then requested that the Standing Committee I open a supervisory 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.

The Standing Committee I commenced its investigation into the employees of GISS and State Security in December 2012. Various investigative acts were performed. The investigation will be concluded in 2014.

II.11.6. PERSONNEL OF CUTA AND SOCIAL MEDIA

A joint investigation with the Standing Committee P was also started 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 control over the functioning of CUTA is observed by both Committees jointly.

This report can also be completed in 2014.

II.11.7. INTELLIGENCE POSITION OF THE INTELLIGENCE SERVICES AND CUTA IN RELATION TO A TRAINEE PILOT

In July 2012, various press articles appeared citing from an investigation of the Standing Committee P into '*information flows at airports*'. Reference was made, among other things, to a person who was able to attend pilot training at a Belgian airport even though his past pointed to possible radicalisation. This example could highlight shortcomings in the exchange of information between the various police services at airports. After reading the report, the Standing Committee I decided to open a joint investigation in June 2013 '*on the intelligence position and monitoring by the support services of CUTA – including into the evaluation of the threat by CUTA – regarding a private individual X who was admitted to attend a aeroplane pilot course in Belgium*'.

The investigation is in its final phase.

II.11.8. COMPLAINT OF THE CHURCH OF SCIENTOLOGY AGAINST STATE SECURITY

Various newspaper articles appeared during January and February 2013 stating that State Security would check whether politicians were in contact with organisations such as Scientology (see II.2). A classified memorandum and the *'Phenomenon analysis on interference activities not directed by a State'* (free translation) of State Security were also cited. In March 2013, the Church of Scientology decided to file a complaint with the Standing Committee I. The Committee decided to open an investigation into how State Security had drawn up and disseminated a report relating to that church. Most investigative acts were completed in 2013. The final report was finalised in mid-2014.

II.11.9. 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 CUTA Act). In their joint meeting in early May 2013, the Standing Committees I and P decided to investigate how CUTA carries out that assignment.[192] All the parties involved were extensively questioned in 2013.

II.11.10. 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 for this purpose to information from State Security regarding '*important facts inherent to the person*'. This information would be an obstacle to his naturalisation. The person involved felt that he was the victim of a misunderstanding that led to an infringement of his individual rights by State Security. At the end of July 2013, the man filed a complaint with the Standing Committee I. The Committee then opened an investigation that was finalised in February 2014.

II.11.11. COMPLAINT ABOUT HOW STATE SECURITY MONITORS THE MANAGER OF A BELGIAN EXPORT COMPANY

In response to a complaint, the Standing Committee I opened an investigation early in October 2013 '*into how State Security approaches and treats the manager of a Belgian company that has specific information about exports to Iran*'. Various investigative acts were carried out. The complainant and representatives from the relevant intelligence service were heard several times. The final report will be completed in the course of 2014.

II.11.12. FOUR INVESTIGATIONS RELATING TO THE SNOWDEN REVELATIONS

On 6 June 2013, *The Guardian*[193] and *The Washington Post*[194] published information from tens of thousands of documents (classified and otherwise) that had been leaked by Edward Snowden, who held various positions in or

---

192 *'Joint investigation into how CUTA maintains international relationships with similar foreign or international services pursuant to Article 8, 3° of the CUTA Act of 10 July 2006'.*

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

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

for American intelligence services. New revelations have been quick to follow since.

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

These revelations sounded the starting shot for many investigations (parliamentary, judicial and intelligence) 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. Not only the US intelligence service NSA, but the United Kingdom is also alleged to have intercepted and analysed massive amounts of data. Secondly, the Monitoring Committee wishes the Standing Committee I to investigate the consequences for protecting the economic and scientific potential of our country, 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).

The Standing Committee I then opened three investigations that are obviously closely connected with each other. This also applies to a fourth investigation[195] that was initiated after a complaint from the chairman of the Flemish Bar Association at the Brussels Bar.

The first investigation[196] – that was discussed at the start of 2014 in the Monitoring Committee of the Senate – provides an answer to the following questions:

- what capacity do major powers such as the United States and Great Britain possess for the large-scale interception and exploitation of the data of people, companies or institutions based in Belgium (or that have any link to Belgium) and which data are 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 in view of their legal assignments)? Was intelligence gathered in this regard or was it

195 *'Investigation following a complaint by the chairman of a bar into the use of information originating from massive data capturing in Belgian criminal cases'.*

196 *'Investigation into the intelligence position of the Belgian intelligence services regarding the capacity of certain states to carry out massive data collection and mining and the manner in which these states would engage in political espionage in so-called 'friendly countries'.* The results of this investigation were discussed with the Monitoring Committee of the Senate and submitted to the competent ministers in mid-April 2014.

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? Although this aspect of the revelations (particularly certain operations by intelligence services of so-called 'friendly countries' in relation to international or supranational institutions in which Belgium is represented, or in relation to Belgian interests) was not explicitly included in the terms of reference of the Monitoring Committee, the Standing Committee I decided to pay attention to this, in view of the intrinsic importance of the question.

The second investigation[197] – which has already been discussed in the senatorial Committee – deals with the international and national 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, companies or institutions based in Belgium (or that have any link to Belgium). In terms of international rules, attention was obviously paid to Article 8 ECHR (explaining both the 'horizontal effect' of these provisions and any 'positive obligations' that arise from them for a State), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Directive 95/46/EC of 24 October 1995, Convention no. 108 of 28 January 1981 of the Council of Europe and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU). However, other more specific rules were also discussed: the rules on Passenger Name Record, Swift, Safe Harbour, etc. Lastly, the internal rules relating to the protection of privacy and data protection were explained: the Personal Data (Processing) Act, its implementing decree, and the provisions that are specific to the operations of intelligence services. This second investigation also provides an overview of the legal options that States, citizens, or companies have to take action against actual or potential infringements of constitutional and other rights.

The third investigation[198] – that has not yet been finalised – deals with the possible implications of data mining for the protection of the scientific and

197 *'Investigation into the rules applicable in Belgium to the protection of privacy in relation to resources that permit the large-scale interception and exploitation of the data of people, companies or institutions based in Belgium (or that have any link to Belgium)'*. The results of this investigation were submitted to the Monitoring Committee of the Senate and the competent ministers in mid-February 2014.

198 *'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 major forces and/or intelligence services'*.

economic potential of the country. It wishes to check whether Belgian intelligence services:

- have paid attention to this phenomenon;
- have detected a real or potential threat 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 fourth investigation, following a report by the chairman of a bar, mainly relates to any use of data that has been captured massively (and illegally).

