ACTIVITY REPORT 2010
ACTIVITY REPORT 2011

ACTIVITY REPORT 2010
ACTIVITY REPORT 2011

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 2010. Activity Report 2011. 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 978-1-78068-102-3
D/2012/7849/98
NUR 823

CONTENTS

LIST OF ABBREVIATIONS

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)*
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)*
Classification Act	Act of 11 December 1998 on classification and security clearances, certificates and advice *(Wet betreffende de classificatie en de veiligheids-machtigingen, veiligheidsattesten en veiligheids-adviezen – Loi relative à la classification et aux habilitations, attestations et avis de sécurité)*
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
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
IACSSO	Information and Advisory Centre on Harmful Sectarian Organisations *(Informatie- en Adviescentrum inzake schadelijke sektarische organisaties – Centre d'information et d'avis sur les organisations sectaires nuisibles)*

ICT	Information and Communications Technology
IMINT	Image intelligence
Intelligence Services Act	Act of 30 November 1998 on the intelligence and security services *(Wet houdende regeling van de inlichtingen- en veiligheidsdienst – Loi organique des services de renseignement et de sécurité)*
JHA	Justice and Home Affairs
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
NSA	National Security Authority *(Nationale Veiligheids-overheid – Autorité nationale de sécurité)*
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)*
P&O	Personnel and Organisation
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*)
SEP	Scientific and economic potential
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	Signal intelligence
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
SLA	Service Level Agreement
SMART	Specific, Measurable, Acceptable, Realistic, Time-bound
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

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.

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 its military counterpart, the General Intelligence and Security Service. In addition, it supervises 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 Senate, the Chamber of Deputies 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 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. They are appointed by the Senate. 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 2010 and 2011 that are most relevant to the international intelligence community (the 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 third to be published in English by the Standing Committee I, after the *Activity Report 2006–2007* and the *Activity Report 2008–2009* (see www.comiteri.be).

Guy Rapaille, Chairman
Gérald Vande Walle, Counsellor
Peter De Smet, Counsellor
Wouter De Ridder, Secretary

1 September 2012

ACTIVITY REPORT 2010

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2010

PREFACE

The Standing Committee I is well known for its investigations. In the context of this mandate, the Committee has been reviewing the operations of the two intelligence and security services since 1993 and making investigation reports. These reports – at present, more than 200 in number – identify the cases in which the services have acted in a legitimate and effective manner and where shortcomings or failures were noted. In the latter cases, the Standing Committee I formulates recommendations for remedying or improving the functioning, which are forwarded to the legislative or executive authority. In this respect, Belgium has long been following one of the best practices formulated by the Human Rights Council of the United Nations: '*An effective system of intelligence oversight includes at least one civilian institution that is independent of both the intelligence services and the executive*.'[1]

Over the years, however, the range of tasks as well as the sphere of action of the Standing Committee I have expanded considerably.

At the end of 1998, the Standing Committee I was assigned the role of an 'Appeal Body for security clearances' and served, in this context, as a judicial body. In 2005, the competence of this body was extended to include disputes with regard to security certificates and advice. In addition, the composition of the Appeal Body was modified: since then, the Chairman of the Standing Committee I as well as the Chairmen of the Standing Committee P and the Privacy Commission are members of this body.

Furthermore, in 2003, the Committee was entrusted with the task of controlling security interceptions carried out by the military intelligence service, the GISS. Three years later, the Coordination Unit for Threat Assessment (CUTA) and its supporting services were placed under the review of the Standing Committees P and I.

The Act of 4 February 2010 governing the data collection methods by the intelligence and security services, known as the SIM Act, has again assigned significant additional tasks to the Standing Committee I.

First, the Committee has been assigned an advisory role in the context of certain criminal proceedings: if SIM data are used in a criminal case, the

---

1 United Nations General Assembly, Human Rights Council, *Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including their oversight*, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin SCHEININ, 17 May 2010, A/HRC/14/46, 30.

concerned judicial authority may obtain an opinion from the Committee regarding the legitimacy of the manner in which the information was acquired.

But even more important – and certainly more labour-intensive – is the monitoring task of the Standing Committee I in the context of the application of special intelligence methods, as described in a new chapter in the Intelligence Services Act of 30 November 1998. This new responsibility consists in assessing, as a judicial body, the legality, proportionality and subsidiarity of the specific and exceptional methods of data collection used by the intelligence services. If necessary, the Committee may recommend the discontinuation of a method as well as the destruction of illegally obtained information.

The Standing Committee I is required to present a half-yearly report to the Senate on the application of the new SIM Act. But this Act also introduced changes in the present Activity Report: from now on, the Committee must pay *specific attention to the specific and exceptional collection methods*. This obligation has led to the introduction of a new Chapter III: '*Control of special intelligence methods*'. From this it appears that it has been rather difficult to implement the SIM Act: the necessary implementation decrees were long in coming and the absence of the administrative SIM Commission – which, along with the Standing Committee I, forms a necessary link in the control of the specific and exceptional methods – meant that this Act was initially operating at only half its strength. Nevertheless, between 1 September and 31 December 2010, the two intelligence services took more than a hundred decisions with regard to the use of special intelligence methods.

It was only since 4 January 2011 that all the provisions of the SIM Act came fully into force, since this was the day on which the SIM Commission was officially installed. This is also reflected in the figures: during the first five months of this year, several hundreds of special methods had already been authorised. The application of the SIM Act seems to be cruising ahead and the Committee can fully assume its new and significant powers. However, we are still awaiting the judgements of the Constitutional Court in response to two annulment requests targeted at various provisions of the SIM Act.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2011

CHAPTER II
INVESTIGATIONS

In 2010, the Standing Committee I received fourteen complaints or reports from private individuals. Until now, two complaints have resulted in an investigation. For two other complaints, it is still being examined whether there are sufficient grounds for initiating an investigation. No action was taken regarding the remaining complaints or reports because, after verification of a number of details, it appeared that these were unfounded (Art. 34 of the Review Act) or because the Committee was not competent for the matter in question. In the latter case, the complainants were referred, wherever possible, to the competent authority.

In addition to the two investigations resulting from a complaint, the Standing Committee I initiated seven other investigations, one of which was opened at the request of the President of the Senate. Two investigations (regarding an aspect of the operations of the CUTA) were initiated and carried out jointly with the Standing Committee P in accordance with the Review Act of 18 July 1991.

Eleven investigations were completed in 2010. In addition, investigative steps were taken in several other cases. This chapter will first discuss the completed investigations (II.1 to II.11). This will be followed by a summary and brief description of the background of ongoing investigations (II.12).

It should be noted in advance that the SIM Act of 4 February 2010 has introduced some changes to the obligations of and options available to the Standing Committee I in its supervisory role.

Firstly, the Standing Committee I may, based on a reasoned application by its Chairman, request the administrative authorities (other than State Security, the GISS and the CUTA) to notify the Committee of the regulations, guidelines and documents issued by these authorities which the Committee considers essential for the performance of its task. The concerned administrative authority may itself assess whether it is relevant to communicate the requested information.[2] With this, the legislator wants to offer a solution for the fact that the guidelines of the Ministerial Committee for Intelligence and Security were not being communicated to the Committee.

Members of the intelligence services, the CUTA and its supporting services are obliged to disclose to the Committee the secrets they hold, even – and this is

[2] Art. 33 §2 of the Review Act.

new – if these secrets are related to an ongoing criminal investigation or judicial inquiry. In this event, the only requirement is that the Standing Committee I consults the competent magistrate in advance.[3]

At the time of setting up the CUTA in 2006, the legislator had chosen not to give the House of Representatives and the Senate the possibility of instructing the Committee to conduct an investigation into the operations of the CUTA and its supporting services, while this was possible with respect to the two intelligence services. Since 1 September 2010, the Committee can be entrusted with this task with regard to the CUTA as well.[4]

Furthermore, the obligation of the Committee to report to the Parliament every six months regarding the operations of the CUTA and its supporting services has lapsed. However, the annual Activity Report must pay specific attention to the *implementation of the Threat Assessment Act of 10 July 2006*.[5]

Finally, the Committee may use the information it obtains in the context of its jurisdictional SIM mandate, for its review task.[6]

II.1. ESPIONAGE IN THE *JUSTUS LIPSIUS* BUILDING

II.1.1. INTRODUCTION

At the end of February 2003, a fault was found in the telephone equipment of a translation booth in the *Justus Lipsius* building in Brussels. The offices of the General Secretariat of the Council of the European Union are located in this building. A technician was given the task of repairing the unit, whereby it was discovered that a wire was connected to a 'black box'. This involved phone-tapping equipment (which could be activated remotely) intended for eavesdropping on the British delegation. The Security Office of the Council opened an investigation and requested the assistance of State Security. On 19 March 2003, a French newspaper reported that phone-tapping equipment had been found in the EU building. The Council was forced to confirm this information, after which the Belgian and international press dug up the case further. In the meantime, the Security Office had discovered several other boxes, connected to installations of several other delegations.

---

3 Art. 48 §2 of the Review Act.
4 Art. 32 of the Review Act.
5 Art. 35 §1, 1° of the Review Act (and Art. 11, paragraph 1, 1° of the Review Act with regard to the Standing Committee P). Also see Chapter V.2.
6 Art. 43/7 of the Intelligence Services Act.

However, the Council was unable to find out who was responsible for installing the electronic equipment.[7] Moreover, it was even possible that this espionage equipment had been installed in the building during its construction in the mid-1990s. The fact that the equipment found was highly sophisticated gave rise to speculations that only an intelligence service, with access to very advanced technical resources, could have been responsible.

In May 2006, following a request from the President of the Senate, the Standing Committee I decided to initiate an investigation into the manner in which the Belgian intelligence services had intervened in response to this phone-tapping case. The request of the President of the Senate was more than justified; the case perfectly illustrated the relevance of numerous warnings issued by the intelligence services regarding the need to protect information systems from interceptions and/or cyber-attacks.[8]

The investigation could only be completed in 2011. This was due to many reasons, which will be explained in the following section. Subsequently, the manner in which State Security and the GISS handled this case will also be addressed.

II.1.2. DIFFICULTIES IN THE INVESTIGATION

While conducting this investigation, the Standing Committee I encountered a number of significant obstacles.

II.1.2.1. Taking cognizance of the judicial inquiry

Parallel to the investigation, a judicial inquiry had been initiated as a result of a complaint from the Council of the European Union.[9] In order to examine the contents of this judicial dossier, the Committee contacted the Federal Prosecutor. But the examining magistrate in question considered this examination to be premature. The Standing Committee I therefore considered it expedient to suspend its investigation.

It was only after repeated requests that the Federal Prosecutor allowed examination by the Committee in the beginning of January 2008. However, the Committee could only make notes; taking copies was not permitted.

The possible outcome of the judicial inquiry is not known to the Standing Committee I.

---

7 Reply by the Council to a written question E-1488/03 from Johanna BOOGERD-QUAAK dated 2 May 2003, *Official Journal*, no. 051, 26 February 2004, 66.

8 This problem is also the subject of a specific investigation (Chapter II.12.1. Protection of communication systems against possible foreign interceptions and cyber-attacks).

9 A judicial inquiry into the same events had been launched in Germany.

II.1.2.2. Application of articles 48 and 51 of the Review Act

The Committee requested State Security for a copy of a summary report that the service had prepared at the request of the Federal Prosecutor's Office. However, based on Article 51 of the Review Act, State Security refused to comply with this request as, according to State Security, the requested document had been sent to the examining magistrate and was therefore a part of the judicial dossier. The refusal to provide this document led to reasoned correspondence between the Standing Committee I and State Security regarding the application of Articles 48 and 51 of the Review Act. State Security interpreted the aforementioned Articles as a general principle preventing the service from providing the Committee with any information with regard to an ongoing criminal investigation or judicial inquiry. However, Article 51 of the Review Act only prohibits the seizure of such documents but not the right to examine them or take copies of them. Furthermore, although Article 48 of the Review Act allowed members of the intelligence services to refuse to disclose confidential information of which they were aware and which was related to a criminal investigation or judicial inquiry, this was an optional provision and not an obligation.[10]

II.1.2.3. Incompleteness of the initial dossier sent by State Security

Three years after the start of the investigation, State Security sent the Standing Committee I new documents (letters, internal memos and reports) regarding the case. It appeared that the examination of these documents was essential for reconstructing and assessing State Security's intervention.

II.1.2.4. Hearing of former members of the intelligence services

Naturally, the Standing Committee I wanted to question the then Administrator-General in order to understand the nature of the instructions related to the handling of this case. However, the Administrator-General was convinced that he could not provide any further useful information. Since he was no longer serving as a member of an intelligence service, the Standing Committee I had no means of forcing him to testify. This is because Article 48 §1 of the Review Act only allowed the Committee to summon for questioning the presently serving members of an intelligence service.[11]

---

10 With the implementation of the SIM Act, the members of the intelligence services are now obliged to disclose information to the Standing Committee I, even – and this is new – if this information is related to an ongoing criminal investigation or judicial inquiry (Art. 48 §2 of the Review Act).

11 This lacuna has meanwhile been remedied pursuant to a recommendation of the Standing Committee I (STANDING COMMITTEE I, *Activity Report 2009*, 88). Article 48 of the Review Act was amended such that, henceforth, former employees were also obliged to

II.1.2.5. Absence of other assessment criteria

Other assessment criteria required for making an objective assessment of the intervention of the Belgian intelligence services were also absent. For example, the Standing Committee I was not aware of:

- the position adopted by European governments with regard to this dossier;
- the position of the official delegations whose premises and telephone lines had been tapped;
- the actions taken by the intelligence services of the European countries which had been the object of the phone-tapping operations;
- the response of Belgian ministers who were informed of the case by State Security and the measures taken by them.[12]

II.1.3. MANNER IN WHICH STATE SECURITY HAS HANDLED MATTERS

II.1.3.1. Account of the facts

A few days after the detection of the fault on the telephone line, the Security Office of the Council initiated an investigation into this matter. The Head of Department of the Security Office and his immediate superior, both of whom were former members of State Security, requested their former colleagues informally for technical assistance. From 5 March 2003, with the verbal *fiat* of State Security management and the Security Office[13], a so-called '*covert action*' was set up. Working discretely, a State Security technical team installed cameras in the room where the phone-tapping equipment was first found. These cameras were to record all comings and goings and detect any intervention related to this equipment. A member of the Belgian Institute for Postal Services and Telecommunications was also called in: his task was to examine the equipment in an attempt to locate the transmitter-receiver. Meanwhile, the Security Office had discovered three more boxes, connected to the telephone installations of other delegations. This also involved transmission equipment which would record the discussions held in the conference rooms. As a result of this find, the State Security technical team decided to set up additional observation

respond to a summons for questioning (Act of 9 February 2011, *Belgian Official Gazette* 29 March 2011).

12 In addition, the Standing Committee I is not aware of any feedback which State Security might have received from other bodies regarding its intervention in this matter.

13 On 18 March 2003, the then Administrator-General of State Security sent a letter to the Deputy Secretary-General of the Council to formally confirm that his service had agreed to extend its cooperation in the context of an internal security investigation.

equipment. Intelligence services of several countries organised briefings in the field and the phone-tapping systems were removed a few days later.

On 13 March 2003, State Security sent a memorandum classified as 'SECRET' to the Prime Minister and the Ministers of Justice and Foreign Affairs. This memorandum informed the Ministers about the case.[14]

On the same day that the French newspaper reported the case, a meeting was held at the initiative of the Security Office at the offices of the Council. The 'Counter-espionage' division of State Security was informed of the facts for the first time. At this time, the Analysis Department of State Security was still unaware of the existence of this dossier. A day later – on 20 March 2003 – a new memorandum was sent to the Prime Minister and the Ministers of Justice and Foreign Affairs. The memorandum mentioned the fact that the phone-tapping equipment found had been targeted at a number of other delegations. In this memorandum, State Security stated that it is competent in matters involving interference, espionage and the protection of the scientific and economic potential. In the same memorandum, the service criticised the lack of staff and the absence of a legal framework enabling it to deploy technical resources. '*Par voie de conséquence, les services de renseignement de plusieurs autres Etats membres ont été intégrés à l'enquête*'.[15]

The technical team appointed by State Security continued its intervention until 21 March 2003, two days after the case was made public by the press. Another classified report was prepared.

In early April, a series of informal meetings were held between State Security, the Security Office and the foreign intelligence services in question. After an internal investigation, the Security Office provided State Security with the names of four technicians who were considered as suspicious. Two of these technicians had been trained by an Israeli company which had installed the translation system at the *Justus Lipsius* building. Therefore, the Security Office requested the assistance of State Security for screening these suspects. As it appeared later, the investigation of the four persons yielded no results. In its turn, State Security requested the Security Office to draw up a list of companies that might be considered as suspicious.

A month and half after the discovery of the facts, the Council submitted a complaint to the Prosecutor-General in Brussels against unknown persons for the installation of equipment designed to intercept telephone traffic in premises that serve as the meeting place for various delegations.