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS

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 methods for intelligence gathering, as referred to in Article 18, 2° of the Act of 30 November 1998 on the intelligence and security services [and] to the application of Chapter IV, 2° of the same Act*'.[199] This chapter therefore deals with the use of special intelligence methods by both intelligence services and the manner in which 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 of the Senate.[200] In addition to a number of quantitative details (number of authorisations, duration of methods, people involved), these half-yearly reports must also deal with the 'results achieved' by means of the special intelligence methods (SIM). Due to the importance of this, the Committee has decided to present a short version of its analysis in this regard in this activity report.

III.1. RESULTS ACHIEVED

'Although the financial costs of an intelligence operation are often tangible, the benefits that it produces are often intangible… This is especially true when the object of an operation is the non-occurrence of an event, such as a terrorist attack'.[201] This citation immediately summarises how difficult it is to measure what result is achieved in a particular operation or method within an intelligence context. Moreover, the problem of measuring 'results' is not unique to the intelligence world. It also applies to the judicial world, such as when it wishes to measure the results of its special investigation methods. We note, however, that

199 For an analysis on the special intelligence methods and on the manner in which they are monitored, please refer to: STANDING COMMITTEE I, *Activiteitenverslag 2010* (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.

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

201 H. BORN and A. WILLS, *Overseeing Intelligence Services – A Toolkit*, DCAF, 2012.

the judicial authorities do not conduct such an analysis, despite the wording of Article 90*decies* of the Code of Criminal Procedure.[202]

Notwithstanding this difficulty, the Committee tried to gain insight into the 'usefulness' of the applied SIM, firstly by holding a simple survey at the two intelligence services themselves and then by means of an in-depth analysis of four substantial cases.

The survey at the intelligence services related to 238 SIM decisions and authorisations in the period from September 2010 to December 2012, or, in other words, a little more than 9% of the total authorisations.[203] Both services were asked how they evaluated the efficiency of the applied methods based on the intended objectives of the authorisation. State Security was of the opinion that all the intended objectives were achieved in 84% of the cases, some of the objectives were achieved in 8.5% of the cases, and none of the objectives were achieved in 7.5% of the cases. GISS answered as follows: all the intended objectives were achieved in 72% of the cases, some of the objectives were achieved in 16% of the cases, and none of the objectives were achieved in 12% of the cases.

Building on this self-evaluation, the Committee carried out a substantive investigation in which all the methods applied to the four different targets (i.e. a person or organisation) were investigated in detail. The particular SIM that were used in succession and what actual results were achieved, based on the purpose of the method (e.g. exposing the network of a person or obtaining certainty about a threat), were examined for each target. A total of 160 methods were applied to the four targets.

The first target was the subject of an SIM on a total of 18 occasions. Although the results achieved did not serve to confirm the service's suspicion, they did reinforce it, among other things because the service gained a better insight into the person's network. This was moreover the stated objective. SIM produced relevant information that could not be obtained using 'normal' intelligence methods. This case also showed that the monitoring of the subject was started at the request of a foreign intelligence service. The information obtained was shared with that intelligence service in accordance with Article 20 of the Intelligence Services Act.

---

202 *'Lastly, a further comment must be made about assessing the 'result' of the various measures. It proves to be very difficult in practice to adequately define 'the result' of the various measures, on the one hand, and to check the result 'in isolation' (for each measure), on the other hand, given that there is normally parallel use of different detection and investigative methods. It is moreover impossible to present the 'result' correctly or at least adequately without any additional information relating to the context in which the measures were used and without information on the assessment by the court hearing the case on the merits'* (free translation). (Criminal Policy Service, *2013 Report under Article 90decies of the Code of Criminal Procedure (2012)*, *s.l.*, 6).

203 Of these, 94 were for specific and 71 for exceptional methods in case of State Security and 48 were for specific and 25 for exceptional methods in case of GISS.

A second target – an organisation – was the subject of 47 methods. In order to expose who is in contact with whom, subscribers to electronic means of communication were often identified. There was also the possibility to locate people on the basis of their telecommunication and to shadow them. It may be affirmed in this case that the stated objectives of the SIM were generally achieved. This case also properly illustrates the connection between the 'normal' methods and SIM, and among the various SIM themselves where one method builds on the other.

A total of 79 methods were applied in a third case. The majority of these involved identifications and localisations. The target in this case as well was 'introduced' to the Belgian intelligence service by a partner service. However, the methods did not allow for any confirmation that this person effectively posed a threat. It did turn out, however, that he had been in contact with people that constituted a real threat. It could moreover be proved, via access to banking details, that specific financial flows at the time coincided with some activities of people that were also on the intelligence services' radar. The Committee had to conclude in this dossier that the intelligence position of the service concerned was not significantly strengthened despite the use of 79 methods.

The last case was based on 16 SIM that were used with regard to a specific organisation. This involved mainly lengthy surveillance with the aid of technical devices and the examination of banking details. The aim of the investigation was to check who could be considered part of the organisation's network. The Committee concluded that the technical devices used were sometimes defective, leading to a lack of results. In addition, part of the information obtained (visual material) could only be partially processed due to a lack of time and staff. The information that could be analysed was incorporated in dozens of intelligence reports. The Committee's study showed that the surveillance and the analysis of the financial information certainly contributed towards the achievement of the stated objective.

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

Between 1 January and 31 December 2013, the two intelligence services combined granted 1,378 authorisations for the use of special intelligence methods: 1,224 by State Security (of which 1,102 were specific and 122 exceptional) and 154 by GISS (of which 131 were specific and 23 exceptional).

The following table draws a comparison with the figures of 2011 and 2012. It must be noted that the Committee has since January 2013 been applying a different counting method for one specific special method. Previously, the number of 'Inspections of identification data of electronic communications,' were referred to in the footnote but not counted as such in the totals. This was previously opted for because the heads of intelligence services allowed most

'Inspections of identification data' in the same document where, for example, 'Inspections of call data' or 'Inspections of localisation data' were also allowed. Since this relates to another method, strictly speaking, the Standing Committee I held that counting 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 in this report is higher than for the same period of the previous year, this is largely due to a different counting method and thus not because so many more methods were used. The impact of the new counting method is immediately clear in the following table.

	GISS		State Security		TOTAL
	Specific method	Exceptional method	Specific method	Exceptional method	
2011	60	7	731	33	831
2012	67	24	655	102	848
2013	131	23	1102	122	1378

What appears at first sight to be a sharp increase must therefore be qualified. Based on the counting method that was used in previous years, there would have been only 960 methods in 2013. Around 13% more SIM were thus used compared to 2012. The following tables make it clear where the increase lies.