The 'Counter-espionage' division meanwhile drew up a summary of the state of affairs: the conclusion was that the installations, which had been placed

---

14 The Committee was not informed of how the concerned Ministers responded to this memorandum.

15 '*As a result, the intelligence services of several other Member States got involved in the investigation*' (free translation).

meticulously and expertly, dated from 1994 or 1995. The targeted countries carried out additional technical evaluations.

In mid-June 2003, State Security was informed of the fact that the Federal Prosecutor's Office had decided to open a judicial inquiry. The Federal Magistrate requested technical assistance from State Security and organised a meeting to discuss the composition of the investigation team and the strategy to be followed. A representative of the 'Counter-espionage' division, two members of the GISS and members of the Federal Police were present at this meeting. State Security was requested to prepare a summary of its dossier.

In October 2003, an internal State Security report outlined a summary of the state of affairs. The above-mentioned Israeli telecommunications company was known to State Security, as evident from the documentation of the service. The report also contained a summary of the contents of two meetings with members of the Security Office (July and October 2003). At these meetings, State Security had the impression that the investigation was by no means a priority for the Council management.

Since then, for six months, nothing further seems to have been done regarding this matter at State Security. But one year after the facts, the division in charge of organised crime prepared a report on one of the suspects who had undergone a technical training in Israel. This, however, did not contain any elements that could help take the investigation forward.

In June 2004, the Federal Police requested State Security for additional information. It is only at the end of January 2005 and after several reminders, that a – albeit incomplete – dossier was sent to the Federal Magistrate. During the same period, the 'International Relations' division of State Security consulted a foreign intelligence service. The Federal Police also approached the division for information concerning the possible involvement of the Israeli company in the espionage activities.

In May 2005, a meeting was again held with the Federal Police. The police officers were acting based on a written order from an examining magistrate. Information was again requested about the Israeli company. In September 2005, the Administrator-General of State Security sent his report to the Federal Magistrate.

Afterwards, there were no further changes in the situation until 22 February 2006, the day on which another meeting took place between representatives of State Security and the Federal Police. The most recent documents related to this case found at State Security are e-mails exchanged in February and March 2006 between the International Relations division, the Director of Operations and the Analysis Department regarding a planned meeting with the representative of the foreign intelligence service in Belgium. However, this meeting did not take place.

II.1.3.2. Some findings

The Standing Committee I believes that State Security correctly assessed the importance of the phone-tapping affair as well as the possible diplomatic repercussions on our country's position in the European context.

Article 20 of the Intelligence Services Act states that the intelligence services and administrative and judicial authorities must ensure that their mutual cooperation, as well as their cooperation with foreign intelligence services, progresses as efficiently as possible. Such cooperation should take place within the limits of a protocol approved by the concerned Ministers (Art. 20 §2 of the Intelligence Services Act). However, there is no protocol regarding assistance between the European bodies and State Security. Therefore the request for cooperation by the Security Office remained verbal and informal.

The same request for (technical) assistance was accompanied by the explicit recommendation to not inform the judicial authorities. This recommendation was to be respected as long as the Council had not decided on a particular standpoint in the context of this case. Even though the facts clearly constituted an offence or an attempted offence (Art. 314*bis* of the Penal Code), the State Security agents who knew of these facts, did not report them to the Public Prosecutor. Although this is required by Article 29 of the Code of Criminal Procedure.[16]

The 'Counter-espionage' division was only informed by the management after the press had made the case public. Moreover, prior to October 2004, this dossier does not contain any evidence of an intervention by the Analysis Department. Given the clandestine nature of the equipment found and the fact that this system was clearly designed for espionage purposes, the Committee believes that both the 'Counter-espionage' division of the Operational Departments and the Analysis Department of State Security should have been informed of the facts immediately after the discovery of the equipment. The Committee is surprised to find that, due to a very narrow interpretation of the '*need to know*' principle, the competent divisions did not get immediately involved in the case. Therefore, the Committee cannot say that State Security was entirely efficient in its handling of this case. In the opinion of the Standing Committee I, State Security acted in a rather informal and somewhat chaotic manner, without a structured plan of action. While various divisions were involved in this dossier, there seemed to be no one at State Security entrusted with the overall coordination and monitoring of this case.

---

16 This observation does not alter the fact that the Committee had earlier questioned the usefulness and appropriateness of this absolute reporting obligation. In its *Activity Report 2004* (147) the Committee had advocated a more flexible regulation that would allow the most appropriate option (judicial or intelligence) to be chosen so that an intelligence service could continue its work. In the same vein: STANDING COMMITTEE I, *Activity Report 2009*, 106.

At the time of the facts, State Security did not have access to any special intelligence methods. The service informed its Minister that this might create a problem with respect to the deployment of the required technical resources. This problem has meanwhile been resolved with the introduction of the SIM Act.

It should be noted that the exchange of information with the Federal Police was particularly difficult, since the police service sometimes received answers to its questions only after several reminders.

II.1.4. MANNER IN WHICH THE GISS HAS HANDLED MATTERS

No documents of the GISS were found in the judicial dossier of the Federal Prosecutor's Office. It also appeared that none of the divisions of the GISS had been officially informed of the events.[17] The service did not receive any official request for assistance and therefore, it neither took any initiative, nor did it prepare any document regarding this.

However, after the removal of the phone-tapping equipment, the GISS had carried out a sweeping at the *Justus Lipsius* building.[18] During this operation, carried out in the meeting rooms at the request of the European institutions, no clandestine phone-tapping devices were found. There is no explicit legal framework pertaining to such assignments and neither is there any protocol in place. Also, the operation was carried out unofficially and no written reports were prepared. The Standing Committee I considers that this is a special point of attention.

II.2. MONITORING OF HARMFUL SECTARIAN ORGANISATIONS

One of the phenomena that State Security must pay attention to is harmful sectarian organisations.[19] In the past, the Standing Committee I has focused its attention more than once on certain aspects of this issue.[20] At the beginning of

---

17 However, State Security reports showed that the GISS was present at a meeting organised by the Federal Prosecutor's Office. But the individuals in question stated that they did not recall having participated in such a meeting.

18 A '*sweeping*' is a thorough inspection of a room using electronic means to ensure that there are no hidden devices for monitoring or intercepting telecommunications. It is in fact not uncommon for international institutions located in Belgium to request the technical services of the GISS to carry out a '*sweeping*' of their buildings.

19 Articles 7 and 8 of the Intelligence Services Act.

20 STANDING COMMITTEE I, *Activity Report 1995*, 146–149 (Investigation of sects); *Activity Report 2003,* 253–258 (Investigation report of the complaint by an applicant regarding the advice given by State Security on his naturalization application); *Activity Report 2005*, 51–59

January 2007, the Committee decided to open a thematic investigation into the manner in which State Security monitors harmful sectarian organisations. The Committee wanted to identify the organisations which are kept under watch by State Security in this context and the manner in which these are monitored. It also examined the criteria used by the intelligence service to determine whether or not to consider a sectarian movement as dangerous, the analyses sent by State Security to the various authorities and the purpose of these analyses. Finally, the Standing Committee I wanted to gain an insight into the human and material resources made available by State Security for this task and the status of the cooperation with domestic and foreign services.

In the light of the final objective of the Standing Committee I, the importance of such a thematic investigation is obvious: monitoring by an intelligence service of groups with a philosophical or religious purpose, or which appear to be such, and which are described as 'harmful and sectarian' is an extremely sensitive issue. It is definitely a matter of fundamental rights such as the freedom of religion and association.

II.2.1. MONITORING OF HARMFUL SECTARIAN ORGANISATIONS PRIOR TO THE ACT OF 30 NOVEMBER 1998

As early as in the beginning of the 1970s, State Security had begun focusing its attention on sects. These organisations were then monitored as 'totalitarian groups'. However, in the 1990s, this problem received more attention from a political angle. In 1993, the Minister of Justice entrusted State Security with the task of studying the sects while paying particular attention to the plight of children.[21] Since then, State Security has applied the following definition: a harmful sect is *'any group that, under the pretext of professing a certain spirituality or philosophy and of owning the elitist monopoly over the path to truth, wisdom or salvation, intends to establish its total and exclusive mastery over people through systematic mental manipulation'*(free translation). With this, the service placed harmful sects on the 'subjects list' of political, extremist and

(Complaint by a private individual regarding the communication of information to the *Office de la Naissance et de l'Enfance* (ONE)); *Activity Report 2006*, 62–66 (Religious movement or harmful sectarian organisation?).

21 In 1994, the Minister of Justice once again assigned this task to State Security. In October 1995, the Minister assigned State Security the task of centralizing all information related to this topic.

terrorist groups, associations and movements to be monitored, whether or not at close quarters.[22, 23]

The Standing Committee I was also convinced that the monitoring of harmful sectarian organisations was part of the tasks of State Security. The Committee believed that, in this respect, State Security must primarily focus on the threats against the democratic order: *'This task is traditionally characterised by the collection of information on extremist groups. The sects are small (and sometimes large) totalitarian associations, one of whose characteristics is that they incite their members by cutting them off from civil society. The sects are an indirect threat to the State since they destabilise civil society by undermining its foundations.'* (free translation)[24]

In 1996, the establishment of the Parliamentary Inquiry Committee on Sects[25] in the House of Representatives signified a turning point in the government's approach. This Committee focused attention on the lack of legal investigation resources available to the intelligence services. Based on the Committee's report, a comprehensive policy was outlined, the implementation of which was entrusted to the Information and Advisory Centre on Harmful Sectarian Organisations (IACSSO), the Administrative Coordination Cell for the Fight Against Harmful Sectarian Organisations[26] and State Security.

Two years later, on 30 November 1998, the legislator explicitly entrusted State Security with the task of monitoring threats posed by harmful sectarian organisations (Art. 8, e) of the Intelligence Services Act.

---

22 The so-called 'subjects list' of 1996 contained the names of some fifty sectarian movements. In 1999, this list only contained 38 movements, each of which was assigned the letter 'A', 'B', 'C' or 'D'. This indicated, in descending order, the order of priority assigned by State Security with respect to monitoring these movements. Most of the movements were assigned the letter 'B' and no movement was indicated as 'A'. In 2006, there were once again more than fifty movements on the 'subjects list'.

23 This is by no means an 'official list' of the sects that are considered harmful. No such list exists in Belgium. The document regularly referred to as the 'list of harmful sects' (i.e. the synoptic table from the report of the Parliamentary Inquiry Committee) is not an official list. This is only an overview of the various movements and organisations interrogated by the Committee members or those mentioned during parliamentary proceedings (*Parl. Doc.* House of Representatives 1996–97, no. 49K313/8, 285).

24 STANDING COMMITTEE I, *Activity Report 1995*, 146–149.

25 'Parliamentary inquiry with a view to developing a policy to combat the illegal practices of sects and the hazards posed by these to individuals and especially to minors'.

26 The task of this Cell is to coordinate the actions taken by the services, investigate the evolution of illegal practices of harmful sectarian organisations, propose measures that are likely to improve the coordination and effectiveness of these actions, promote – in consultation with the competent services and authorities – a prevention policy to protect citizens against the activities of harmful sectarian organisations, develop a close cooperation with the IACSSO and lastly, to take the necessary measures for carrying out the recommendations and proposals of this Centre.

II.2.2. MONITORING OF HARMFUL SECTARIAN ORGANISATIONS AFTER THE ACT OF 30 NOVEMBER 1998

At present, State Security is bound by the definition given in the Intelligence Services Act of 30 November 1998, which was almost entirely taken over from the definition in the Act of 2 June 1998 governing the establishment of an Information and Advisory Centre on Harmful Sectarian Organisations and an Administrative Coordination Cell for the Fight Against Harmful Sectarian Organisations: *'any group with a philosophical or religious purpose or one which appears to be such and which, in terms of its organisation or practices, carries out harmful illegal activities, causes harm to individuals or society or violates human dignity.'* (free translation)[27]

Based on the legal definition, State Security determined three cumulative criteria for distinguishing between harmful sectarian organisations and other groups: (1) it must be a group (a single individual cannot constitute an organisation); (2) the group must have, or appear to have, a philosophical or religious purpose[28]; (3) the group must pursue illegal activities that are 'harmful' to the individual or society and/or[29] which violate human dignity.

To precisely determine the 'harmful nature' of a sectarian organisation, State Security uses a primary criterion and a number of secondary criteria. Not all secondary criteria must be satisfied in order to consider a movement as 'harmful'; however, the presence of the primary criterion is essential.

This primary criterion is the use of mental manipulation, moral coercion and violation of intellectual integrity. State Security acknowledges that 'mental manipulation' is not easy to describe. It defines this concept as '*a set of actions aimed at ensuring the complete obedience of the individual to the message propagated by the sect*'. Therefore, mental manipulation includes everything that may restrict the free will of the follower and harm his or her psychological integrity.

---

27 Article 2 of the Act of 2 June 1998 reads as follows: *'any group with a philosophical or religious purpose or one that appears to be such and which, in terms of its organisation or practices, dedicates itself to carrying out harmful illegal activities, causes harm to individuals or society or affects human dignity' (free translation).* To this, the Act adds that *'The harmful nature of a sectarian organisation will be investigated on the basis of the principles laid down in the Constitution, laws, decrees, ordinances and in the international conventions on the protection of human rights ratified by Belgium' (free translation).*
Unlike for the membership of an 'association of wrongdoers' (Art. 322 ff. of the Penal Code), there is no specific criminal law definition of the membership of a 'harmful sectarian organisation'. However, several legislative proposals have already been submitted in order to punish certain practices found within sects.

28 This second requirement is sometimes difficult to determine.

29 For State Security, these requirements are not cumulative but alternative.

The secondary criteria are:

- excessive financial demands from the follower or the 'gifts' that are collected for the benefit of the leaders of the sect;
- exploitation of the members for the benefit of the leaders of the sect, i.e. providing services in return for a symbolic or non-existent consideration;
- indoctrination of children and the fate that awaits them in the sect (breaking of family ties, sexual abuse);
- (progressive) isolation as a result of which the follower breaks off all ties with his or her reference environment;
- rejection of traditional medicine through the promotion or use of ineffective therapies or therapies that could adversely affect the physical integrity of the members;
- infiltration in and lobbying with political, social, administrative or economic bodies[30];
- the (more or less) anti-social and radical discourse of the sect leaders that can lead to acts of violence (collective suicide, attacks).

The legal definition and development of detailed criteria led to the settlement of a long-standing debate within State Security. This debate involved the question of whether or not to include groups with a therapeutic purpose within the category of 'harmful sects'. Should or could State Security focus attention on small sectarian communities that unite their followers around a guru and encourage them to move away from conventional medicine in order to seek refuge in practices whose therapeutic effectiveness has not been scientifically proved and which can be a threat to one's health? State Security decided that it will not, in principle, monitor movements with purely therapeutic goals. However, some non-conventional therapeutic practices expose their followers and sometimes their families to a '*mise en état de sujétion*' (state of subjection), which is closely related to the first criterion. In this case, according to the Standing Committee I, monitoring these movements becomes necessary.

According to State Security, only a minority of the organisations with a philosophical or religious purpose, or which appear to be such, and which are present and active in Belgium meet the above criteria. In the State Security Action Plan for 2010, harmful sectarian organisations are categorised according to the three intervention models which are also applied by State Security with respect to all other threats: sects requiring 'active priority monitoring'[31], sects

30 Some movements attempt to infiltrate certain sections of society (such as political circles, the business world, the education and training sector and even the prisons) in order to influence policy-makers in these sectors.

31 However, harmful sectarian organisations were not a priority in the National Security Plan of the government and were not among the priorities defined by the Board for Intelligence and Security in 2010.

requiring 'active monitoring' and sects for which 'reactive treatment' is sufficient.

II.2.3. PRODUCTS AND CUSTOMERS OF STATE SECURITY

Specifically with respect to sects, State Security believes that its primary responsibility is to raise awareness regarding the risks that practices of harmful sectarian organisations can represent for society. The role of State Security is also to centralise all information on this matter, which is then processed in the form of analysis reports, summary memoranda and a newsletter.

II.2.3.1. Analysis reports and summary memorandums

The relevant analysis reports of State Security basically consist of three sections: an ideological outline, a practical outline and a supplementary memorandum which may contain classified information and is only sent to the Federal Prosecutor. However, due to the limited number of analysts assigned to this mission, State Security cannot always draw up its analysis reports according to the above structure. Sometimes, summary memorandums are prepared from these analysis reports.

Between 1 January 2007 and 30 August 2009, State Security prepared about fifty analyses. In accordance with Article 19 of the Intelligence Services Act, these analysis reports were sent to the various political, administrative and judicial authorities. The external recipients of the analysis reports were usually:

- the Ministers of Justice, Foreign Affairs and Home Affairs;
- the Federal Prosecutor;
- the Public Prosecutors;
- the Director of the CUTA;
- the IACSSO;
- the Director-General of the penal institutions.

Information was also occasionally sent not just to certain Ministers of the Regions and Communities, but even to the Belgian Financial Intelligence Processing Unit.

As part of the parliamentary activities for the preparation for the Intelligence Services Act of 30 November 1998, it was repeatedly stated that the municipal administrations and educational institutions also have a legitimate interest in taking cognizance of certain information on sects.[32] With regard to the

[32] *Parl. Doc.* House of Representatives 1995–96, no. 49K638/7, 6 and no. 49K638/14, 71.

municipal administrations, the Standing Committee I was unable to fully establish whether they were recipients of such information.

The important question is, of course, whether these reports and memorandums are meaningful and perceived of as being useful by the customers. Naturally, it was difficult to determine this objectively without a thorough quantitative and qualitative study. The Standing Committee I limited itself to a thorough inspection of the documents and conducted a survey among several agents from the Operational Departments and Analysis Departments and a number of representatives of other services involved in the problem of sects. According to the Committee, the analysis reports and summary memorandums demonstrated an impartial and rigorous approach; they were well-substantiated, objective and did not make any value judgements about the philosophies developed by the sects. In general, the representatives of other services also found the work done by State Security in this matter to be relevant, and even essential. Especially the broader approach to the phenomenon of harmful sects was welcomed. Since the police services usually limit themselves to monitoring only those sects that pose a problem for public order or at the judicial level. However, the customers of State Security indicated that, in their opinion, the service deploys insufficient staff resources for monitoring the sects. The competence and goodwill of the new analysts of the 'Sects' service within State Security (see below) were certainly appreciated. But, according to the interviewees, these qualities were not enough to compensate for the lack of relevant experience.

II.2.3.2. Newsletter

Since 2007, State Security also sends a periodic newsletter entitled '*Cultic Overview*' to the Minister of Justice, the IACSSO and the members of the Office of the Administrative Coordination Cell. This document contains general and current information, taken from open and therefore unclassified sources, about organisations considered as sectarian and harmful and which are active in Belgium as well as abroad.

II.2.4. STAFF RESOURCES

In 2006, the Working Group responsible for Monitoring the Recommendations of the Parliamentary Inquiry Committee on Sects explicitly pointed out the lack of staff at State Security.[33] What was the situation in 2010?

Within the 'Security' pillar of the Operational Departments of State Security, there is a division specially entrusted with the monitoring of harmful sectarian

[33] *Parl. Doc.* House of Representatives 2005–06, no. 51K2357/1, 11.

organisations. Over the years, the staffing of this division has considerably decreased as a result of transfers, retirement and because agents who left the service were not replaced. Though the number of staff in this division increased again in 2010, it did not reach the 1999 level.

The staff of the Provincial Posts monitor the sects within their respective sectors. As far as possible, each Provincial Post makes the necessary efforts to act on the written orders issued by the Analysis Department. The approach towards and importance of the topic of 'harmful sects' differ greatly from post to post. The activity in the provinces in this area depends largely on the staffing of each post and the opportunities and priorities defined by the management of the concerned post.

As with the central service of the Operational Departments, the Analysis Department has a special division for monitoring harmful sects. In recent years, a number of transfers have led to a significant reduction in staffing. Since 2010, the number of staff in this service is again the same as in 2000.

II.2.5. COOPERATION WITH VARIOUS PLAYERS

The report of the Working Group responsible for Monitoring the Recommendations of the Parliamentary Inquiry Committee on Sects identified a clear lack of coordination between the services involved in dealing with sects, both in terms of gathering and exchanging information as well as at the operational level.[34] The Standing Committee I questioned some of the privileged partners of State Security regarding this.

II.2.5.1. Cooperation with the IACSSO

There appeared to be a good relationship between the Information and Advisory Centre on Harmful Sectarian Organisations and the Analysis Department of State Security. In 2008, State Security established a structural cooperation with this Centre. Discussions are held between the two services, where unclassified information and analyses on ongoing investigations are exchanged in a rather informal manner. The IACSSO is also a recipient of the newsletter entitled '*Cultic Overview*'.

II.2.5.2. Cooperation with the Administrative Coordination Cell

The Administrative Coordination Cell occupies a privileged place in the relations between the individuals and authorities involved in combating harmful sectarian organisations. The Cell consists of an Office and a Plenary Session.

---

34 *Parl. Doc.* House of Representatives 2005–06, no. 51K2357/1, 10.

The Office is composed of representatives of the Board of Prosecutors-General, the Federal Police, State Security and the GISS. A representative of the IACSSO participates in the meetings of the Office on invitation. The Plenary Session consists of the members of the Office as well as representatives of the Federal Prosecutor's Office and the Federal Public Services for Foreign Affairs, Justice, Home Affairs and Finance. Representatives of the IACSSO and the Communities and Regions (e.g. family services agencies *Office de la Naissance et de l'Enfance* and *Kind & Gezin*) also take part in these sessions on invitation.

Both at the Office and the plenary session, State Security is represented by both its Analysis Department and the Operational Departments. The secretarial services of the Office and plenary session are performed by the representative of the Analysis Department of State Security. The original plan of hiring a person to carry out the secretarial work, who would be on the payroll of the Coordination Cell, has not yet been carried out.

II.2.5.3. Cooperation with the GISS

Since harmful sectarian organisations do not, as such, fall under the competence of the GISS[35], there is no structured or special cooperation with State Security. However, the GISS also receives the '*Cultic Overview*' and it sometimes questions State Security regarding the sectarian and harmful nature of religious movements in the context of security investigations. In return, the GISS immediately sends all sect-related information which occasionally comes to its notice to the Administrative Coordination Cell within which State Security is represented.

II.2.5.4. Cooperation with the CUTA

The report of the Working Group responsible for Monitoring the Recommendations of the Parliamentary Inquiry Committee on Sects also mentioned that the CUTA should receive all useful information on sectarian practices that could be a threat to the country.[36] However, the Standing Committee I noted that the Threat Assessment Act of 10 July 2006 does not include the threat posed by harmful sectarian organisations as such under the assessment tasks of the CUTA. Despite this, during 2007 and 2008, State Security sent memorandums to the CUTA with answers to requests for information regarding public demonstrations related to a sect.

---

35 This is the case, however, if such sects could endanger the military security of the country.

36 *Parl. Doc.* House of Representatives 2005–06, no. 51K2357/1, 41.

II.2.5.5. Cooperation with the Federal Police

State Security and the police services have formal work agreements only with regard to 'radicalism' and not with regard to sectarian movements. However, the lack of a general protocol agreement has not been – at least according to the discussion partners – an obstacle to good cooperation in this field. For example, there are meetings between representatives of both services within the Administrative Coordination Cell, agents from the Operational Department sometimes gather information from the local police and from the 'District Information Crossroads' (free translation) (AIK/CIA) of the Federal Police and the services also work together in the context of criminal investigations (Art. 20 §2 of the Intelligence Services Act) involving sects.

II.2.5.6. Cooperation with the judicial authorities

The cooperation with judicial authorities also occurs at various levels.

If, in the context of its intelligence mission, State Security establishes that a criminal offence has been committed, it is obliged to inform the Public Prosecutor thereof (Art. 29 of the Code of Criminal Procedure). Between 2007 and 2009, this happened several times in the context of monitoring certain sects (evidence of child prostitution, drug trafficking and the organisation of forced convenience marriages). In addition, as part of ongoing judicial inquiries, State Security occasionally provides general information, e.g. with regard to the possible use of banned psychotropic substances and suspected convenience marriages with the intention of obtaining Belgian nationality (Art. 19 of the Intelligence Services Act).

Finally, there is the issue of technical assistance (Art. 20 §2 of the Intelligence Services Act). Such assistance is provided in accordance with the procedure described in the Circular COL 12/2005. In principle, each Public Prosecutor's Office of First Instance has a reference magistrate who is competent for harmful sectarian organisations.[37] In practice, all requests for assistance are sent in writing to State Security. If the Analysis Departments are unable to respond to the request immediately, an agent from the Operational Department and an analyst are entrusted with the dossier. These are the contact persons who participate in coordination meetings convened by the magistrate. Usually, the assistance provided consists in helping the magistrate gain a better insight into the structure of a movement, the persons involved therein, *modi operandi*, links with criminal environments, modes of financing, etc. However, this assistance

[37] In the Federal Prosecutor's Office as well, a magistrate has been specifically entrusted with the task of managing sect-related dossiers. The cooperation between State Security and the Federal Prosecutor's Office occurs primarily in the context of the Administrative Coordination Cell.

may also include the verification of the authenticity of certain documents in the dossier, providing information about the author(s) of some of the documents or providing instructions that allow to verify the authenticity of the statements of certain individuals.

II.2.5.7. Cooperation with foreign intelligence services

As established by the Working Group responsible for Monitoring the Recommendations of the Parliamentary Inquiry Committee on Sects[38], coordination between various countries in the context of dealing with harmful sectarian organisations is not always easy. This is due to differing views on sects and the manner in which one should respond to them. Moreover, Belgium is one of the few countries where an intelligence service is explicitly entrusted with monitoring harmful sects. Most democratic countries do not want their intelligence services to be involved in monitoring religious movements, as this might be interpreted as an attack on the freedom of religion. If the intelligence services of some European countries show any interest at all in sects, this is only insofar as these organisations interfere in domestic affairs or proclaim extremist opinions. The contacts and information exchange between State Security and its foreign counterparts are, therefore, limited to the organisations which (can) pose such threats.

II.2.6. CONCLUSIONS

The Intelligence Services Act of 30 November 1998 states that '*the safety and physical and moral freedom of individuals*'[39] (free translation) are interests which State Security must safeguard if this is threatened by, among others, harmful sectarian organisations. This means that the service is authorised to monitor any sectarian tendency targeted against individuals and families, as well as activities that a sect might develop against the State, its institutions or the collective security. This approach – which may seem strange for a service which is traditionally focused on the security of the State rather than the safety of individuals – was also apparently adopted by the Working Group responsible for Monitoring the Recommendations of the Parliamentary Inquiry Committee on Sects: '*the sectarian issue is special, in the sense that it is not so much the protection of the interests of the State (the most important task of State Security) but also – and above all – the protection of the individual that is at stake. If an*

38 *Parl. Doc.* House of Representatives 2005–06, no. 51K2357/1, 29.

39 These interests are an integral part of the '*internal security of the State and the survival of the democratic and constitutional order*' as stated in Article 8, 2° of the Intelligence Services Act.

individual is harmed, then this naturally also harms the community within which he or she lives' (free translation).[40]

The Standing Committee I has established that State Security – given its limited staff resources – gives priority attention to the harmful sectarian organisations that constitute a threat to the State and its democratic functioning. While the Committee understands this decision, it also immediately adds that the unpredictability and uncertainty that characterise some organisations with a philosophical or religious purpose, or those that appear to be such, justify the constant vigilance of State Security with regard to their practices and abuses against individuals and families.

The monitoring of sects can come into conflict with the freedoms of religion and association. Under no circumstances may State Security obstruct the exercise of these freedoms and the Committee was given the task of effectively monitoring this. In practice, it is seen that State Security operates on the basis of objective and relevant criteria, which are used as a touchstone in qualifying a movement, and the service sets priorities depending on the severity of the threat.

The Standing Committee I is, therefore, convinced that State Security, in its monitoring of harmful sectarian organisations, has not violated any rights which the Constitution and the law confer on individuals. The Committee appreciates the manner in which the service has cooperated with other concerned bodies and believes that, given the limited number of staff, it has acted efficiently.

II.3. PROTECTION OF CLASSIFIED INFORMATION AND PERSONAL DATA OUTSIDE OF SECURE SITES

In December 2007, the Standing Committee I decided to open an investigation into the *manner in which the GISS protects classified information and/or personal data outside of secure sites*. This was because the military intelligence service encountered four incidents in which personal data was lost and/or classified information was compromised.[41] All these incidents took place outside of 'secure sites'. These are sites '*primarily intended for handling and storing classified documents and protected by a security system intended to prevent access by any unauthorised persons*' (Art. 1, 7° of the Royal Decree on classification and security clearances, certificates and advice – free translation). Despite their

40 *Parl. Doc.* House of Representatives 2005–06, no. 51K2357/1, 17.

41 These incidents involved three cases of theft from vehicles and one incident caused by force majeure (a fatal traffic accident).

rather sporadic nature[42], such incidents are potentially detrimental to the proper functioning and image of an intelligence service.

In its investigation, the Standing Committee I examined these four incidents and how they had been handled. In this context, it also tested the security procedures implemented within the GISS against the prevailing regulations.

The rules applicable to situations where GISS employees are required to move classified and/or personal data outside of a secure site, are spread out over various legal sources. For many years now, in addition to the existing, generally applied regulatory framework[43], security instructions are issued by the Armed Forces in general and by the GISS in particular.[44] These instructions are clear, feasible and easy to understand. However, the Standing Committee I concluded that the focus of these instructions lies mainly on the protection and safeguarding of classified information. This is understandable given the context, namely the intelligence environment. Nevertheless, it should not be forgotten that purely personal data processed in the intelligence context also enjoys special legal protection.

The existence and contents of the above-mentioned laws, instructions, regulations and orders are made known to all members of the GISS during a general security briefing when they join the service. Partly as a result of earlier recommendations of the Standing Committee I, briefings for raising awareness are subsequently organised on a regular basis. Therefore, it may be reasonably assumed that these instructions are known to the staff.

Despite this, it should be noted that the way in which the individuals were dealt with *in casu*, was not in conformity with the procedures. For example, the rule that classified documents must never be left in public places, was not uniformly observed. Also, in only one case was it really necessary to take the data carriers outside of the secure site. In all other cases, it had been entirely advisable, from a security point of view, to leave the data (or classified objects) at the secure site.

However, the Committee found that the required internal reporting obligation had always been respected. Procedures for conducting investigations into these security incidents had also been strictly followed within the GISS.

---

42 In 2004, another security incident by the GISS had already been the subject of an investigation (STANDING COMMITTEE I, *Activity Report 2005,* 37–45). But from the end of 2007 until the termination of the present investigation at the end of 2010, no new incidents of similar nature were reported.

43 The Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data, the Act of 11 December 1998 on classification and security clearances, certificates and advice, the Royal Decree of 24 March 2000 implementing the Act of 11 December 1998 on classification and security clearances and the Directive of 21 May 2001 of the Ministerial Committee for Intelligence and Security defining the minimum requirements for the storage of classified documents outside of secure sites.

44 The IF5 Regulation on military security, the *Standing Operating Procedures*, the *Intelligence Summary* and the intake brochure for new GISS employees.

On the other hand, it appeared that the GISS had only reported one case to the judicial authorities. The remaining omissions were apparently not deemed serious enough. The Standing Committee I was of the opinion that, in view of a possible criminal prosecution, it is not the responsibility of the GISS to assess this; the power to assess this expediency falls under the sovereign authority of the Public Prosecutor's Office.

Finally, the Standing Committee I established that these security incidents had resulted in personal data of contacts and persons who were subjects of a security investigation, being lost. In none of these cases had the individuals concerned been informed of this by the GISS because of reasons of expediency. At present, in the absence of appropriate provisions, the risks faced by the service and those faced by the individual concerned are considered on a case-by-case basis. However, this should be done more meticulously since an incorrect assessment could undoubtedly compromise the civil-law liability of the Belgian State.

This investigation has primarily shown that the incidents were caused by the manner in which individual staff members had dealt with the applicable regulations. As already concluded in the investigation of 2004, it again appears that the human factor is, and remains, the weakest link in any security system.

II.4. COMPLAINT AGAINST SURVEILLANCE OPERATIONS PERFORMED BY STATE SECURITY

In February 2009, the Standing Committee I received an anonymous complaint from within State Security referring to an ongoing surveillance operation at State Security that was allegedly problematic in light of earlier recommendations of the Standing Committee I.

During 2006, in two of its investigations, the Standing Committee I had found that State Security had been requested to carry out tasks falling outside its legal scope of competence.[45] *In concreto*, this involved tasks for localising individuals with another purpose than to strengthen the information position of State Security. At that time, the Standing Committee I had concluded that an intelligence service has every reason to avoid giving the impression that it can be used as *passe-partout* whenever another public service fails to or cannot intervene. Therefore, the intelligence services were advised that, in case of doubt regarding the legality of a task, it should carry out an objective (legal) analysis and officially inform the competent minister(s) of this. If necessary, the service or the Minister could consider obtaining the opinion of the Standing Committee I.

---

45 STANDING COMMITTEE I, *Activity Report 2006*, 24–34 and 51–61 (the Erdal and Kimyongür cases).

The complainant was of the opinion that the new surveillance assignment was not legal. *In casu,* at the request of the Policy Office of the then Minister of Justice, an individual who was about to be released from prison, was kept under surveillance for 24 hours immediately after his release. The individual concerned had been detained pending a possible extradition. After the period of surveillance, the service was supposed to go over to 'monitoring'[46] the individual concerned and this was to be continued until the date of the final decision on his extradition. State Security was also requested to inform the concerned sister service if the *target* were to flee the country.

The complaint was clearly prompted by a concern of the operational staff of State Security regarding the legality of the assignments entrusted to them. However, the investigation showed that State Security management had also expressed its own concerns on the matter in the form of a tenable, well-founded and explicitly critical opinion addressed to the competent minister. Since, although State Security immediately and faithfully carried out the assignment, it repeatedly presented arguments *against* this task. For example, the service had warned that a report and subsequent arrest abroad might be perceived as an attempt to circumvent the current extradition procedure and sideline the courts.