Three major categories are distinguished for each service below: figures on specific methods, figures on exceptional methods, and figures on threats and the interests to be defended that are envisaged by the methods.

III.2.1. AUTHORISATIONS WITH REGARD TO GISS

III.2.1.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMB. 2011	NUMB. 2012	NUMB. 2013
Entry into and surveillance of or in places accessible to the public, using a technical device	7	8	14
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

NATURE OF SPECIFIC METHOD	NUMB. 2011	NUMB. 2012	NUMB. 2013
Inspection of identification data of electronic communications, requesting the cooperation of an operator or direct access to data files	23 dossiers	25 dossiers	66 methods[204]
Inspection of call data of electronic communications and requesting the cooperation of an operator	17	30	15
Inspection of localisation data of electronic communications and requesting the cooperation of an operator	13	4	36
TOTAL	**60**	**67**[205]	**131**[206]

In relation to specific methods used by GISS, the comparison with previous years revealed two striking trends: the number of observations and localisations rose sharply.

III.2.1.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2011	NUMBER 2012	NUMBER 2013
Entry into and surveillance in places not accessible to the public, with or without a technical device	0	1	1
Entry into and searching of places not accessible to the public, with or without a technical device	0	0	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	7	5
Penetrating an IT system	0	2	0
Monitoring, intercepting and recording communications	2	14	17
TOTAL	**7**	**24**[207]	**23**[208]

204 A decrease can be noted compared to previous years: the 66 authorisations relate to 16 dossiers.

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

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

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

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

III.2.1.3. Interests and threats justifying the use of special methods[209]

GISS is authorised to 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 2011	NUMBER 2012	NUMBER 2013
Intelligence assignment	38	63	183
Military security	8	7	26
Protection of secrets	19	21	50

Unlike for State Security, the threats to which GISS may or must pay attention are not laid down in the Act. Despite this, the service systematically mentions the threat being targeted in its authorisations. Such transparency is to be recommended. The figures show, in relation to the use of special methods, that combating espionage has remained the first priority of the military intelligence service.

NATURE OF THREAT	NUMBER 2011	NUMBER 2012	NUMBER 2013
Espionage	54	78	157
Terrorism (and radicalisation process)	10	3	11
Extremism	3	3	42
Interference	0	2	2
Criminal organisation	0	1	28
Other	0	5	29

[209] Each authorisation may involve multiple interests and threats.

III.2.2. AUTHORISATIONS WITH REGARD TO STATE SECURITY

III.2.2.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2011	NUMBER 2012	NUMBER 2013
Entry into and surveillance of or in places accessible to the public, using a technical device	89	75	109
Entry into and searching of places accessible to the public, using a technical device	0	1	0
Inspection of identification data of postal traffic and requesting the cooperation of a postal operator	4	2	0
Inspection of identification data of electronic communications, requesting the cooperation of an operator or direct access to data files	355 dossiers	254 dossiers	613[210] methods
Inspection of call data for electronic communications and requesting the cooperation of an operator	237	147	136
Inspection of localisation data of electronic communications and requesting the cooperation of an operator	46	176	244
TOTAL	**731**	**655**[211]	**1102**[212]

In relation to specific methods used by State Security, the comparison with previous years revealed two striking trends: the number of observations and localisations rose sharply.

III.2.2.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2011	NUMBER 2012	NUMBER 2013
Entry into and surveillance in places not accessible to the public, with or without a technical device	2	8	6
Entry into and searching of places not accessible to the public, with or without a technical device	3	6	6

210 A decrease can be noted compared to previous years: after all, the 613 authorisations relate to 243 dossiers.

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

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

NATURE OF EXCEPTIONAL METHOD	NUMBER 2011	NUMBER 2012	NUMBER 2013
Setting up and using a fictitious legal person	0	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	4	12	6
Collecting data on bank accounts and banking transactions	10	16	11
Penetrating an IT system	3	10	12
Monitoring, intercepting and recording communications	11	50	81
TOTAL	**33**	**102**[213]	**122**[214]

The figures again show a significant rise in the number of tapping measures: from 11 in 2011 to 50 in 2012 and 81 in 2013. No significant differences were noted for the other exceptional methods

III.2.2.3. Interests and threats justifying the use of special methods[215]

State Security may take action only in order to safeguard the following interests:

- the internal security of the State and maintenance of democratic and constitutional order;
- the external security of the State and international relations;
- safeguarding the key elements of the scientific or economic potential.

NATURE OF INTEREST	NUMBER 2011	NUMBER 2012	NUMBER 2013
Internal security of the State and maintenance of democratic and constitutional order	694	704	1994
External security of the State and international relations	571	693	1965
Safeguarding the key elements of the scientific or economic potential	24	15	18

The following table provides an overview of the (potential) threats targeted by State Security when using specific and exceptional methods. Of course, a single method may be directed against multiple threats. State Security may use specific

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

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

215 Each authorisation may involve multiple interests and threats.

methods in the context of all threats falling under its jurisdiction (Article 8 of the Intelligence Services Act). Exceptional methods may not be used in the context of extremism and interference. They are allowed, however, in the context of the radicalisation process that precedes terrorism (Article 3, 15° of the Intelligence Services Act).

NATURE OF THREAT	NUMBER 2011	NUMBER 2012	NUMBER 2013
Espionage	193	243	561
Terrorism (and radicalisation process)	371	288	1086
Extremism	319	177	602
Proliferation	17	28	27
Harmful sectarian organisations	4	7	15
Interference	3	10	27
Criminal organisations	3	5	18

These figures show that terrorism, extremism, and espionage remain State Security's priorities, at least in regard to the use of SIM.

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

III.3.1. STATISTICS

A referral may be made in five ways to the Standing Committee I to deliver a decision on the legality of special intelligence methods (Article 43, 4° of the Intelligence Services Act).

- 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' (Articles 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure). When requested, the Committee gives its opinion on whether or not it is legal to use intelligence acquired by means of specific or exceptional methods, in a criminal case. The decision to ask for the Committee's opinion rests with the examining courts or criminal court judges. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

METHOD OF REFERRAL	NUMBER 2011	NUMBER 2012	NUMBER 2013
1. At its own initiative	13	19	16
2. Data Protection Commission	0	0	0
3. Complaint	0	0	0
4. Suspension by SIM Commission	15	17	5
5. Authorisation by Minister	0	2	2
6. Pre-judicial consulting body	0	0	0
TOTAL	**28**	**38**	**23**

The figures show that the decrease in the number of referrals to the Committee can be attributed to the lower number of suspensions handed down by the SIM Commission.