The investigation also showed that the individual concerned had been monitored by State Security both before and after the ministerial order. This monitoring was legitimate. Hence, from the perspective of a good intelligence operation, it had also been advisable to localise him. State Security often allowed their efforts to coincide with the times when the individual's case came up for hearing. This is by no means illogical, since the individual was expected to make an appearance at those moments. The Committee has also noted that there was never a permanent surveillance of the individual concerned.

Therefore, in the opinion of the Standing Committee I, State Security has also acted correctly and cautiously in this case. The Committee was pleased to note that State Security has evidently incorporated the previous recommendations from the Erdal and Kimyongur cases in its organisational culture. However, the Standing Committee I is not authorised to comment on

---

46 At the time of the investigation, the terms 'surveillance', 'tailing' or 'monitoring' were not mentioned in the Act of 30 November 1998. Precisely due to this reason and having regard to Article 8 of the ECHR and Article 22 of the Constitution, until recently there had been disagreement regarding whether the intelligence services could use such methods. The Standing Committee I has repeatedly stated that surveillance or shadowing by intelligence services should be defined through further legal regulations (see e.g. *Activity Report 2006*, 31 (footnote 35), 59 and 79). In the same context, see Corr. Brussels, 16 February 2006, Chamber 54*bis* and W. VAN LAETHEM, '*Een (on)duidelijke regeling voor de observatiebevoegdheid van de Veiligheid van de Staat*', *R.W.* 2008–2009, 1635–1638 (note under Cass. 27 June 2007). *Contra*: Brussels 19 January 2007, 12th Chamber, *Criminal Law Journal.* 2008/4, 281 and Cass. 27 June 2007, *R.W.* 2008–09, 1634–1635. The SIM Act of 4 February 2010 has meanwhile resolved this issue by explicitly granting the intelligence services the power to carry out surveillance assignments. Therefore, the investigation did not go further into this aspect.

the actions or instructions of the competent ministers. Moreover, the intelligence services are obliged to effectively execute the orders issued by their supervisory authorities if these authorities stand by their position unless, of course, these orders were to be manifestly illegal.

II.5. ADVISORY OPINIONS IN THE CONTEXT OF THE EXPORT OF HIGH-TECH EQUIPMENT TO IRAN

In May 2009, the Minister for Climate and Energy was questioned in the House of Representatives about the export of a 'tabletting machine for graphite' (a rotary press for making graphite tablets) to Iran in 2005. Apparently, the Advisory Committee for the Non-Proliferation of Nuclear Weapons (CANVEK/CANPAN) had initially issued a positive opinion in this dossier, which was later changed to a negative opinion. The Minister replied that while the original order did not imply any risk of nuclear proliferation, the change in the order had given rise to such a risk.[47] Although he found the Minister's answer to be sufficiently clear, the then President of the Senate still wanted an investigation to be conducted into the role of State Security in the dossier in question and, if possible, into whether the control procedures had been respected by all.

Naturally, the Standing Committee I is not authorised to issue a technical opinion regarding the recommendations of the CANVEK/CANPAN and neither is it competent to assess the legitimacy of the decisions of the competent authorities regarding the export of equipment. Therefore, the investigation was limited to the question of whether the intelligence services were in possession of relevant information and analyses regarding the dossier and whether they provided the competent authorities with this information and the analyses in the appropriate manner.[48]

II.5.1. FACTS

The CANVEK/CANPAN is a body which must advice the competent Regional Minister prior to the export of *nuclear materials, nuclear equipment, nuclear*

47 *Annals* House of Representatives, 2008–2009, 52 COM 557, 12 May 2009, no. 13174, 23.

48 In this investigation, the Committee requested both State Security and the GISS for a copy of the minutes of meetings of the CANVEK/CANPAN. The GISS immediately provided the requested documents. However, State Security stated that, under the rules of procedure of the CANVEK/CANPAN, it was not authorised to provide these documents without the prior consent of the CANVEK/CANPAN. The Committee could not agree with this view since Article 33 of the Review Act grants the Committee the right to consult all documents it considers necessary for the performance of its task.

technology information and derivatives thereof.[49] This advisory body consists of twelve members, including a representative of State Security and the Minister of Defence (i.e. an officer of the Armed Forces as a full member or a member of the GISS as his substitute).

On 1 March 2005, the CANVEK/CANPAN had to look into the matter of a licence to export a rotary press to an Iranian company. This meeting was attended by representatives of State Security and the GISS. The latter drew the attention of the Advisory Committee to a number of important points. In his opinion it was not impossible that, in cases where the requested equipment did not include properties required for nuclear applications, Iran could adapt this equipment locally or could obtain the additional material required for such applications from other sources.

The State Security representative had additional information at his disposal: in the past, France had already refused an export licence to the Iranian company in question in an export dossier related to high-purity graphite blocks.

However, partly on the basis of detailed, technical information communicated by the exporter, the CANVEK/CANPAN unanimously decided that the machine could not be used for nuclear purposes. Since, as a result of this, the equipment in question no longer fell under either the '*guidelines*' of the *Nuclear Suppliers Group*[50] or relevant Belgian legislation, the CANVEK/CANPAN declared itself incompetent.[51] It therefore did not formulate any recommendations and the dossier was forwarded, along with the minutes of the meeting, to the appropriate Regional Minister. The Minister decided that no prior licence was needed for the equipment in question. In the course of 2005, the Belgian exporter delivered the press to the Iranian company.

In April 2006, the same company received a new order from the Iranian company, this time for spares and chased parts for the previously delivered rotary press. Subsequently, the company submitted a new licence application to the CANVEK/CANPAN. The Secretariat of the Advisory Committee referred the exporter to the Flemish Region for further investigation. In July 2006, the Flemish Government informed the exporter that no licence or export control

---

49 The Act of 9 February 1981 governing the conditions for the export of nuclear materials, nuclear equipment and technological information and the Royal Decree of 12 May 1989 governing the transfer of nuclear materials, nuclear equipment, nuclear technology information and derivatives thereof to non-nuclear countries.

50 See in this regard STANDING COMMITTEE I, *Activity Report 2005*, 29.

51 In this dossier, the CANVEK/CANPAN has strictly limited itself to its legal competence to advise on the export of nuclear weapons and nuclear equipment. Therefore, it has not expressed an opinion regarding the possible ballistic applications of the equipment ordered by Iran, since this aspect falls under the Missile Technology Control Regime (MTCR) and not under the Non-Proliferation Treaty. The MTCR is an informal grouping of countries that endorse the non-proliferation of unmanned carriers of weapons of mass destruction and try to coordinate the national efforts of the member countries to prevent the proliferation of such carriers through national systems of export licenses.

was required. In order to execute the order, the Belgian company asked its customer for the blueprints of the desired parts. While reviewing these documents, the manufacturer concluded that there might be a problem. The exporter sent this additional information to the Secretariat of the CANVEK/CANPAN.

Based on these new elements, the Secretariat again submitted the export licence application to the members of the CANVEK/CANPAN. The dossier was discussed during the meeting of 27 October 2006. However, since the GISS representative was abroad during this period on a four-month assignment, the military intelligence service was not represented at this meeting. No substitute was sent because no other employee of the service had the necessary scientific skills. Therefore, the GISS did not give its advice in this matter.[52]

The CANVEK/CANPAN issued a negative advisory opinion. According to the Advisory Committee, the new application was related to products mentioned in the Annexes to the Royal Decree of 16 July 1993 which meant that their export was subject to special conditions. This is why the second order of the Iranian company was blocked.

In this investigation, the Standing Committee I concluded that both State Security and the GISS had relevant information and analyses related to the order of equipment by an Iranian company. This information had, moreover, been made available to the competent authorities, i.e. the CANVEK/CANPAN, the Minister of Justice[53], certain foreign intelligence services and, via the minutes of the CANVEK/CANPAN, to the competent regional authority. Therefore, in this case they have proved that they actually improved the exchange of information with the competent Belgian authorities (such as the CANVEK/CANPAN and the Minister of Justice), despite not having been specifically ordered to do so by the competent ministers or the Ministerial Committee for Intelligence and Security. Based on this, the Committee was of the opinion that *in casu* both intelligence services acted in accordance with the assignment entrusted to them with respect to the fight against proliferation.

II.5.2. MONITORING OF THE EXPORT OF EQUIPMENT TO SO-CALLED 'STATES OF CONCERN'

Partly based on previous investigations into the proliferation issue, the Committee has gained an insight into the general approach of the two

52 Nevertheless, the GISS explicitly stated that the Ministry of Defence representatives had subsequently been informed of the case and the conclusions of the CANVEK/CANPAN. Since they were in agreement with the advisory opinion, they did not raise any objections.

53 In November 2006, State Security had sent a memorandum to the Minister of Justice to inform him of the export dossier.

intelligence services with respect to the export of equipment to so-called 'states of concern'.

Within the GISS, there is a division dedicated to regularly monitoring the evolution of certain dossiers with respect to the proliferation of weapons of mass destruction and their carriers. Certain countries are the focus of special attention in this respect. The GISS is aware of the strategies adopted by these countries to circumvent export control systems. The Committee was of the opinion that the GISS has a thorough command of all aspects of this matter (strategic, diplomatic, political, economic, scientific, technical and military).

With respect to the proliferation of weapons of mass destruction and missiles, State Security pays special attention to certain countries. State Security is aware that these countries try to obtain the knowledge, technologies and products required to produce such weapons, from Belgium. To circumvent embargoes and control procedures, roundabout methods are used to obtain this equipment and knowledge – for example, by using front companies to order 'dual-use' products. Some countries do not hesitate to make use of their intelligence services for this purpose. Therefore, from this perspective, it is obvious that State Security, along with other competent authorities, should be involved in the monitoring processes.

II.5.3. MANNER IN WHICH PREVIOUS RECOMMENDATIONS OF THE STANDING COMMITTEE I WERE IMPLEMENTED

The Standing Committee I has repeatedly formulated recommendations regarding the role to be played by Belgian intelligence services in the fight against proliferation.[54] Consequently, the Committee took advantage of this investigation to draw up a report of the current status.

II.5.3.1. Better cooperation with other public services

Although they did not receive any special instructions from their respective competent ministers and the Ministerial Committee for Intelligence and Security, both State Security and the GISS proved in this case that the exchange of information with the competent authorities had progressed very well.

However, according to the Standing Committee I, it would be best to strengthen the cooperation between the competent authorities through the conclusion of cooperation agreements between the intelligence services, the CANVEK/CANPAN and the regional authorities.

54 STANDING COMMITTEE I, *Activity Report 2005*, 16 and *Activity Report 2008*, 43 ff.

II.5.3.2. Exchange of classified information within the CANVEK/CANPAN

The Standing Committee I had recommended that it should be possible for the intelligence services and administrations represented within the CANVEK/CANPAN to exchange classified information. This required the members of the CANVEK/CANPAN, its staff and correspondents in the Administration of Customs and Excise to hold a security clearance. The Royal Decree of 9 December 2008 stipulated that all effective, substitute and acting members should be holders of such a clearance.

But the fact that classified information *may* be shared, does not, of course, mean that this is actually happening. Therefore, the Committee recommended that the services in question should conclude an agreement thereto under Article 14 of the Intelligence Services Act. To the extent that the Committee could verify, there is still no protocol between the intelligence services and other services represented within the CANVEK/CANPAN.

State Security does not see any point in entering into a cooperation agreement with the CANVEK/CANPAN. The Committee, however, believes that this is necessary in order to determine how classified data can be forwarded to members of this Advisory Committee in a secure manner.

II.5.3.3. Continuity of representation in the CANVEK/CANPAN

The Standing Committee I had also recommended that it should be ensured, as far as possible, that the same persons guarantee the continuity of the representation of the intelligence services in the CANVEK/CANPAN and that, in the absence of the permanent representative, his substitute should be informed about the dossiers and advisory opinions handled by the permanent representative.

The Standing Committee I regrets that the only employee of the GISS entrusted with this matter could not be replaced by a competent person at the meeting of the CANVEK/CANPAN on 27 October 2006. The Committee can therefore only reiterate its recommendation that the GISS should be able to guarantee its representation at all the meetings of the CANVEK/CANPAN.

II.5.3.4. Adequate human and material resources

The Standing Committee I has urged that the GISS and State Security be assigned adequate human and material resources to enable these services to perform their legal assignments in the fight against the proliferation of non-conventional and very advanced weapons systems. In relation to this, the Standing Committee I once again emphasised in its *Activity Report 2008* that both intelligence services were assigning too few employees to this task. The Committee was deeply concerned about this situation. But had the situation improved?

The number of staff in the new division within State Security, who is responsible for proliferation and for the contacts with companies involved in this issue, was significantly increased in 2008.

At the assessment level, the proliferation issue is handled by a service which was also entrusted with the task of monitoring the protection of the scientific and economic potential and organised crime. A restructuring of the Analysis Department was made possible thanks to the recruitment plans of 2003 and 2004. These recruitments have helped to gradually fill up the vacant staff positions.

However, the Standing Committee I regretted the fact that it had to once again conclude that the GISS had a clear shortage of staff for this task.

In 2008, the GISS recruited new statutory staff and the division responsible for the assessment of cross-border phenomena was somewhat strengthened.

The Standing Committee I believes that this measure is not sufficient to deal with all aspects of the problem. Furthermore, the recruitment criteria defined for the examinations do not always help attract people with the specific scientific skills required for monitoring this particular field. Moreover, the Standing Committee I is still unsure whether the salary level for the position of an analyst at the GISS is sufficient to attract highly qualified scientists.

II.6. COMPLAINT OF TWO PRIVATE INDIVIDUALS IN THE CONTEXT OF A 'NATIONALITY DECLARATION' PROCEDURE

In September 2009, a couple filed a complaint with the Standing Committee I. The complainants wished to obtain Belgian nationality on the basis of the procedure detailed in Article 12*bis* of the Belgian Nationality Code. This request was rejected. Information received from State Security was allegedly the reason for this refusal.

The Standing Committee I limited its investigation to the information collected, processed and presented by State Security to the Public Prosecutor, as it is not competent to verify or assess the advisory opinions and decisions of judicial authorities.

II.6.1. LEGAL FRAMEWORK

According to the above-mentioned Article 12*bis*, the registrar of births, marriages and deaths who receives a nationality declaration, is obliged to send a copy of the dossier to the Public Prosecutor '*for advice*'. The Public Prosecutor has four months to issue a negative opinion, if necessary. This opinion must be

justified on the basis of '*important facts, specifically related to the person*'. The precise implications of this are explained in a number of ministerial circulars.[55] If the Public Prosecutor issues a negative opinion, the individual concerned can appeal to the Court of First Instance. This Court will issue a judgement on the merits of this opinion. Appeal to a higher court is possible against the decision of the Court of First Instance.

Besides the Public Prosecutor's Office and the courts, there are two other bodies involved in the 'nationality declaration' procedure: Article 12*bis* requires the registrar of births, marriages and deaths to send a copy of the dossier to the Immigration Service and to State Security. However, for these two services, the Belgian Nationality Code does not specify the kind of intervention expected from them or the period within which they must respond. These aspects are also regulated in the ministerial circulars. These circulars state that the two services have a period of two months to submit their '*comments, if any,*' to the Public Prosecutor.

In practice, the service within State Security responsible for dealing with nationality declarations and applications will verify whether the name of the applicant appears in State Security documentation. If this is not the case, the Public Prosecutor is immediately informed. If his name does appear, then the application is passed on to the Analysis Department of State Security. This service assesses which comments need to be brought to the notice of the Public Prosecutor and which do not. A further investigation is started if the Analysis Department considers this useful. The Public Prosecutor is notified of this.

Usually, the Analysis Department provides non-classified information; sometimes even at the explicit request of the Public Prosecutor. But what if classified information is sent? The Classification Act of 11 December 1998 does not stipulate that a nationality applicant should be able to consult classified information that State Security has brought to the notice of the Public Prosecutor. The same applies to the elements contained in the State Security investigation dossier.

II.6.2. FACTS

In casu, the names of the two complainants appeared in State Security files. Moreover, the Analysis Department considered it appropriate to carry out an additional verification. As usual, the competent magistrate from the Public Prosecutor's Office was informed accordingly.

---

55 For example, the existence of a criminal conviction of the applicant for Belgian nationality might be an important fact. But this is not necessarily so in all cases. Therefore, everything must be assessed on a case-by-case basis.

But State Security did not provide any additional data within the legal period of two months. Despite this, the Public Prosecutor – who is bound by a period of four months – found that there were sufficient elements to justify the formulation of a negative opinion. In one of the cases, he justified his opinion by pointing out that the individual concerned had been the subject of an investigation by State Security.

II.6.3. CONCLUSIONS

The Standing Committee I concluded that State Security had not provided the Public Prosecutor with any element whatsoever that could be considered as '*important facts, specifically related to the person*' which could form an obstacle to the acquisition of Belgian nationality.