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 formal 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 (43, 5°, §1, first to third paragraphs of the Intelligence Services Act);
5. Request for additional information from the relevant intelligence service (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). This section does not refer to the additional information that is often obtained by the Investigation Service I before the

actual referral to the Committee and which is, therefore, obtained in a more informal way;

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 judge (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 intelligence service assignments (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 legal or partially legal, proportionate and subsidiary by the Committee.
14. No competence for 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 (Article 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 the referral was 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	2011	FINAL DECISION 2011	2012	FINAL DECISION 2012	2013	FINAL DECISION 2013
1. Invalid complaint	0		0		0	
2. Manifestly unfounded complaint	1		0		0	
3. Suspension of method	3		1		0	
4. Additional information from SIM Commission	4		0		0	
5. Additional information from the intelligence service	9		6		0	
6.Investigation assignment of the Investigation Service	17		11		50	
7. Hearing of SIM Commission members	0		0		0	
8. Hearing of intelligence service members	1		0		0	
9. Decision regarding investigative secrecy	0		0		0	
10. Sensitive information during hearing	0		0		0	
11. Discontinuation of method	12		4		9	
12. Partial discontinuation of method	7		18		5	
13. Lifting or partial lifting of ban imposed by SIM Commission	5	**39**	13	**38**	2[216]	**23**
14. No competence	0		0		0	
15. Lawful authorisation / No discontinuation of method / Unfounded	15		3		7	
16. Pre-judicial advice	0		0		0	

III.3.2. DECISIONS

The 23 final decisions delivered by the Standing Committee I in 2013 are briefly presented below. The summaries have been stripped of all operational information. Only the information that is relevant to the legal question has been included.[217]

The decisions have been grouped into five categories:

– Legal (procedural) requirements prior to the implementation of a method;
– Justification for the authorisation;

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

[217] All decisions of the Committee in this matter were marked for 'limited dissemination'. One decision was marked as 'CONFIDENTIAL' and one as 'SECRET'.

- Proportionality and subsidiarity requirements;
- Legality of the method in terms of 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 sections.

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

No special method may be used without prior written authorisation from the head of service. Moreover, in case of an exceptional method, a draft authorisation and the assent of the SIM Commission must be presented. If such methods are used without written authorisation or assent, the Committee may obviously intervene.

III.3.2.1.1. No competence for the intelligence service

An intelligence service wished to monitor the incoming and outgoing calls of a certain mobile telephone number (dossier 2013/1835). After all, it had coincidentally become clear from another SIM that the target was probably involved in international smuggling or a scam. The service wanted certainty in this regard. It also wished to establish whether the foreign authority to which the target belonged was involved in the case. In its description of the threat, the service referred only to the '*damage caused by criminal organisations and the clandestine nature of the described scam that is at least a potential threat to the economic interests of Belgium*' (free translation). However, the Committee noted that the authority to monitor criminal organisations is limited to those organisations '*that actually relate to the activities of espionage, terrorism, extremism, proliferation, harmful sectarian organisations, and interference*' (Article 8, 1°(f) of the Intelligence Services Act). As a sufficiently compelling case for this was not made out in the authorisation, the method was found to be unlawful.

III.3.2.1.2. Authorisation by the competent minister

As in the previous year[218], the intelligence service made two referrals to its Minister on the basis of Article 18, 10°, §3, third paragraph of the Intelligence Services Act because the SIM Commission could not validly convene due to the holiday period (dossiers 2013/2327 and 2013/2328). This provision allows the

[218] STANDING COMMITTEE I, *Activiteitenverslag 2012* (Activity Report 2012), 55.

intelligence service to request its Minister to authorise the method if the Commission does not issue an opinion within four days of receipt of the draft authorisation for an exceptional method. The Committee had already decided, in view of the specific circumstances and the need for the service to be able to continue performing its legal assignments, that it had no objection to the immediate referral to the Minister. The Minister had signed but not dated the draft authorisation in the two new files. There was also no indication of when the head of service needed to report on the course of the method and the Minister failed to notify the Committee of the decision. Both obligations are included in Article 18, 10°, §3, third and fourth paragraphs of the Intelligence Services Act. Even so, the Committee held that the method was valid. It repeated that in view of the specific circumstances and the need for the service to be able to continue performing its legal assignments, it had no objection to the reliance on Article 18, 10°, §3, third paragraph of the Intelligence Services Act. The Committee also noted that this provision simply requires the permission of the competent minister without imposing obligations other than those set out in Article 18, 10°, §1 of the Intelligence Services Act. The Committee added that the '*lack of such an indication* [meaning the indication of when the head of service must issue his report, author's comment] *does not affect the lawfulness of the decision or compromise the permission of the Minister*'(free translation).

III.3.2.1.3. Method not covered by the (required) authorisation

When surveillance with a technical device was extended for the second time, the Committee noted that the extension had been erroneously requested seven days too late (file 2013/2653). In other words, the camera continued recording for a short period without the necessary authorisation. The intelligence service's position was that the Committee need not intervene because the service did not save the recorded images in its files and thus would not have been able to use them. However, the Committee held that the service's decision not to save the images '*cannot result in the Committee being deprived of the prerogatives granted to it by law regarding the fate that must be afforded to data gathered and recorded without a legal mandate*' (free translation). The images therefore had to be destroyed.

The same occurred in another dossier: the camera continued recording for 25 days between the second and third extensions of the method and the data was not destroyed because it could not/would not have been used. The Committee emphasised that '*the illegal implementation of a method provided for in Article 18, 17° of the Intelligence Services Act may constitute the infringement referred to in Article 259bis of the Criminal Code*' (free translation).

In a third dossier (2013/1760), the head of the relevant intelligence service decided to carry out a short surveillance operation with a camera on the

entrance of a hall that was accessible to the public and where a specific event would be held. The intelligence service was of the opinion that this was a specific method. However, from the additional information obtained by the SIM Commission, it transpired that the entrance '*was separated from the public road by a strip of land with a gate that can be closed, and that the hall was thus situated in a place that is not accessible to the public*' (free translation). In other words, this involved an exceptional method for which the required procedure had not been followed. The Committee thus agreed with the view of the SIM Commission and declared the method unlawful.

III.3.2.2. Justification for the authorisation

In 2013, the Committee came across five decisions that pointed to a lack of adequate or coherent justification for the authorisation.

An intelligence service wished to trace, identify and locate the call data of three telephones (dossier 2013/2618). However, the authorisation explicitly justified the localisation of only one telephone. On request, the intelligence service informed the SIM Commission that the intention was to locate only one of the three telephones. Reference to the localisation of the three telephones both in the authorisation itself and in the request to the operator was said to be an administrative error. The SIM Commission therefore ordered a partial suspension. However, the Committee '*to which the entire decision was referred by operation of law*' (free translation) ruled otherwise. After all, it was not possible to determine whether there had really been an administrative error. For this reason, the request for the localisation of two numbers for which no justification was given, was regarded as unlawful.

In another dossier (2013/1912), an intelligence service wished to identify the holder of a mobile telephone number. After all, he was alleged to have been in very regular contact with an active member of a certain foreign extremist organisation that was opposed to NATO, among others. However, according to the Committee, '*an examination of the documents does not show that the condition of legality of the method or the principles of subsidiarity and proportionality, as referred to in Article 18, 3°, §1, first paragraph of the Intelligence Services Act, were observed*' (free translation). Indeed, the threat that was to have emanated from the organisation was not specified by a single item of information in the decision. The Committee decided to intervene in this case with a view to obtaining additional information. It wanted further detail about '*the potentially threatening character of the subject of the specific method concerned*' (free translation) and '*the level of priority that the problem(s) had in its Action Plan*' (free translation). As the service concerned was able to give specific answers to both questions, the Committee held that the authorised method was lawful, proportional, and subsidiary.

An intelligence service wished to know via surveillance who would participate in a meeting that would likely discuss a new political initiative and new system in a certain country (dossier 2013/2420). They also expected that members of the relevant foreign intelligence service would be present. In its authorisation, the service stated that the following interests were under threat: '*the external security of the State and international relations, espionage, interference*' (free translation). Evidence of the seriousness of the threats was limited to the following: '*a real possibility that intelligence officers will carry out clandestine activities in Belgian territory*'. According to the Committee, '*The monitoring of activities that foreign intelligence services carry out in national territory is justified only in case of a specific threat to the security of the Belgian State and its international relations, since such monitoring is not the inherent task of the intelligence services*' (free translation). Since it was also not clear from the additional information how any clandestine activities could pose a threat to the security of the State and international relations, the method was unlawful.

In a final dossier, the Committee held that the method could not be authorised because '*the justification of the method is on the one hand inconsistent and on the other hand inadequate. It does not enable the Committee to assess its lawfulness*' (free translation) (dossier 2013/2447). The intelligence service had intended to carry out surveillance with '*surveillance cameras focused on open places that are accessible to the public, such as airports or train stations*' (free translation). The service referred for this purpose to Article 18, 4° of the Intelligence Services Act that provides for surveillance using technical devices in public places or in private places that are accessible to the public. However, it transpired from the justification for the decision that the intention was to check who lived in or visited a residence whose owner had been deprived of his freedom at that stage. Since the residence was part of a complex of dwellings, the Committee asked for a further explanation of how the surveillance would be carried out in practice. It followed from this that it was not the intention to carry out surveillance at places like stations and airports at all. '*The information provided at the Committee's request is more than a simple additional explanation but reveals the true purpose of the method*' (free translation). The disputed method was namely intended as preparation for another method (the surveillance of people who had access to the residence).

III.3.2.3. Proportionality and subsidiarity requirements

Six decisions were made in which the requirement of proportionality and/or subsidiarity was decisive.

In two dossiers (relating to the same operation), an intelligence service wished to trace and identify the call data of four people's telephone numbers (dossier 2013/2067) and their localisation at the same time (dossier 2013/2068).

However, the numbers were not known at that time. They would have to be obtained using another method. The Committee stated '*in the absence of information obtained by this first method, it cannot be judged whether the principles of subsidiarity and proportionality have been observed and whether the current method is thus lawful*' (free translation). The Committee therefore ordered its discontinuation.

The Committee arrived at the same conclusion in a later dossier (2013/2337). The intelligence service in question wished to monitor a number of mobile telephone numbers. However, some of the numbers were unknown at the time of the authorisation. The service wanted in fact to monitor some numbers that were or could be linked to a specific and known mobile telephone number. The number and identity of those numbers could only be known precisely when the method was actually used. As the method thus related '*to an undetermined number of mobile telephone numbers; that in the absence of information about the number of telephone numbers and the actual telephone numbers that would have to be monitored*' (free translation), it was impossible to judge its subsidiarity or proportionality. The method was therefore discontinued in relation to the unknown numbers.

When an intelligence service wished to trace the call data of the mobile telephone of a specific person and obtain the localisation data at the same time (dossier 2013/2417), the Committee suspended the methods: '*However, there is no further information about this [person]. His profile and activities appear difficult to evaluate… A convincing case has also not been made that this person actually constitutes a threat*' (free translation). The intelligence service had included a number of considerations in its authorisation that related to the person himself and a number of more general aspects of a geopolitical nature. The Committee asked the service for additional information. It followed from this that there was a certain contradiction between statements that the person had made at the time to a Belgian authority and his activities. '*This strange and ambiguous behaviour allowed for him to be regarded as a potential threat to the internal and external security of the country*' (free translation). On the other hand, the Committee stated that '*in the absence of more precise information about his actual activities, the request for localisation data seems disproportional at this time*' (free translation). The first method (tracing of call data) was therefore declared to be legal, while the second method (localisation) was overturned.

In support of a shadowing operation, the intelligence service wanted to be able to record images for one year during the surveillance (dossier 2013/2446). The Committee questioned the duration of this specific method. The Committee had already upheld authorisations for the use of cameras for one year, but that was for permanent cameras that were focused, for example, on an entrance located on a public road. In this case, however, it related to shadowing. '*Even if shadowing is an ordinary method that is not subject to the jurisdictional control of*

the Standing Committee I, the use of a specific method for a period of one year must still be justified in light of the principles of lawfulness, including the principles of proportionality and subsidiarity; The only explanation provided about the duration of the method in this case is that it is necessary for practical considerations at an operational level because a long period allows for the shadowing (and thus camera surveillance) to be planned taking into account other current or future tailing operations' (free translation). The Committee held that such a justification did not comply with the principles of proportionality and subsidiarity and that the surveillance that was accessory to shadowing must be limited to a reasonable period of four months.