In addition, the Committee questioned whether conducting an additional investigation as a result of a nationality declaration procedure is legally permitted. In any case, such an investigative option is not explicitly defined anywhere; in addition, it cannot be regarded as a security investigation or verification pursuant to the Classification Act.

Nevertheless, the Committee decided that the investigation *in casu* was also part of the general intelligence mission of State Security as defined in Article 7, 1° of the Intelligence Services Act: '*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 […]*' (free translation). Moreover, the Committee was of the opinion that the information already available to State Security amply justified an intelligence investigation.

In addition, there was the question of the use of classified information. In this case, the Committee concluded that the classification had hindered the communication of relevant information to the Public Prosecutor. It was not sufficiently clear to the Standing Committee I whether the classification can form a legal obstacle to the transfer of information to the Public Prosecutor's Office and to the use of such information in the context of a non-judicial inquiry. In this respect, the Committee stressed that the classification may also have repercussions for the person: how can he then defend himself when appealing against a negative opinion?

Finally, the Committee drew attention to the short period available to State Security for formulating its comments. This was not always sufficient for collecting, analysing and providing correct and relevant information to the competent magistrate from the Public Prosecutor's Office.

II.7. INFORMATION POSITION OF THE INTELLIGENCE SERVICES WITH REGARD TO THE RIOTS IN BRUSSELS

At the end of August and early September 2009, serious rioting took place in several municipalities in the Brussels suburbs. During the riots, the police came across Molotov cocktails and Kalashnikovs. In mid-September 2009, there were further incidents. During these incidents, policemen were injured and (police) vehicles damaged.[56] France, Greece and Canada also faced similar problems of urban violence. Open sources revealed that this problem had attracted the attention of various foreign intelligence services.

At the request of the then President of the Senate, an investigation was initiated into '*the monitoring by State Security and the GISS of the phenomena/groups/persons involved in the riots in the capital in 2009 and the weapons possessed by these persons*' (free translation).

II.7.1. MONITORING OF THE RIOTS BY THE INTELLIGENCE SERVICES

The investigation revealed that the General Intelligence and Security Service did not monitor either the city gangs that participated in the riots or the possible arms trafficking in Belgium in relation to these events.

Also, State Security did not specifically monitor the problem of youth gangs. There was no comprehensive investigation of the riots that took place in 2009 in Brussels. The information gathered was extremely general in nature and it said that the incidents had originated in unidentified criminal circles. Neither were any links to Islamist extremist circles found and no specific information could be gathered with regard to possible arms trafficking. State Security justified the fact that it had not specifically monitored the events by pointing out that these were activities of gangs of a purely criminal nature and therefore outside the scope of its competence. The service argued that the lack of an ideological component made it decide that monitoring this issue fell outside its intelligence mission.

---

56 The riots in Brussels were repeatedly the subject of debates in the House of Representatives and the Senate (see e.g. *Parl.Doc.* House of Representatives 2008–09, no. 52K643; *Parl.Doc.* House of Representatives 2009–10, no. 52K778; *Annals* Senate 2009–10, 5 February 2010, no. 4–111).

II.7.2. COMPETENCE ISSUE

Pursuant to Article 11 of the Intelligence Services Act, which defines the competence of the GISS, it appears that this service was in no way competent in the matter of the riots or the weapons discovered during these riots.

But for State Security, the issue of competence is more complex. The service itself was of the opinion that no elements had been observed to imply that the riots fell within its core task as defined in Article 7, 1° of the Intelligence Services Act. Since, there were no clear ideological factors linking the riots to 'extremism' or 'terrorism'.

The Standing Committee I arrived at a more nuanced point of view. State Security is competent to monitor '*any individual or collective activity, developed at home or from abroad, which may be related to […], interference, terrorism, extremism, proliferation, […], criminal organisations*' (free translation).

'Proliferation' is '*the traffic in or transactions with respect to materials, products, goods or know-how which can contribute to the production or development of non-conventional or very advanced weapon systems*' (free translation). A possible trafficking in Kalashnikovs cannot be equated to this. Regarding the possible link with 'terrorism' and 'extremism', the lack of a precise 'ideological component' led State Security to conclude that it had no competence in this matter. This conclusion may indeed be a deciding factor. However, this component is not a prerequisite under the section for 'criminal organisations'. Pursuant to Article 8, 1°, f) of the Intelligence Services Act, such organisations must also be monitored if they '*could have a destabilising effect at a political or socio-economic level*'(free translation). It was *prima facie* not impossible that the riots had been deliberately provoked by organised criminal gangs and that these could, due to their impact on the social fabric, have a destabilising effect at a political and socio-economic level (*no go* areas, closing of schools, etc.). According to the Standing Committee I, State Security should have at least made a thorough analysis of the causes and consequences of the riots, in order to assess whether or not they were competent in this matter.

In addition, the Standing Committee I believes that the riots may also, in principle, be regarded as attempts by groups to create certain areas within the capital that were no longer under the authority of the administrative or judicial authorities and in other words, convert these areas into neighbourhoods where these groups were in control. This could be regarded as a form of interference pursuant to Article 8, 1°, g) of the Intelligence Services Act: '*the attempt to use illegal, fraudulent or clandestine means to influence decision-making processes*' (free translation).

Therefore, the Standing Committee I came to the conclusion that it was not that State Security, *a priori* and *prima facie*, had no competence in this matter.

II.7.3. CONCLUSIONS

The answer to the question of the President of the Senate clearly stated that the intelligence services did not monitor the riots (and the possession of weapons by the persons involved therein) which broke out in Autumn 2009 in certain municipalities in the Brussels suburbs. Both services were of the opinion that they were not competent in this matter. With regard to the GISS, the Standing Committee I shares this view. With regard to State Security, the Committee was of the opinion that the service should have investigated its competence further.

However, more than the question of the basis on which the intelligence services were or were not competent to monitor such phenomena, the Standing Committee I was far more concerned about the fact that these events would be seen merely as issues of public order and that, due to the lack of clear ideological motives of the rioters, State Security would not get involved in this matter. In the opinion of the Committee, this was due to the severity and scale of the riots. It is more than understandable that State Security has priorities other than the monitoring of juvenile troublemakers. But the riots, as they occurred, demonstrated a worrying trend, as was apparent from the attacks targeted against public services, the possession of heavy weapons, etc. According to almost all observers, the riots were related to a very specific, complex social context. But the behaviour of the gangs was, in itself, unacceptable because they threaten the principles of peaceful coexistence in the capital and can lead to the escalation of serious violence in several difficult neighbourhoods, and even in other cities. Therefore, several public services had the responsibility to contain this threat.

The Standing Committee I was of the opinion that State Security did not have a leading role to play in combating the phenomenon. Such a role was obviously the preserve of the police services, as part of their administrative and judicial function, while acting under the orders of their respective supervisory authorities. However, the Committee felt that State Security should monitor this issue, make its interest in this issue known and hence, be notified of all the factual elements by the other services in question.

II.8. HOUSING PROBLEMS OF STATE SECURITY PROVINCIAL POSTS

During 2008, as part of the investigation into the manner in which State Security performs its legal task with regard to harmful sectarian organisations[57], the Standing Committee I visited the eight provincial antennas of this service. Together with the Central Service in Brussels, these form the Operational

[57] See Chapter II.2.

Departments of State Security. They are responsible for providing the information to the Analysis Department based (only) in Brussels.

During these visits, the Committee found that the offices of some of the Provincial Posts were in a poor condition. During the discussion with the Heads of these posts, the Standing Committee I expressed concern about this, assuming that this signal would prompt the State Security management to take action.

In October 2009, the Standing Committee I asked the Administrator-General of State Security about any initiatives that had been taken to improve working conditions in the posts. It appeared that the situation of the unenviable and even unsafe housing of the offices of some employees of State Security remained critical, although concrete actions were pending and in 2007, State Security had apparently issued a '*Guideline for the security of the office buildings of State Security*' (free translation) (the focus, according to the title, being on *security* and not *safety*).

According to the Administrator-General, the continuing delays in remedying this situation could be entirely attributed to the Administration responsible for the public buildings, which allegedly had to contend with all kinds of administrative and budgetary problems.

Since the failure to create a decent work environment for all employees of State Security is a factor that can compromise the efficiency of the service, the Committee decided to start an investigation, although there were indications that the causes of the malaise were external to State Security. The following survey questions were asked: 'What is the state of the housing of the Provincial Posts of State Security?' and 'If this appears to be unsuitable, what is the reason for this, what specific solutions have been planned and by when will they be implemented?' Therefore, the scope of the investigation did not involve the security of the buildings. As mentioned earlier, State Security had already taken the necessary initiatives thereto from 2007 onwards.

In globo, very differing situations were observed, both in the accommodation as well as in the layout of the Provincial Posts. Whereas the Central Services in Brussels – except the garage – have been housed since the mid-nineties in modern, relatively comfortable and fairly functional office spaces, most of the decentralised units continued to be treated in a step-motherly fashion. A turning point came under the present management, for whom the '*Guideline for the security of the office buildings of State Security*' and the subsequent *security* audits appear to have served as a leverage for efforts to improve well-being and *safety* at the workplace. This commitment to the revaluation of the Provincial Posts is also reflected in the Strategic Plan 2008–2012, which provides for an increase in staff at these antennas. This has further increased the need and pressure to ensure adequate and appropriate locations.

At the time of concluding the present investigation, some members of State Security still had to carry out their tasks in premises where it was dangerous to

work and which, so to speak, appeared to no longer meet any of the standards. This compromises the responsibility of the Belgian State. The Standing Committee I found it utterly incomprehensible that a public service, which is regarded as crucial in the security chain, is unable to guarantee a basic level of well-being and physical safety at the workplace for all its employees.

However, after the finalisation of the investigation report, in preparation for a meeting with the Parliamentary Monitoring Committee, it was found that substantial progress had been made and that the Administration responsible for the public buildings had made significant efforts in this respect. For example, the Provincial Posts in the worst state had been permanently closed and transferred to a properly renovated building. For three other posts, a relocation operation was in full swing. This was expected to be completed in 2011. Only one Provincial Posts showed no improvement; here, the renovation works had been stopped since 2007.

II.9. LEGALITY OF A PARTICULAR INTELLIGENCE METHOD USED BY STATE SECURITY

During an investigation, the Committee found that State Security had certain information regarding a target who was suspected of illegal intelligence activities. The Standing Committee I wanted to assess whether State Security had come into possession of this information using lawful means.

The investigation initiated hereto showed that information was obtained from private individuals who, in providing this information, had ignored an obligation of confidentiality for which there were penal sanctions.

However, State Security was of the opinion that this transfer of information was possible pursuant to Article 16 of the Intelligence Services Act. This provision allows the intelligence services to obtain personal data necessary for carrying out their tasks from any person or organisation belonging to the private sector. Citing various passages from the preparatory activities[58], State Security argued that Article 16 of the Intelligence Services Act is a legal exception to obligations of confidentiality. But these passages were only related to Article 14 of the Intelligence Services Act.[59] Indeed, this last provision does provide the option of setting aside an obligation of confidentiality or professional secrecy. But this is only applicable to (officials of) public services who want to pass on

---

58 *Parl. Doc.* House of Representatives 1995–96, no. 49K638/20, 4; *Parl. Doc.* Senate 1997–98, no. 49–758/5, 5 and *Parl. Doc.* Senate 1997–98, no. 49–758/10, 57.

59 '*With due regard for the law, on the basis of any agreements concluded and the rules defined by their supervisory authority, judicial authorities, officials and public service agents may, of their own accord, communicate to the intelligence and security service in question information that is useful for the performance of its tasks*' (free translation).

information to State Security, while the case examined concerned the communication of information by private parties.

The Standing Committee I emphasised that there should not be the slightest confusion about the precise scope of Article 16 of the Intelligence Services Act: the intelligence services *may* obtain information from the private sector, but nowhere does it state that the legal obligations of confidentiality on the part of the respondents are cancelled. The opposite assumption would, for example, imply that a doctor or lawyer may unrestrictedly pass on information protected by the principle of professional secrecy to an intelligence service.

State Security also highlighted the fact that the information came from an 'informant'. Here, it appeared that they were referring to Article 18 of the Intelligence Services Act as a legal ground for exception.[60] The Committee was of the opinion that a private individual who acts as 'human source' is always bound by the obligations of confidentiality applicable to him, if any. For the Committee, the restriction implied in Article 16 of the Intelligence Services Act (see above) may not be circumvented by referring to Article 18 of the same Act.[61]

In this dossier, the Standing Committee I decided that State Security had indeed acted efficiently in the context of its legal assignments, but it had not come into possession of the data in a lawful manner.

However, since 1 September 2010, i.e. the day on which the SIM Act of 4 February 2010 came into effect, this intelligence method in question is permitted, albeit subject to strict administrative conditions and judicial control.

II.10. INFORMATION MANAGEMENT BY THE MILITARY INTELLIGENCE SERVICE

At the end of November 2005, an investigation was initiated into the manner in which the military intelligence service manages and uses the information it obtains. In this respect, the existing instructions were examined and clarifications sought about the way in which the GISS processes the personal data it receives.

The initial reason for starting this investigation was because it was found that, in an actual case, there had been a lack of information flow between the pillars *Intelligence* and *Counterintelligence*. It soon became clear that the fragmentation within the GISS was so great was that each division had its own system of data management and storage. There was absolutely no sign of an integrated information management system. Neither was it possible to establish direct links

60 '*In the exercise of their tasks, the intelligence and security services may call upon human sources for gathering information on events, subjects, groups and natural or legal persons who show an interest in the performance of their tasks, in conformity with the guidelines of Ministerial Committee*' (free translation).

61 See also W. VAN LAETHEM, 'Kan, mag of moet een inlichtingendienst op uw medewerking rekenen?', *Vigiles* 2004, Vol. 4, 117 and 120.

between the various management systems. The very limited exchange of information between the divisions also explained why it was possible for a person to be known to one division but, therefore, not necessarily to another division.

However, the GISS had announced plans to fundamentally change the structure of the service in order to resolve this problem. With this in mind, it was decided in 2008 to suspend the investigation until after the implementation of the proposed reforms. In 2009, concrete plans were duly communicated to the Standing Committee I. But when a progress report was requested at the beginning of 2010, it appeared that the reform had been limited to a few small changes. The reasons cited for this were varied: budgetary constraints, not a high priority project for the military hierarchy, the tendency of the divisions to 'protect' their respective data, internal resistance to the reorganisation, etc.

Despite the goodwill shown by the GISS management, the Committee was forced to conclude that there was a shortcoming in the reform process. The Committee regretted the fact that five years after the discovery of an important lacuna in the information management system of the GISS, considerations of a budgetary nature, coupled with internal resistance, had prevented the required information system from being introduced. This situation is such that it compromises the proper execution of the tasks of the GISS. This was the reason for including the information management problem in the military intelligence service audit started in 2010.[62]

II.11. INVESTIGATION INTO ALLEGATIONS AGAINST THE DIRECTOR OF THE CUTA

In September 2009, an anonymous complaint was sent to the Committee. Mention was made of several problems with regard to the operation of the CUTA, problems that had arisen since the arrival of the new director. Therefore, the Standing Committees P and I initiated a joint investigation into these allegations. However, no dysfunctions were found. The file was therefore closed in 2009 and a report included in the Activity Report.[63]

However, in early 2010, an anonymous letter introduced a new element in the context of the completed investigation and in connection with two threats performed by the CUTA for a Belgian company involved in important projects abroad. These assessments were followed by two statements issued by the CUTA to private companies with regard to the risks of terrorist or extremist actions faced by these Belgian companies in a particular country. The Crisis Centre, the FPS Mobility, the FPS Home Affairs and the Security Advisor of the Prime Minister were aware of this initiative.

---

62 See Chapter II.12.11.

63 STANDING COMMITTEE I, *Activity Report 2009*, 45.

According to the CUTA, these assessments and briefings were part of its responsibilities as defined in Article 3 of the Threat Assessment Act of 10 July 2006. Both Committees did not completely subscribe to this point of view: the question arose whether the service provided was in compliance with the provisions of Article 10 of the Threat Assessment Act, which states that threat assessments are intended for public authorities and not private companies.

II.12. REVIEW INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2010 AND REVIEW INVESTIGATIONS INITIATED IN 2010

This section contains a list and brief description of all review investigations initiated in 2010 and those review investigations continued during the operating year 2010 but which have not been completed as yet.

II.12.1. PROTECTION OF COMMUNICATION SYSTEMS AGAINST POSSIBLE FOREIGN INTERCEPTIONS AND CYBER-ATTACKS

The problem of protecting information and telecommunication systems managed via new IT technologies has regularly come up for discussion in the Federal Parliament. The security of these systems is essential in an information-based society. The current interception possibilities not only constitute a possible threat to the security, military interests and economy of a country, but also to the fundamental rights and freedoms of citizens. The Monitoring Committee of the Senate expressed the desire to be kept informed by the Standing Committee I about the manner in which the intelligence services monitor these developments. It also wished to receive an update of the Echelon Report presented by the Standing Committee I in 2000.[64]

All these elements resulted in the decision of the Standing Committee I at the end of December 2007 to initiate an investigation into '*the manner in which the Belgian intelligence services consider it necessary to protect communication systems against foreign interception*' (free translation). This investigation was started in 2008 and numerous investigative steps have already been taken. The Committee did not focus so much on the actual facts leading to the initiation of

64 See STANDING COMMITTEE I, *Activity Report 2000*, 29–60 (Summary report of the investigation into the manner in which the Belgian intelligence services respond to the possible existence of an American system, named Echelon, for the interception of telecommunications in Belgium).

the investigation, but rather on the general problem of protecting communication systems against possible foreign interceptions. Since then, the investigation has been extended to include threats from cyber-attacks.