In a last dossier (2013/2662), an intelligence service wished to carry out surveillance with a technical device of various members of a certain foreign organisation that operates in Belgium. The intended duration of the surveillance was one year. The service did not want to observe only the employees living in Belgium but also people that occasionally visited Belgium and were part of the immediate environment of the movement. The purpose of the method was to '*identify the contacts and activities of influential members of the monitored movement who are present in Belgium*' (free translation). Under this description, the authorisation did not cover people who were not living in Belgium. It was moreover not clear whether the people that were part of the immediate environment were also influential people. It further transpired that the method had not yet been implemented, even though this had been possible in accordance with the authorisation of the head of the service for almost a full year. Lastly, the Committee held that the authorisation to carry out surveillance of people that sometimes stayed in Belgium for one year was disproportionate. The duration of the authorisation for them had to be limited to the time they spent in Belgium.

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

III.3.2.4.1. Monitoring of the implementation of the SIM

The Act of 30 November 1998 stipulates that only a Belgian intelligence agent as described in Article 3, 2° of the Intelligence Services Act may actually implement a specific or exceptional method. Article 13, 1°, §2, fifth paragraph of the Intelligence Services Act envisages calling for help or assistance from other parties. This is not a problem as long as one or more Belgian intelligence agents '*maintain the service's control over the method*' (free translation). This criterion was specifically tested twice by the Committee.

In the first case (2013/1950), the service wished to carry out surveillance in a private place. The method would have been implemented by an agent of a foreign intelligence service and a private individual. As the service did '*not have direct*

control over the method as required by the legislature' (free translation), the method was discontinued.[219]

The second dossier (2013/2226) differed in this respect. The intelligence service called in the help of three foreign intelligence agents to remove a device from a car. The device had been placed using an earlier method. As assistance was only given by foreign agents with the necessary technical experience, and the Belgian agents thus maintained direct control, the method was lawful.

III.3.2.4.2. Suspension of a discontinued method

A different problem arose in dossier 2013/1728. On the same date as a tapping measure was authorised, the head of the relevant intelligence service discontinued the measure. It had transpired that the mobile telephone that was going to be monitored did not belong to the target. The SIM Commission then suspended the method and ordered its discontinuation. However, the Committee found that '*the factual determination that the target is not using one of the intercepted mobile numbers is not of such a nature that the method, which came into effect in full compliance with the law, would be unlawful per se*' (free translation). The head of the service reacted correctly by discontinuing the method as soon as it was no longer useful for the stated purpose. This constitutes an application of Article 18, 10° of the Intelligence Services Act. The Committee held that the power of the SIM Commission to suspend or discontinue a method (Article 18, 10°, §6 of the Intelligence Services Act) would be meaningful only if the head of service had failed to discontinue the measure. According to the Committee, the SIM Commission's decision was thus devoid of purpose.

III.3.2.4.3. Status of lawyer

An intelligence service decided to use an exceptional method in three dossiers (2013/2518, 2013/2519 and 2013/2536) with regard to a lawyer who was practising as such in a non-EU country but was present in Belgium at the time the methods were used. The Committee questioned whether the lawyer could enjoy the protection afforded under Articles 2 §2[220] and 18, 2°, §3 of the Intelligence

---

219 In addition, the service failed to investigate whether the location where the surveillance would take place was not subject to a special legal status afforded under international law.

220 *'The intelligence and security services are not permitted to acquire, analyse or make use of data which are protected by either the professional privilege of a lawyer or a doctor, or the confidentiality of journalistic sources.*
Exceptionally and where the service in question is in prior possession of serious evidence that the lawyer, the doctor or the journalist is or has been personally and actively involved in the creation or development of the potential threat, as defined in Articles 7, 1°, 8, 1°-4°, and 11, this protected data can be acquired, analysed or used.'

Services Act.[221] The Committee stated, on the basis of Articles 428 and 428*bis* of the Judicial Code[222] that the protection could not apply to someone who '*cannot practise as or use the title of lawyer in Belgium*' (free translation).

III.3.2.4.4. Duration of an exceptional method

The SIM Commission gave assent for luggage to be searched in a private place that was not accessible to the public (dossier 2013/2520). It did stipulate one provision: the authorisation could last only for a maximum of five days, and not for the two months stated in the draft authorisation. This threshold is provided for in Article 18, 12°, §1 of the Intelligence and Security Services Act. However, this was not taken into consideration in the authorisation itself, which was valid for two months. The SIM Commission therefore proceeded with partial suspension. The Committee upheld the SIM Commission's view.

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

The Committee held in dossier 2013/1728 that the tapping on a mobile telephone that did not belong to the target was lawful (see III.3.2.4.2). However, the intention was definitely not to gather that information. The Committee nevertheless considered that it was '*not authorised to assess whether or not it would be useful for an intelligence service to retain data gathered by means of an exceptional method that has been legally implemented; this evaluation lies with the intelligence service itself under Article 13 of the Intelligence Services Act and the Personal Data (Processing) Act of 8 December 1992*' (free translation).

Tracing of communication of a specific mobile telephone number was found to be unlawful in dossier 2013/1835 (see III.3.2.1.1). The Committee ordered the

---

221 '*If one of the methods referred to in §§1 and 2 is applied to a lawyer, a doctor or a journalist, or to their premises or the means of communication that they use for business purposes, or of their home or place of residence, this method may not be carried out until the appropriate one of the Chairman of the Flemish Bar Council, the Francophone and German-Speaking Bar Council, the National Council of the Order of Physicians or the Association of Professional Journalists has been notified of this fact by the Chairman of the Commission referred to in Article 3, 6°. The Chairman of the Commission is required to provide the necessary information to the Chairman of the Bar Council or of the Association of Professional Journalists of which the lawyer, the doctor or the journalist is a member. The Chairman in question is bound by confidentiality. The penalties set out in Article 458 of the Criminal Code are applicable to breaches of this obligation of confidentiality*' (free translation).

222 *Article 428 'Nobody may use the title of lawyer or practise as a lawyer unless they are Belgian or a national of another EU Member State, in possession of a doctorate or other qualifying degree in law, have taken the oath referred to in Article 429, and are registered on the Bar Council's roll of lawyers or the list of trainee lawyers. An exception may be made to the condition of nationality in the cases determined by the King on the recommendation of the Flemish Bar Council and the Francophone and German-Speaking Bar Council. Apart from the statutory exceptions, no further specifications may be added to the title of lawyer*' (free translation).

discontinuation of this method insofar as it was still being implemented. It also held that '*the data obtained and that may still be obtained under the methods declared to be unlawful*' (free translation) may not be used and must be destroyed.