In 2009, the remarks of the intelligence services were published in an initial interim report, various briefings were organised and additional investigative actions were performed.

The final investigative steps were taken in 2010 (including the questioning of the National Security Authority) and a report was drafted which was approved in February 2011.

II.12.2. A MISSION ABROAD PLANNED BY THE CUTA

The Standing Committee I learned that the Coordination Unit for Threat Assessment had planned a foreign mission in the course of 2009 which, however, had been abandoned at the last minute. In the plenary session of the Standing Committees I and P of June 2009, it was decided to initiate a joint investigation into this proposed mission. Although the mission in question had been cancelled, both Committees considered it useful for the future to determine whether, in general, undertaking certain foreign missions is part of or results from the tasks assigned to the CUTA by the legislator. The investigation also aims at verifying whether, from the point of view of coordination and effectiveness, the CUTA had taken the necessary preparations and precautions, both internally and externally, and whether these were appropriate to the specific situation of the country to be visited.

The investigations were completed during 2010 and published in a joint final report in January 2011.

II.12.3. EVALUATION OF THE MANNER IN WHICH STATE SECURITY PERCEIVES ITS ROLE IN THE FIGHT AGAINST PROLIFERATION AND THE PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL

The Standing Committee I had already conducted various investigations into the manner in which the intelligence services carry out the fight against proliferation[65] and the protection of the scientific and economic potential (SEP).[66] In both these matters, State Security has an extremely important role to play

---

65 For example, see STANDING COMMITTEE I, *Activity Report 2005*, 9–28; *Activity Report 2008*, 42–57 and Chapter II.5. of the present report.

66 For example, see STANDING COMMITTEE I, *Activity Report 2008*, 60–66; *Activity Report 2005*, 67 and *Activity Report 2005,* 24–133 and 134–138.

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) persons. Moreover, the interests in the fight against proliferation and those with regard to the protection of the SEP do not always necessarily coincide. In this investigation, the Standing Committee I wants to determine, on the basis of an actual case, whether State Security has worked meticulously in this context. The chosen case offers the opportunity to carry out an assessment that covers a fairly long period.

The investigation could not be completed in 2010.

II.12.4. BELGIAN REPRESENTATION AT INTERNATIONAL MEETINGS ON TERRORISM

The Belgian police and intelligence services and the CUTA regularly participate in international meetings on the fight against terrorism. The question arises, however, whether the participation at these meetings is organised efficiently and effectively and the extent to which there are coordinated agreements in this respect. To answer this question, in accordance with Article 53, 6° of the Review Act, the meeting of the Standing Committees I and P decided in November 2009 to initiate a joint investigation into '*the participation at international meetings on the fight against terrorism by the Belgian police and intelligence services, the CUTA and the supporting services of the CUTA*' (free translation).

The final report was approved in the first half of 2011.

II.12.5. INVESTIGATION WITH REGARD TO THE ACTIVITIES OF THE GISS IN AFGHANISTAN

Belgian military troops take part in various operations abroad, for example, in Afghanistan, where the troops are part of the International Security Assistance Force (ISAF). They are active in Kabul, Kunduz and Kandahar. The major part of the Belgian troops in the Afghan capital consists of a protection company for the international airport. In Kunduz, Belgium provides support to the provincial reconstruction teams and provides *Operational Mentoring and Liaison Teams*. In Kandahar, Belgium contributes to the military effort with F-16s.

At the end of 2009, the Standing Committee I received a briefing from the GISS regarding the local situation. From this it appeared that this service had used various intelligence methods (HUMINT, OSINT, IMINT, SIGINT, etc.) and worked closely together with the intelligence services of other countries. In order to get a complete picture (and to develop a possible frame of reference), the Committee decided in early 2010 to open an investigation into '*the role of the GISS in monitoring the situation in Afghanistan*' (free translation). This

investigation included topics such as the deployed personnel, intelligence methods used, cooperation with foreign intelligence services as well as the transmission of information.

II.12.6. COMMUNICATION OF INTELLIGENCE TO THE CUTA BY THE SUPPORTING SERVICES

Information originating from the so-called 'supporting services' – i.e. State Security, the GISS, police services, Administration of Customs and Excise, Immigration Service and the FPS Mobility & Transport and Foreign Affairs – constitute the main source of information for the CUTA. The legislator requires these services '*to communicate to the CUTA, at their own initiative or at the request of the Director of the CUTA, all information they possess in the context of their legal tasks and which is relevant for performing the tasks defined in Article 8, 1° and 2°*' (Art. 6 of the Threat Assessment Act – free translation). Each of these departments or services must organize a central contact point thereto (Art. 11 RD CUTA).

For a considerable time now, the Standing Committees P and I had planned to dedicate a special report on the supply of information by these supporting services. In early July 2010, this plan was made concrete through the initiation of a joint investigation.

II.12.7. MONITORING OF A PERSON DURING AND AFTER HIS DETENTION IN BELGIUM

According to a press article from the British newspaper *The Independent*[67], a terrorist of Moroccan nationality who was convicted in connection with the Nizar Trabelsi trial in Belgium and who was serving his sentence in the prison of Forest, had allegedly been put under pressure by an agent of the British secret service. This news report was extensively covered in the Belgian press. It was alleged that the man in question was illegally transferred to the United Kingdom and 'imprisoned' at a secret base where he was interrogated and forced to work for the British secret service. According to his lawyer, this operation could not have happened without the approval, if not knowledge, of the Belgian intelligence services as well as the Federal Prosecutor's Office.

The Standing Committee I thereupon decided to open an investigation into '*the possible monitoring of a person (M.J.) by State Security and the GISS during and after his detention in Belgium*' (free translation). The results of the investigation will be presented to the Monitoring Committee in 2011.

67 *The Independent*, 23 July 2010.

II.12.8. PUNCTUAL ANALYSES BY THE CUTA IN THE CONTEXT OF VISITS OF FOREIGN PERSONALITIES

In October 2010, the Standing Committee I, together with the Standing Committee P, initiated an investigation into '*the threat assessment performed by the CUTA with respect to the visit of foreign personalities to Belgium*' (free translation). The figures cited by the CUTA in its annual reports suggested that such punctual analyses imply a huge investment in time and resources for this service. In this respect, the Committees focused their attention on the legality of this task and the scope (*workload*) for the CUTA. The difficulties faced by this service were also examined.

The investigations have been completed. The final report is expected in 2011.

II.12.9. COMPLAINT BY AN EMPLOYEE AND HIS SPOUSE AGAINST STATE SECURITY

In August 2010, the Committee received a complaint from a member of State Security and his spouse. The complaint was directed against State Security and concerned three aspects of the internal functioning of the service.

Because the complainant had also appealed against the revocation of his security clearance to the Appeal Body for Security Clearances, Certificates and Advice, the Standing Committee I decided to suspend the investigation (Art. 3 of the Appeal Body Act). These investigations could only be resumed after the end of the appeal procedure, in the spring of 2011.

II.12.10. INFORMATION POSITION OF THE INTELLIGENCE SERVICES WITH RESPECT TO A SUSPECTED TERRORIST

On 10 September 2010, a bomb exploded (prematurely) in a hotel in Copenhagen. A few hours after the explosion, the Danish police arrested the alleged perpetrator. The man was identified as Lors Doukaev, a Belgian national of Chechen origin. The Standing Committee I opened an investigation into '*the information position and actions taken by the Belgian intelligence services with respect to a suspected terrorist*' (free translation). The aim of this investigation is to determine what information and intelligence the Belgian intelligence services had in their possession with respect to this suspected terrorist prior to the events of 10 September 2010.

The final report of the Standing Committee I will be prepared in the autumn of 2011.

II.12.11. AUDIT OF THE MILITARY INTELLIGENCE SERVICE

At the request of the Monitoring Committee of the Senate, at the end of November 2010, the Standing Committee I initiated an '*audit with a view to identifying and verifying the conditions necessary for the effective use of resources at the GISS, with particular attention paid to the leadership and management of staff, information flows and risk management*.' (free translation)

The following questions were addressed in the audit:

- what are the conditions for the effective use of resources of the GISS and are these met?
- how are the GISS staff led and managed?
- how do the information flows occur?
- what are the possible risks?

The audit was started by drafting an audit plan and developing a well-founded methodological basis. The audit was divided into four phases. A first phase (exploratory talks and an interview with management and staff of the GISS) could be completed as early as 2010. The next steps are the written staff survey (phase 2) and feedback to the GISS and, based on in-depth interviews with managers and other resource people, the testing and closer examination of the identified issues (phase 3). Finally, a report will be drawn up (phase 4). This is planned for in the autumn of 2011.

II.12.12. ADVISORY OPINIONS ISSUED BY STATE SECURITY IN THE CONTEXT OF NATURALISATION APPLICATIONS

One of the questions that came up in the so-called Belliraj case[68] was how State Security might have intervened in the naturalisation of this person. This is an item to which the members of the Monitoring Committee of the Senate returned in detail when discussing the investigation in November 2010.

In line with this discussion, the President of the Senate requested the Standing Committee I to open an investigation '*into the manner in which and the circumstances under which State Security investigates and handles requests for information regarding procedures for obtaining Belgian nationality*' (free translation). This investigation, which includes a legal, descriptive and quantitative section, is expected to be completed in the course of 2011.

---

68 STANDING COMMITTEE I, *Activity Report 2009*, 30–40.

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS

On 4 February 2010, the King signed the so-called SIM Act[69], which eventually came into force on 1 September 2010. This Act has provided the two Belgian intelligence services with an extensive additional arsenal of special (specific or exceptional) powers. The SIM Act is thus the final piece of the legal framework of the intelligence services. Until this Act, there was no comprehensive regulation to govern their powers.

This situation was rightly perceived as being undesirable. On the one hand, the Belgian intelligence services remained too dependent on their foreign counterparts, while certain threats increased in intensity. On the other hand, the lack of an explicit legal basis for the (covert) collection of data was also a problem in the context of the ECHR. Since, the actions of an intelligence service usually entail an infringement of the privacy of citizens, which is protected under Article 8 of the ECHR. For these reasons, an amendment to the legislation was required.

This new 'Chapter III' of the Activity Report will address the special intelligence methods and the new role assumed by the Standing Committee I in this regard. Since, Article 35 §1, 1° of the Review Act, as amended by Article 25 of the SIM Act, specifies that, in its annual Activity Report, the Committee must devote *'particular attention to the specific and exceptional intelligence collection methods, as intended in Article 18/2 of the Intelligence Services Act of 30 November 1998 [and] to the implementation of Chapter IV/2 of the same Act'* (free translation), this being the new controlling task of the Standing Committee I.

The Standing Committee I has decided to fulfil this obligation by preparing an abbreviated version of the half-yearly reports it is required to draw up for the Monitoring Committee of the Senate[70] under Article 35 §2 of the Review Act.[71]

---

69 Act of 4 February 2010 on the data collection methods of the intelligence and security services, *Belgian Official Journal* 10 March 2010.

70 Article 66*bis* §2, third paragraph of the Review Act, as amended by Article 28 of the SIM Act, specifies that the half-yearly report is intended for the Monitoring Committee of the Senate.

71 Article 35 §2: *'Every six months, the Standing Committee I shall report to the Senate on the implementation of Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services. A copy of this half-yearly report shall also be presented to the Ministers of*

For a clear understanding, the key aspects of the SIM Act are outlined below.[72]

III.1. A BRIEF INTRODUCTION TO THE SIM ACT

III.1.1. THE VARIOUS INTELLIGENCE METHODS

The coming into force of the SIM Act has created a distinction in the Intelligence Services Act between three types of powers, i.e. ordinary, specific and exceptional data collection methods, grouped according to the potential seriousness of the infringement of the rights and freedoms of citizens. Within each group, the application conditions, safeguards and control mechanisms are largely the same, but there are significant differences between the individual groups.

III.1.1.1. Ordinary data collection methods

The 'old' powers, that were already included in the Intelligence Services Act before the SIM Act, are now grouped under the term 'ordinary intelligence methods'. For the most part, they have not undergone any substantial changes. Specifically, these methods include:

- requesting information from public authorities (Art. 14 of the Intelligence Services Act);
- obtaining information from private organisations and individuals (Art. 16 of the Intelligence Services Act);
- entry into places accessible to the public (Art. 17 of the Intelligence Services Act);
- use of human sources (Art. 18 of the Intelligence Services Act);
- observation and searching of public places or private places accessible to the public insofar as no technical devices are used (Art. 16/1 of the Intelligence Services Act).

Justice and National Defence, who shall have the opportunity of drawing the attention of the Standing Committee I to their comments.
The report shall contain the number of authorisations granted, the duration of the exceptional intelligence collection methods, 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' (free translation).

72 Not all aspects of the SIM Act are covered here. For a full analysis, see: W. VAN LAETHEM, D. VAN DAELE en B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

Only these last powers are new.

No special application conditions have been established for the ordinary methods, in the knowledge, of course, that these methods may only be used in the context of the assignments of the services. Within these limits, therefore, an intelligence officer may always apply the ordinary methods at his own initiative.

III.1.1.2. Specific data collection methods

All specific data collection methods are new. More specifically, these include:

- entry into and observation of or in places accessible to the public using a technical device (Art. 18/2 §1, 1° and 18/4 of the Intelligence Services Act);
- entry into and searching of places accessible to the public using a technical device (Art. 18/2 §1, 2° and 18/5 of the Intelligence Services Act);
- inspection of identification data of postal traffic and requesting the cooperation of a postal operator (Art. 18/2 §1, 3° and 18/6 of the Intelligence Services Act);
- inspection of identification data of electronic communication, requesting the cooperation of an operator, or direct access to data files (Art. 18/2 §1, 4° and 18/7 of the Intelligence Services Act);
- inspection of call-associated data of electronic communication and requesting the cooperation of an operator (Art. 18/2 §1, 5° and 18/8 of the Intelligence Services Act);
- inspection of localisation data of electronic communication and requesting the cooperation of an operator (Art. 18/2 §1, 5° and 18/8 of the Intelligence Services Act).[73]

The conditions for the application of all specific methods are largely the same. Firstly, State Security may use these methods only in the context of its intelligence work. Hence, specific methods may not be used for protection assignments, security investigations or verifications or for the remaining tasks assigned to it by or in implementation of another law. The GISS too may use the specific methods only for its intelligence work and not, for example, for security investigations. Secondly, the specific methods may only be used within Belgian territory. Thirdly, the use of specific methods is only allowed if the ordinary methods are considered insufficient for the task and the actual specific method must always be selected depending on the degree of seriousness of the potential

[73] Although the inspection of call-associated data and localization data of electronic communication are dealt with in the same section of the Act, the two methods have a different objective: the first method provides information on who has communicated with whom, when and for how long, while localization aims at monitoring the movements of a target. In this sense, the latter method is more a form of surveillance.

threat. Therefore, the use of these methods is subject to the principles of subsidiarity and proportionality. Fourthly, the use of a specific method always requires a written and reasoned authorisation from the Head of Service of the intelligence service in question.

Finally, the Act provides for a three-fold control of the implementation of the specific methods. Firstly, the intelligence officer appointed to apply the specific method must keep his Head of Service regularly informed regarding the implementation. Additional control is carried out by the SIM Commission during the implementation of the specific methods (see III.1.2) and by the Standing Committee I during and after the completion of the implementation (see III.1.3.1).

III.1.1.3. Exceptional data collection methods

Exceptional data collection methods include:

- observation of private places not accessible to the public, private residences or professional premises of a lawyer, doctor or journalist (Art. 18/2 §2, 1° and 18/11 of the Intelligence Services Act);
- searching of private places not accessible to the public, private residences or professional premises of a lawyer, doctor or journalist (Art. 18/2 §2, 2° and 18/12 of the Intelligence Services Act);
- establishment of legal entities and collection of intelligence under cover (Art. 18/2 §2, 3° and 18/13 of the Intelligence Services Act);
- opening and inspecting post (Art. 18/2 §2, 4° and 18/14 of the Intelligence Services Act);
- collection of bank details (Art. 18/2 §2, 5° and 18/15 of the Intelligence Services Act);
- penetration of an IT system (Art. 18/2 §2, 6° and 18/16 of the Intelligence Services Act);
- interception of communications (Art. 18/2 §2, 7° and 18/17 of the Intelligence Services Act).

The conditions for the application of the exceptional methods are similar on a number of points to those of the specific methods. For example, the use of these methods is also limited to the Belgian territory and within the context of the intelligence work. However, threats arising from extremism or interference do not justify the use of exceptional methods by State Security. The principles of subsidiarity and proportionality must also be taken into consideration and any persons, objects or events constituting the subject of the method must be of demonstrable importance for the performance of the assignments of the intelligence service.