In dossier 2013/2446, where the method was found to be disproportional (see III.3.2.3), the Committee stated that the requested surveillance, which was accessory to the shadowing, had to be limited to a reasonable period of four months and '*that the method was unlawful for periods in excess of four months*' (free translation).

When the intelligence service failed to take into account in its authorisation that a certain exceptional method can only be used for a maximum of five days (dossier 2013/2520 – also see III.3.2.4.4), the Committee found the method to be unlawful '*BUT ONLY insofar as it had been implemented AFTER the expiry of a five-day period, calculated from the authorisation of the head of service*'. In other words: only '*the data obtained and that may still be obtained under the part of the method declared to be unlawful, […] may [not] be used and must be destroyed*' (free translation).

In a last file (2013/2662 – also see III.3.2.3), an intelligence service wished to carry out surveillance with a technical device of various members of a certain foreign organisation that operates in Belgium. The intended duration of the surveillance was one year. The Committee held that this was disproportionate in relation to targets that were only in Belgium on a sporadic basis and stated '*their surveillance must therefore be limited to the duration of their stay in Belgium and, if necessary, to apply the urgency procedure. […] Rules that the method is unlawful as regards 'those previously responsible' who are no longer staying in Belgium but 'sometimes' return and as regards people who 'form part of the immediate environment' of the targeted movement; As the method has not yet been implemented, neither discontinuation nor the destruction of data gathered with regard to these people needs to be ordered*' (free translation).

III.4. CONCLUSIONS

The following conclusions may be formulated with regard to operating year 2013:

- The number of methods used increased as compared to 2011 and 2012. However, this cannot be referred to as growth that points to the unrestrained use of special methods.
- The increase is largely due a sharp rise in the number of surveillances and localisations by State Security.
- An increase in the number of authorised tapping measures is to be noted for the third consecutive year.

- The investigation into the results achieved shows that one target may be the subject of a significant number of methods.
- For GISS, the fight against 'espionage' remains the one that requires the most special methods. Attention to this threat (at least as far as special intelligence methods are concerned) is also increasing within State Security. On the other hand, both services authorised fewer methods in the fight against terrorism.
- Twelve specific and exceptional methods were used in relation to a lawyer, doctor, or professional journalist. The previous year there were 24. As several such methods can be applied to one person, this figure says nothing about the number of professionals targeted by an SIM.
- In 2013, 23 referrals were made to the Standing Committee I, in contrast to 38 the year before. This decrease in the number of referrals can be attributed to the lower number of suspensions handed down by the SIM Commission.

CHAPTER IX
RECOMMENDATIONS

Based on the investigations concluded in 2013 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 on 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. IMPLEMENTATION OF ARTICLES 19 AND 20 OF THE INTELLIGENCE SERVICES ACT[223]

The Committee reiterates that pursuant to Articles 19 and 20 of the Intelligence Services Act, it is up to the competent ministers and the Ministerial Committee for Intelligence and Security to determine the conditions under which the Belgian intelligence services must or may cooperate with foreign intelligence services. The Standing Committee I considers that is it essential for this purpose for both intelligence services to submit a joint proposal to the Ministerial Committee, discussing all aspects of the problem, by no later than mid-2015.

The Standing Committee I specifically recommends to GISS that a study be conducted into any responsibility that may arise when the service exchanges information and/or intelligence with a foreign intelligence service or institution.

223 This recommendation stems from the investigations into 'The role of the General Intelligence and Security Service in monitoring the conflict in Afghanistan' (see II.1) and the 'Monitoring of political representatives by the intelligence services' (II.4).

IX.1.2. A DIRECTIVE ON INTELLIGENCE WORK RELATING TO PERSONS WITH SPECIAL RESPONSIBILITIES AND POLITICAL PARTIES[224]

The Standing Committee I wants State Security and the General Intelligence and Security Service to take a joint initiative to the Ministerial Committee for Intelligence and Security with a view to adopting a uniform directive with clear and unambiguous rules for the collection, processing, consultation (including any internal screening), storage, and archiving of data regarding certain categories of persons who bear or who have borne special responsibilities as well as political parties. The details of this directive must take into consideration freedom of association, freedom of expression, and the guidelines outlined in the judgment of the European Court for Human Rights in the case 'Segerstedt-Wiberg and others', and must give shape to the principle stated in Article 2 of the Act of 30 November 1998: '*In the execution of their assignments, these services are responsible for compliance with and contribute to the protection of individual rights and freedoms and to the democratic development of society.*'

The Committee lastly pointed out that it is up to the legislature, if required, to incorporate special guarantees for political representatives by amending legislation, if needed (e.g. the SIM Act), and/or entrusting special oversight to the Standing Committee I. However, the interests of the normal functioning and development of democratic institutions as well as the legal assignments of the intelligence services must also be taken into consideration.

IX.1.3. UNAMBIGUOUS DIRECTIVE ON REPORTING THE MONITORING OF POLITICIANS

Further to the previous recommendation, the Committee is of the opinion that it is up to the competent ministers – as the hierarchically and politically responsible party – to determine the cases in which and when they wish to be notified. It is also important that ministers clearly describe the purposes and terms[225] of such notice.

---

224 This recommendation is made in response to the investigations into 'Confidential memoranda about Scientology in the press' (II.2) and 'An informant within Vlaams Belang?' (II.3) and 'Monitoring of political representatives by the intelligence services' (II.4). The Committee thus reiterates the recommendation from its 'reserved dossiers' investigation, see STANDING COMMITTEE I, *Activiteitenverslag 2008* (Activity Report 2008), 110–111.

225 Immediate or periodic notice; only reporting collection documents, analysis reports and/or reports intended for external services; reporting also for regional ministers and members of parliament and/or high-ranking officials of the judicial authority; any monitoring of this by the Standing Committee I via autonomous access to the database, etc.

IX.1.4. PERMANENT TRAINING AND REAL QUALITY MONITORING OF COLLECTION REPORTS[226]

The Committee is very much aware that it is not always immediately evident at the time of collection in intelligence work what information will or will not ever turn out to be relevant. However, that in no way detracts from the fact that the applicable requirements – such as those set out in the Intelligence Services Act as well as the Data Protection Act (purpose limitation principle, adequacy, accuracy, etc.) – must be observed. This means, for example, that whether and to what extent specific information must be included in a collection report constitutes a crucial fact. The manner of input should be a topic of permanent training and subject to serious quality monitoring.

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

IX.2.1. RECOMMENDATIONS IN THE CONTEXT OF GISS'S FOREIGN MISSIONS

Various *ad hoc* recommendations were made as part of the investigation into 'The role of the General Intelligence and Security Service in monitoring the conflict in Afghanistan' (II.1).[227] The Standing Committee I:

- recommends that GISS defines the connections that must be made between operational, tactical and strategic intelligence and the legal assignments described in the Intelligence Services Act;
- recommends that GISS prepare a volume of the texts that are applicable during its deployments, including both the international and national rules. As far as the latter is concerned, better integration and consistency of the content is needed;
- believes that it is necessary to improve the training of personnel before they depart on assignments and encourages GISS to continue with the improvements already being made;

---

226 This recommendation stems from the investigation into 'alleged criminal offences by a foreign intelligence service and State Security's intelligence position' (II.6).

227 In reaction to the report, GISS stated that the recommendations '*can make a real contribution to the optimisation of GISS's organisation and functioning. Although the investigation focuses on one operation, which has undergone significant changes in more than a decade, it certainly remains representative of GISS's intelligence work*' (free translation). It also appears as though the service has already started implementing the various recommendations. The Commission can only be pleased about this.

– believes that it is vital for GISS to apply the C*omprehensive Preparation of the Operational Environment* method (or any other methodology with the same purpose) and, in particular, to take into account the needs that military partners express in relation to the preparation of assignments;
– recommends that GISS adopts a proactive attitude to its clients, in order to be able to determine their expectations more precisely and to provide clients with a clear picture of what GISS can deliver;
– recommends that GISS makes a general estimate of the risks to military and civilian personnel deployed to conflict zones, and makes proposals for dealing with those risks;
– encourages GISS to further determine the role of analysts who are used in an environment where collection is done, specifically with a view to guaranteeing the objectivity of the assessment function;
– recommends that GISS adopts a more systematic approach to deploying personnel in a conflict zone. Such an approach, based on the threats that GISS must monitor under the Intelligence Services Act, is essential to determine what human and material resources need to be deployed;
– believes that GISS personnel deployed to the conflict zone must have appropriate equipment, particularly as regards the means of communication and vehicles that are provided to BENIC.

IX.2.2. A DEBATE ON THE USE OF SIMS ABROAD

In order to intercept communications originating abroad, for example for the security and protection of our troops and those of our allied partners during missions abroad, GISS has a specific statutory mandate (Article 259*bis* §5 of the Penal Code, as read together with, Article 11 §2, 3 of the Intelligence Services Act). That is lacking for the use of special intelligence methods. The Committee recommends that the legislature hold a debate about the need to make certain SIMs possible abroad. The Minister of Defence agreed to pay specific attention to this issue – among other reasons with a view to complying with human rights and operational needs in the field – and linked this to an evaluation of the Special Intelligence Methods Act.

IX.2.3. UNAMBIGUOUS CONCEPTS FOR THE ORGANISATION OF THE DATABANK

In its investigation into the monitoring of political representatives (II.4), the Standing Committee I concluded that the concepts underlying the organisation of GISS's database create fundamental problems because they are not interpreted or applied unambiguously. As a result of this, there is a risk that intelligence

work will lose its efficiency and effectiveness because not all correct reports will 'come to the surface' when this is necessary for the purpose of assessment work. There is also the risk that incorrect conclusions will be drawn. The Standing Committee I therefore holds the view that GISS must urgently review these concepts, especially when they appear in documents that are distributed outside GISS.

The Standing Committee I is further of the view that a concept is currently missing: indicating the (presumed) role of a person mentioned in the report in relation to the threat as being a 'passer-by', 'potential victim', 'key figure', or 'actor', etc.

IX.2.4. RECORDING CONCLUSIONS OF ASSESSMENT WORK IN WRITING[228]

The Committee recommends that GISS systematically complete each assessment with a conclusion (in essence, the concise or preliminary conclusion), in order to record whether, how, and with what intensity the subject of the assessment (person, group, event, or phenomenon) must continue to be monitored.

IX.2.5. MONITORING OF FOREIGN INTELLIGENCE SERVICES

An extension of the powers of intelligence services in relation to monitoring foreign intelligence services has once again proved necessary.[229] The Committee therefore reiterates its own recommendation and the Senate's recommendation to include a specific power for monitoring the legitimacy of the activities of foreign intelligence services in Belgian territory in the Intelligence Services Act.[230]

IX.2.6. URGENCY PROCEDURE UNDER ARTICLE 13, 1°, §2 OF THE INTELLIGENCE SERVICES ACT

Article 13, 1°, §2, third paragraph of the Intelligence Services Act gives the (plenary) SIM Commission the option of granting intelligence officers express authority to commit criminal acts that are strictly necessary for the effective

---

228 This recommendation stems from the investigation into 'alleged criminal offences by a foreign intelligence service and State Security's intelligence position' (II.6).

229 This recommendation stems from the investigation into 'alleged criminal offences by a foreign intelligence service and State Security's intelligence position' (II.6).

230 STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 132.

implementation of an SIM or to ensure their own safety or that of others. However, the Act has not provided for an urgency procedure in this regard. The Committee is of the opinion that if the special method itself can be instituted on an urgent basis, the possibility must also be provided for the accessory power under Article 13, 1°, §2, third paragraph of the Intelligence Services Act to be exercised on an urgent basis.

IX.3. RECOMMENDATIONS RELATED TO THE EFFECTIVENESS OF THE REVIEW: STRICT APPLICATION OF ARTICLE 33 §2 OF THE REVIEW ACT

Article 33 §2 of the Review Act stipulates that *'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.'* This is not the first time[231] that the Standing Committee I has concluded that this obligation is not being strictly observed, particularly as regards GISS, CUTA and the support services. The precise application of this article by the monitored services forms a *conditio sine qua non* for the due performance of the Committee's task. For this reason, the Commission once again stresses the importance of the punctual, full and automatic provision of this information.

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

APPENDIX

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT

[Amendments brought until 31/08/2015]

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 supporting 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 supporting 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 I – 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 supporting 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 a new term of six years 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 Ministerial Committee, with regard to the Coordination Unit for Threat Assessment or the other supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 to the Chamber of Representatives every six months regarding the application of Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services. A copy of this semi-annual report shall also be provided to the Ministers of Justice and Defence, 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 supporting 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 31/08/2015]

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, §2, 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, §2, 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.]

(…)