However, in the context of exceptional methods, a special authorisation procedure is applicable: the Head of Service draws up a 'draft authorisation' that becomes effective only after the SIM Commission has given its assent. For this, the Commission shall first determine whether the legal provisions for the method in question have been observed (see III.1.2).

Finally, the Act provides for a four-fold control of the implementation of the exceptional methods. First, the intelligence officer appointed to apply this method must keep his Head of Service regularly informed regarding the implementation. In certain cases, the Head of Service is obliged to discontinue the use of the exceptional method. In addition, just as for the specific methods, additional control is carried out by the SIM Commission during the implementation of the exceptional methods (see III.1.2) and by the Standing Committee I during and after the completion of the implementation (see III.1.3.1).

III.1.2. CONTROL BY THE SIM COMMISSION

In order to control the specific and exceptional intelligence methods (and not the ordinary methods) the legislator has created a new administrative body: the SIM Commission. This Commission is composed of three active members serving in the capacity of magistrates.[74] The Commission takes a decision by majority vote and is completely independent in its decision-making.

In principle, the SIM Commission does not intervene in decisions regarding the use of special methods. It only controls the legality, subsidiarity and proportionality of the methods from the moment they are authorised for use until their discontinuation. For this, the members of the Commission may enter any premises where data related to the specific or exceptional method is received or stored by the intelligence services, appropriate any relevant documents and hear the members of the services. If the SIM Commission finds that intelligence has been obtained under circumstances that are non-compliant with the legal provisions in force, it forbids the exploitation of this data and suspends the method used, if this is still ongoing. It also notifies the Standing Committee I of this without delay.

There are two exceptions to the rule that the SIM Commission does not, in principle, play any role in taking decisions regarding the use of the methods: if the intelligence service wishes to apply a specific method against a lawyer, a doctor or a journalist or wishes to apply an exceptional method,

74 The members are appointed by the King on a motion of the Ministers of Justice and Defence and after deliberation in the Council of Ministers. The Chairman is an examining magistrate. The other two members are a sitting magistrate and a magistrate from the Public Prosecutor's Office.

then the Commission verifies in advance whether the 'draft authorisation' for the intelligence service is legal, subsidiary and proportional. If the verification is positive, the SIM Commission gives its assent and the method may be used. The SIM Commission must give its opinion within four calendar days after receiving the draft.[75] If the Commission fails to deliver an opinion within this deadline, this does not mean that the intelligence service is allowed to use the method; it merely means that the service in question may, if desired, approach its responsible Minister, who may authorise (or not) the method.[76]

If the SIM Commission does not give its assent, the exceptional method may not be used. The SIM Commission informs the Standing Committee I of each request for authorisation and its advice.

In addition to its own controlling task, the SIM Commission also plays a key role at the crossroads between legal action and intelligence work. For example, the intelligence services have an obligation to inform the SIM Commission each time they open an investigation that may have a repercussion on an ongoing criminal investigation or judicial inquiry. The SIM Commission then decides – in consultation with the Federal Prosecutor's Office or the competent magistrate and the Head of the service concerned – whether and under which rules the intelligence service may pursue its investigation. The Standing Committee I must be informed thereof.

In addition, a special procedure has been provided for the application of the reporting obligation with respect to crimes, which applies to all civil servants. When the use of specific or exceptional methods reveals serious indications of a crime or offence or raises reasonable suspicions regarding criminal offences which have been planned or have already been committed but not yet revealed, the intelligence services must report this to the SIM Commission. If the latter finds such indications or suspicions, it must draw up a non-classified report, to be immediately passed on to the Public Prosecutor or the Federal Prosecutor. This non-classified report may eventually be included in a criminal dossier. If case of doubts regarding the legality of the manner in which the intelligence having resulted in this report have been gathered, the advice of the Standing Committee I may be requested (see III.1.3.2).

---

75 For extremely urgent cases and when any delay in taking a decision will jeopardize certain critical interests, the prior assent of the Chairman of the Commission shall be sufficient. However, this approval is then valid for a maximum of forty-eight hours.

76 In this case, the Minister communicates his decision to the Chairman of the Commission and to the Chairman of the Standing Committee I.

III.1.3. TWO NEW TASKS OF THE STANDING COMMITTEE I[77]

III.1.3.1. Task of controlling specific and exceptional methods: the Committee as a jurisdictional body

The new controlling task of the Standing Committee I is limited to the specific and exceptional methods; it is not related to the ordinary methods. The Committee is authorised to initiate its controlling task as soon as an authorisation is issued or assent given and it retains this power during the entire implementation period of the method as well as after its discontinuation.

In concrete terms, the Committee must – just as the SIM Commission – rule on the legality of the authorisations to use special methods, as well as on the compliance with the principles of proportionality and subsidiarity. Therefore, in principle, the control by the Standing Committee I includes a test of legality and not an assessment of expediency.

Naturally, this control is only done in the dossiers which the Committee has been officially referred to in a matter. There are various ways in which the Committee can be referred to in a matter.

Firstly, the Committee is considered as being automatically referred to if the SIM Commission has suspended a specific or exceptional method due to illegality or if the competent Minister has taken a decision in the absence of a timely opinion from the SIM Commission. Secondly, the Committee may be referred to at the request of the Privacy Commission.[78] But citizens may also entrust the Committee with a certain matter: anyone who can demonstrate a personal and legitimate interest may file a complaint to the Committee. This complaint must be made in writing under penalty of nullity and state the grievances. All complaints will be looked into, unless they are manifestly unfounded. Finally – and this is important – the Committee may also intervene at its own initiative. In order to determine the dossiers in which such intervention seems appropriate, the Committee must, of course, have all the necessary permissions. This is why the SIM Act states that the Standing Committee I must be immediately notified by the competent authority of all decisions, advice and authorisations relating to specific and exceptional methods and of the so-called monthly listings containing additional information on the specific methods actually implemented in that month.

---

77 For detailed information, please refer to P. DE SMET, 'Checks and balances. A priori en a posteriori controle' in W. VAN LAETHEM, D. VAN DAELE en B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 93–118.

78 This request must be made in conformity with the rules contained in Article 14 of the Royal Decree of 12 October 2010 on the implementation of various provisions of the Intelligence Services Act of 30 November 1998, *Belgian Official Journal* 8 November 2010.

Unless the Committee rules otherwise, its intervention does not imply a suspension of the method in question.

Once the Committee has been referred to, the legislator grants the Committee all the facilities required for a thorough control. Firstly, the Committee must have access to the complete files of the intelligence service in question and of the SIM Commission. In addition, the Committee is authorised to hear the members of the SIM Commission and the members and the Head of Service of the intelligence services which have used the specific or exceptional methods.[79] During these hearings, the members of the intelligence services are obliged to inform the Standing Committee I of any secret information in their knowledge. If this secret information is related to an ongoing criminal investigation or judicial inquiry, the Standing Committee I shall first consult the competent magistrate. If the member of the intelligence service believes that the secret information to which he is privy may not be disclosed because such disclosure would be prejudicial to the protection of the sources, the protection of privacy of third parties or prejudicial to the implementation of the assignments described in Articles 7, 8 and 11 of the Intelligence Services Act, the matter shall be submitted to the Chairman of the Standing Committee I, who shall rule after hearing the Head of Service. In the context of its controlling task, the Standing Committee I may even entrust investigation assignments to its Investigation Service. In this case, this service shall have all the powers granted to it by the Review Act, such as the power to carry out useful observations, enter premises where intelligence officers perform their duties, confiscate documents, request assistance from public authorities, etc.

If the Standing Committee I has been referred to as a result of a complaint, the complainant and his lawyer shall be heard at their request. They may consult the dossier at the secretariat of the Standing Committee I. This dossier must contain all relevant information and intelligence, with the exception of any elements that impair the protection of sources, the protection of privacy of third parties, the classification rules or the performance of the assignments of the intelligence services. Nevertheless, the dossier that is accessible to the complainant and his lawyer shall at least include the following:

- the legal framework that has justified the use of the specific or exceptional data collection method;
- the nature of the threat and the degree of seriousness that have justified the use of the specific or exceptional method;
- the type of personal data collected during the use of the specific or exceptional method insofar as this personal data is only related to the complainant.

---

79 The hearing shall always take place in the absence of the complainant, if any, and his legal adviser.

From the time it is referred to, the Standing Committee I has a month to make its decision.[80]

If the Committee finds an irregularity, it may recommend the discontinuation of the method (possibly suspended by the Commission), forbid the exploitation and order the destruction of any intelligence already collected. On the other hand, if the Standing Committee I finds that a specific or exceptional method is in accordance with the legal provisions while the SIM Commission had forbidden the exploitation of the collected data, both the prohibition and suspension shall be cancelled.

If the decision was the result of a complaint from a citizen, the complainant shall be informed of the decision taken by the Committee. However, information that could constitute a violation of certain fundamental state interests[81], shall be excluded from the copy of the decision communicated to the complainant. A similar approach shall be used if the decision contains information that could compromise the secrecy of the information involved in the (criminal) investigation.

No appeal is possible against the decisions of the Committee.

III.1.3.2. Task of controlling the legitimacy of intelligence used in criminal cases: the Committee as a pre-judicial advisory body

The criminal court[82], faced with an unclassified report in a dossier (see III.1.2), may request the Standing Committee I for written advice on the legitimacy of the intelligence method used to collect the information in the report.

The judge either acts *ex officio*, by order of the Public Prosecutor's Office or at the request of the accused, the civil party or their lawyers. This demand or request must be put forward, at the risk of forfeiture, before any other remedy at law.[83] The court will then send the dossier to the Public Prosecutor's Office, which must, in its turn, refer to the Standing Committee I.

The actual decision regarding legitimacy lies with the acting judge, as well as the decision on the consequences he wishes to attach to any irregularity.

---

80 There is no penalty if this period is exceeded.

81 More specifically, this involves the protection of the inviolability of national territory, military defence plans, performance of the assignments of the armed forces, the safety of Belgian nationals abroad, internal security of the State, including aspects relating to nuclear energy, the maintenance of democratic and constitutional order, external security of the State and its international relations, operation of the decision-making bodies of the State and the protection of sources or the privacy of third parties.

82 This refers to the judges in the Council Chamber and in the Indicting Chamber, in the Correctional Courts and Courts of Appeal and the presiding judges of the Assize Courts.

83 There is one exception to this rule: i.e. if the remedy at law relates to concrete or new elements which have come to light during the (court) session.

III.2. CONCLUSIONS FROM THE FIRST HALF-YEARLY REPORT

The first report prepared in implementation of these provisions covered the period from 1 September 2010 (the date on which the SIM Act came into effect) to 31 December 2010.[84] The text was sent to the Monitoring Committee of the Senate in the beginning of January and discussed at the meeting of 16 February 2011. Given the sensitivity of the information it contains, the report was classified for 'restricted'. For the same reason, the present (public) Activity Report does not include all aspects. This was also clearly not the intention of the legislator: the reporting to the Monitoring Committee of the Senate (Art. 35 §2 of the Review Act) must be much more extensive than the information contained in the annual Activity Reports of the Standing Committee I (Art. 35 §1, 1° of the Review Act).

The Activity Report does address the following topics: the preparations made by the Standing Committee I pending the entry into force of the SIM Act, the difficulties that occurred during the implementation, certain numerical data related to the special methods and finally, the activities of the Standing Committee I as a jurisdictional body. The Activity Report ends with some tentative conclusions.

III.2.1. PREPARATIONS BY THE STANDING COMMITTEE I

From the publication of the SIM Act in the Belgian Official Journal of 10 March 2010 to its entry into force on 4 January 2011, the Standing Committee I has prepared itself intensively for its new and important task.

Firstly, the Committee has drawn up an extensive internal guideline that should enable all SIM dossiers to be handled quickly and uniformly. The guideline clearly lists the tasks of the various components of the Committee: the administrative intake by the secretariat, an initial substantive monitoring by the Investigation Service I, possible legal assistance from the Documentation & Legal Affairs Service, discussion of certain dossiers in the so-called

[84] The Standing Committee I thought it advisable to limit the scope of this first report to a period of four months for two reasons. All provisions of the SIM Act were fully effective from 4 January 2011, since the SIM Commission had been officially set up from this date onwards. Therefore, the following reports shall be related to a period in which the SIM Act was entirely operational. Furthermore, each of these reports will relate to half of a calendar year (1 January to 30 June and 1 July to 31 December).

'Coordination Meeting'[85] and the final decision taken by the Standing Committee I. The instructions attach great importance to the security of the information to be communicated to the Committee in application of the SIM Act.[86] Another topic extensively described is the initial substantive monitoring of the dossiers sent by the Investigation Service I. To enable this monitoring to be conducted in an objective and structured manner, a comprehensive checklist has been drawn up. Each dossier must be reviewed against this checklist, in order to gain an insight into the legality, subsidiarity and proportionality of the measures. If necessary, additional questions and (depending on the information obtained) a proposal for whether or not to intervene, is formulated. Based on these proposals, the Committee decides whether it will make use its power to intervene in the monitoring of a SIM dossier.

Also in preparation for the implementation of the SIM Act, several meetings were set up with the intelligence services. At these meetings the parties involved have provided clarifications in all openness regarding the state of affairs and discussions of the personnel, logistics, financial and organisational challenges have not been avoided. Just before the SIM Act came into effect, a delegation from the Standing Committee I was invited by State Security for a working visit. During this visit, the Committee established that this service had prepared itself for its new tasks in a very serious and professional manner.

The most important other preparatory actions (such as providing advice for implementation decrees, organisation of a seminar, drafting of a SIM reader, update of the website of the Standing Committee I and adding supplements to the Intelligence Services Codex) shall be discussed further in this report.[87]

III.2.2. DIFFICULTIES IN IMPLEMENTING THE SIM ACT

Article 40 of the SIM Act stated that the new provisions would come into effect "*on a date determined by the King and no later than on the first day of the sixth month following that in which the Act is published in the Belgian Official Journal*" (free translation). Since such a Royal Decree failed to materialise, the SIM Act automatically came into effect on 1 September 2010. But the necessary

85 This weekly meeting is composed of the Chairman and councilors of the Standing Committee I, the Secretary, the Head of the Investigation Service I and the Head of the Documentation & Legal Affairs Service.

86 It goes without saying that authorisations for the use of special intelligence methods contain very sensitive information and require a very strict application of the Classification Act. Hence, access to the SIM dossiers is limited to persons involved in the controlling assignment. This is an application of the well-known *need-to-know* principle.

87 See Chapters V.1, V.5, V.9 and V.10.

implementation decrees[88] and the appointment of the administrative SIM Commission[89] were long in coming.[90]

In particular, the absence of the SIM Commission – a vital link in the control of the specific and exceptional methods – created problems for the two intelligence services. Since, the Act states that the specific methods may be used only after a written and reasoned decision taken by the Head of Service and the notification of this decision to the Commission (Art. 18/3 §1, second paragraph of the Intelligence Services Act). For the exceptional methods and the specific methods with respect to lawyers, doctors and journalists, the problem faced was even more complex: these methods may only be used after the SIM Commission has given its assent (Art. 18/3 §1, third paragraph and 18/10 §1 of the Intelligence Services Act). These requirements could evidently not be met.

To avoid compromising ongoing operations, the GISS suggested an interpretation of the SIM Act such that the statutory requirements would apply only to specific and exceptional methods used from 1 September 2010 onwards. The Standing Committee I has argued extensively that this view is not in keeping with the spirit and the letter of the law, as the safeguards linked to the use of intrusive intelligence methods are valid from 1 September 2010. The Heads of Service of the intelligence services conformed to this view and immediately after the entry into force of the Act, they issued a written and reasoned decision for the ongoing methods they wished to continue. But this did not resolve the fact that the specific methods could be used only after notifying the SIM Commission and the exceptional methods only after receiving the Commission's assent.

Regarding the exceptional methods and specific methods with respect to lawyers, doctors and journalists, the Committee judged that, given the legal

---

88 Royal Decree of 26 September 2010 on the secretariat of the administrative commission entrusted with the review of the specific and exceptional methods for data collection by the intelligence and security services, *Belgian Official Journal* 8 October 2010; Royal Decree of 12 October 2010 on the implementation of various provisions of the Intelligence Services Act of 30 November 1998, *Belgian Official Journal* 8 November 2010; Royal Decree of 12 October 2010 on the terms for the legal duty of cooperation in case of requests from the intelligence and security services with regard to electronic communications, *Belgian Official Journal* 8 November 2010.

89 Royal Decree of 21 December 2010 on the composition of the administrative Commission by the intelligence and security services entrusted with the review of the specific and exceptional methods for data collection, *Belgian Official Journal* 24 December 2010, err. *Belgian Official Journal* 12 January 2011. The Commission was composed as follows: Mr. Paul Van Santvliet (Examining Magistrate at the Court of First Instance in Antwerp) (Chairman), Mr. Claude Bernard (Public Prosecutor at the Court of First Instance in Namur) and Mrs. Vivianne Deckmyn (Judge at the Court of First Instance in Mechelen).

90 The failure to appoint the members of the administrative Commission forced the Monitoring Committee of the Senate to adopt a resolution on this matter (draft resolution on the appointment of the administrative Commission entrusted with the review of the specific and exceptional data collection methods of the intelligence and security services, *Parl. Doc.* Senate 2010–11, no. 52–510/2).

requirements, these could not be applied until a SIM Commission had been appointed.

With regard to the specific methods not related to a protected professional category, the Committee agreed that these could be temporarily used in order to safeguard the continuity of the intelligence work. Since, even before the SIM Act, the services (albeit without an adequate legal basis) were carrying out observations using technical devices for example. Simply banning such methods outright, would have been irresponsible. However, the Standing Committee I has closely controlled each decision to use a specific method. This was possible since the Committee had been informed almost immediately[91] of each authorisation. This communication took place directly as far as the GISS is concerned and as far as State Security is concerned, via the Minister of Justice, who signed for inspection.[92] Therefore, it could not be stated that the intelligence services had fewer powers between 1 September 2010 and the installation of the SIM Commission than before this period.

III.2.3. SOME FIGURES WITH REGARD TO THE SPECIFIC METHODS

Between 1 September and 31 December 2010, a combined total of 105 authorisations were granted by the two intelligence services for the use of special intelligence methods: 69 by State Security and 36 by the GISS. It should be noted that a written authorisation by an intelligence service sometimes concerns multiple separate methods. For example, 'observation and searching of the home of person x' or 'observation of persons x and y' are always two separate methods. It is also important to note that certain authorisations which, after the control made by the Committee, actually turned out to be exceptional methods (see III.2.4.2.5), have also been taken into account here.

Below, the figures for the two services are shown separately. Although both services were granted the same new powers, their assignments are so different

91 Initially, it was proposed that the Committee should be notified of the methods used only via the monthly listings (Art. 18/3 §§2 and 3 of the Intelligence Services Act). The Committee has opposed this because this would make any temporary monitoring impossible. Such a manner of working was not in keeping with the spirit of the law and was also a denial of the obligation imposed by Art. 43/3, second paragraph of the Intelligence Services Act to notify the Committee of all decisions regarding specific methods.

92 Since the Ministers of Justice and Defence had submitted a proposal for the composition of the Commission to the Council of Ministers in October 2010, the Minister of Justice did not wish to receive any further authorisations from State Security which he would then have to forward to the Committee. As the final composition of the Commission was still pending, in a number of urgent dossiers the Minister of Justice reverted to his earlier decision of not forwarding any authorisations.

that very few lessons can be drawn by making a comparison between the two services with regard to this aspect.

III.2.3.1. General Intelligence and Security Service

The table below shows the number of specific methods authorised.

NATURE OF SPECIFIC METHOD	NUMBER
Entry into and observation of or in places accessible to the public using a technical device	14
Entry into and searching of places accessible to the public using a technical device	0
Inspection of localisation data of postal traffic and requesting the cooperation of a postal operator	0
Inspection of identification data of electronic communication, requesting the cooperation of an operator or direct access to data files	8
Inspection of call-associated data of electronic communication and requesting the cooperation of an operator	7
Inspection of localisation data of electronic communication and requesting the cooperation of an operator	7
TOTAL	36

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

It is notable that a large number of methods were authorised by the GISS in the reference period, but not actually implemented. The Standing Committee I asked the GISS how this was consistent with the requirements of proportionality and subsidiarity. The service argued that, for some observations, a specific authorisation had been requested for the use of a mobile camera, with the understanding that this camera would be used only if recording was necessary. However, the permission to record these events still had to be requested in advance. Hence, the Committee decided that the working method of the service had taken into account the principles of proportionality and subsidiarity. However, the Committee wants to prevent a specific mandate being systematically requested for each observations assignment 'in the event that…'

The Standing Committee noted that, in its monthly listings, the GISS had given an indication of the results delivered by the various methods. The Committee, which is required to report the results obtained to its Monitoring Committee I, commended this openness and took it upon itself to find out, together with the service, how to optimise this practice.

The GISS is authorised to use specific methods in the context of three of its tasks: the intelligence task in the context of a military threat (Art. 11 §1, 1° of the

Intelligence Services Act), the task of ensuring the preservation of military security (Art. 11 §1, 2° of the Intelligence Services Act) and the task of protecting military secrets (Art. 11 §1, 3° of the Intelligence Services Act). The Committee found that the GISS had insufficiently indicated the context of the legal task(s) within which the use of a method had been requested. Of course, this did not prevent the Committee from investigating whether or not the method was authorised. For example, a specific surveillance assignment was discontinued because it did not fall under one of the three tasks (see III. 2.4.2.1).

III.2.3.2. State Security

The table below shows the number of specific methods authorised.

NATURE OF SPECIFIC METHOD	NUMBER
Entry into and observation of or in places accessible to the public using a technical device	18
Entry into and searching of places accessible to the public using a technical device	0
Inspection of localisation data of postal traffic and requesting the cooperation of a postal operator	0
Inspection of identification data of electronic communication, requesting the cooperation of an operator or direct access to data files	15
Inspection of call-associated data of electronic communication and requesting the cooperation of an operator	30
Inspection of localisation data of electronic communication and requesting the cooperation of an operator	6
TOTAL	69

This table clearly shows that the majority of the methods were related to the (simple) identification of a phone or mobile number. It is a matter of 51 identifications/localisations. Of course, these identifications are not linked to an equal number of separate intelligence investigations. In some investigations, multiple identifications/localisations were requested simultaneously.

State Security has chosen not to send monthly listings to the Committee. For this, they have based themselves on the (then) draft Royal Decree, which stated that the obligation to forward these listings to the Committee rested with the SIM Commission. Therefore, the Committee could not provide an indication of the number of measures actually implemented.

The following table shows the context of the (potential) threats, as defined in Article 8, 1° of the Intelligence Services Act, within which State Security issued specific authorisations. Of course, a single method may be directed against multiple threats.

NATURE OF THREAT	NUMBER
Espionage	5
Terrorism	54
Extremism	18
Proliferation	0
Harmful sectarian organisations	2
Interference	2
Criminal organisations	0

This clearly shows that, with respect to the use of special methods, terrorism is the top priority for the service.

However, the powers of State Security are not determined merely by the nature of the threat. The service may take action only in order to safeguard the interests as listed in Article 8, 2° of the Intelligence Services Act. Which of these interests were involved for the specific methods in question?

NATURE OF INTEREST	NUMBER
Internal security of the State and maintenance of democratic and constitutional order	48
External security of the State and international relations	41
Safeguarding of the key elements of the scientific or economic potential	0

Just as in the case of the GISS, it was not always clear which interest was involved in the use of a specific method. However, it appears that a considerable number of authorisations were granted in the context of foreign intelligence investigations or at the request of foreign intelligence services. The Committee emphasised that such authorisations are justified only when the fundamental state interests of the countries with which Belgium pursues common objectives or the international and other relations maintained by Belgium with foreign States and with international or supranational institutions could be jeopardised by one of the above-mentioned threats. The Standing Committee I will verify whether this condition has been met *in concreto*.

III.2.4. ACTIVITIES OF THE STANDING COMMITTEE I AS A JURISDICTIONAL BODY

It is clear that, in the initial phase, the intelligence services and the Committee might have had different views with respect to certain aspects of the Act. This was the case, for instance, for the manner in which the authorisations of the Heads of Service had to be formulated and motivated. Hence, the Committee

was of the opinion that a better contextualisation of the relevant intelligence investigation and a more detailed description of the objective of the authorised measure was necessary for a proper assessment of the proportionality and/or subsidiarity.

However, rather than officially intervening in every possibly problematic dossier, the Committee has chosen to work in a consultative mode during the first four months. For example, shortly after the entry into force of the Act, an informal meeting was held to notify the services of the concerns and views of the Committee. Both services were also invited subsequently for a detailed briefing session, where various issues were openly discussed.

In the same spirit of consultation, the Investigation Service I has informally requested and obtained additional information in many dossiers. This has also prevented the Committee from being referred to unnecessarily, either because the additional explanation proved sufficient or because the service modified its earlier decision.

However, this does not imply that the Committee has neglected its role as the 'guardian of fundamental rights and freedoms'. Naturally, the Committee was actually referred to for the dossiers which remained problematic in terms of their legality, proportionality and subsidiarity even after additional information had been provided.

III.2.4.1. Figures

Article 43/4 of the Intelligence Services Act states that the Standing Committee I can be referred to in a matter in five ways (see III.1.3.1):

1. at its own initiative;
2. at the request of the Privacy Commission;
3. as a result of a complaint from a citizen;
4. automatically, whenever the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and has prohibited the exploitation of the data;
5. automatically, if the competent Minister has taken a decision based on Article 18/10, §3 of the Intelligence Services Act.

In addition, the Committee may also be referred to in its capacity as a 'pre-judicial consulting body' (Art. 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure) (see III.1.3.2). When requested, the Committee gives its opinion regarding the legitimacy of intelligence used in a criminal case and acquired by means of specific or exceptional methods. 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. The legislator has set no time limit within which the opinion should be given.

METHOD OF REFERRAL	NUMBER
1. At its own initiative	11
2. Request of Privacy Commission	0
3. Complaint	0
4. Suspension by SIM Commission	0
5. Decision of Minister	0
6. Pre-judicial advisory body	0
TOTAL	11

Once it has been referred to, the Committee may take various kinds of (interim) decisions. However, in two cases (1. and 2.) a decision is taken before the Committee is actually referred to.

1. Declaring the complaint to be null and void due to a formal defect or the absence of a personal and legitimate interest (Art. 43/4, first paragraph of the Intelligence Services Act);
2. decision to not take any action with regard to a complaint that is manifestly unfounded (Art. 43/4, first paragraph of the Intelligence Services Act);
3. suspension of the disputed method pending a final decision (Art. 43/4, last paragraph of the Intelligence Services Act);
4. request for additional information with respect to the SIM Commission (43/5 §1, first to third paragraph of the Intelligence Services Act);
5. request for additional information with respect to the relevant intelligence service (43/5 §1, third paragraph of the Intelligence Services Act);
6. investigation assignment for the Investigation Service I (43/5 §2 of the Intelligence Services Act)[93];
7. hearing of the members of the SIM Commission (Art. 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 (Art. 43/5 §4, first paragraph of the Intelligence Services Act);
9. decision about secrets relating to an ongoing criminal investigation or judicial inquiry to which the members of the intelligence services are privy, after consultation with the competent magistrate (Art. 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, in case the member of the intelligence service believes

[93] In this context, we are not referring to the additional information obtained by the Investigation Service I in a rather informal way before the Committee was actually referred to.

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 (Art. 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 order stating that the information obtained through this method may not be exploited and must be destroyed (Art. 43/6 §1, first paragraph of the Intelligence Services Act);
12. partial annulment of a decision of an intelligence service[94];
13. lifting of the prohibition and suspension imposed by the SIM Commission (Art. 43/6 §1, first paragraph of the Intelligence Services Act);
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 advisory body (Art. 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 following the day on which it was referred to in this matter (Art. 43/4 of the Intelligence Services Act). This period was respected in all dossiers.

NATURE OF DECISION	NUMBER
1. Invalid complaint	0
2. Manifestly unfounded complaint	0
3. Suspension of method	0
4. Additional information from SIM Commission	0
5. Additional information from the intelligence service	0
6. Investigation assignment of Investigation Service I	0
7. Hearing of members of the SIM Commission	0
8. Hearing of members of the intelligence services	0
9. Decision regarding secrecy of criminal investigation	0
10. Sensitive information during hearing	0
11. Discontinuation of method	3
12. Partial annulment of authorisation	6[95]
13. Lifting of prohibition imposed by SIM Commission	0
14. No competence	1
15. No discontinuation of method /Unfounded	1
16. Pre-judicial advice	0
TOTAL	11

[94] This decision, not described as such in the Act, may be compared with a 'partial discontinuation'.

[95] The six dossiers were related to the same issue.

The SIM legislator has paid great attention to the rights of citizens. This is reflected for example in the fact that any interested citizen is permitted to submit a complaint to the Committee. In this case, a number of 'rights of defence' are involved. Given that there were no complainants in the reference period, no further attention has been given to this aspect in this report.

III.2.4.2. Decisions of the Standing Committee I

The eleven decisions taken by the Committee between 1 September 2010 and 31 December 2010 are briefly presented below. The explanations have been stripped of all operational information. Only those elements relevant to the legal issue have been included.[96]

III.2.4.2.1. A specific observation assignment outside the scope of the legal assignments of the GISS

The GISS wanted to carry out specific observation in an investigation where there was '*a possible attempt at subversion, espionage and support for terrorism*' and where (according to additional information) the '*departure or presence in a military operational zone is not inconceivable in the future*' (free translations). However, the Standing Committee I decided that '*the decision of the Head of Service does not reveal any connection between the implementation of the method with respect to the objective and the legal assignments*' (free translation). Therefore, the Committee ordered the discontinuation of the method.

III.2.4.2.2. Period for a specific surveillance assignment

In six separate dossiers, State Security had authorised a specific observation for a period of two years each time. Even though the Act does not lay down a maximum period for specific methods, the Standing Committee I decided that, based on the principles of subsidiarity and proportionality and in view of the existing possibility to extend a method, a reasonable period must always be proposed. Rather than simply discontinuing the methods and ordering that the collected intelligence be destroyed, the Committee nullified the method '*for the part exceeding 12 months*' (free translation). In doing so, the use of already gathered intelligence could be avoided.

96 All decisions of the Committee in this matter are marked for 'restricted' or classified as 'confidential'.

III.2.4.2.3. Exploitation of images obtained via a surveillance camera

The Standing Committee I was informed of the decision regarding '*the exploitation of images recorded by a camera belonging to, installed and controlled by a private security firm*' (free translation). The information gathered revealed that the service in question had no control over where the camera was set up or what images would be recorded at which times. The camera was managed completely independently by a security firm. The Committee concluded that '*merely receiving and viewing video tapes recorded by a camera made available by the operator of a camera system does not constitute observation within the meaning of the Act of 30 November 1998. Therefore, this method is not a specific method, but merely an ordinary method*' (free translation). This is because it involves '*the (gathering of) intelligence required for the performance of their assignments, including personal data, […] from any person or organisation belonging to the private sector*' (free translation) as defined in Article 16 of the Intelligence Services Act and/or obtaining intelligence via human sources as referred to in Article 18 of the Intelligence Services Act. However, the Committee also added that this did not necessarily rule out the fact that problems might still arise from the use of this method pursuant to, for example, the requirements of the Data Protection Act of 8 December 1992 in general and the Act of 21 March 2007 governing the installation and use of surveillance cameras in particular. But this issue falls outside the competence of the Committee as a jurisdictional body.

III.2.4.2.4. Observation of a home

In quite a few dossiers, the Heads of Service of the two intelligence services had granted permission for the observation of a home using a technical device. This refers to observation from a fixed observation point (i.e. a camera) of the front door of a home located on a public road with a view to determining who enters and leaves this home. In other words, this is not an observation of what occurs inside this home or in the garden or any adjoining area; that would constitute an exceptional method (see Article 18/2 §2, 1° of the Intelligence Services Act).

Observation of a home is not regulated as such in the Intelligence Services Act. However, Article18/2 §1, 1° of the Intelligence Services Act defines '*the observation […] of private places not accessible to the public*' as a specific method. But 'homes' are explicitly excluded from the concept of 'private places' as defined in the Intelligence Services Act. Hence, the possibility of putting homes under observation remained *prima facie* unclear. The Standing Committee I has decided to intervene in one of these dossiers with the intention of taking a decision in principle regarding this issue.

The Committee decided that the observation of private places, a residence or the professional premises of a lawyer, doctor or journalist should be considered

as the observation of the publicly accessible place located just in front of the entrance to the location in question. Therefore, such an observation constitutes (depending on whether or not a technical device is used) an ordinary or specific method, so long as what occurs inside the residence or in the garden or in any adjoining area is never put under observation, not even for a one-shot operation or a short period.

III.2.4.2.5. Observation of a home located in a non-publicly accessible place

As explained earlier, the Committee decided that observation of the front door or garage door of a home located on a public street with a fixed camera constitutes a specific method that – except in the case of a protected professional category – may be authorised by the Head of Service without the prior approval of the SIM Commission. However, in one of the authorisations forwarded to the Committee, there was an additional complication: the residence was located in an enclosed area and the entrance was guarded. The area was not freely accessible in the sense that no one could enter without meeting specific conditions (such as, holding a special permit or an individual invitation). Therefore, within the meaning of the Intelligence Services Act, the area had to be regarded as a 'private place not accessible to the public'.

In this dossier, the filming (of the front door or garage door located on a public road) of the home – which constitutes a specific method – also implied observation of a 'private place not accessible to the public'. Such an observation assignment always constitutes an exceptional method within the meaning of Article 18/11, 1° of the Intelligence Services Act, even if no technical device is used. However, an exceptional method may only be authorised after the assent of the administrative SIM Commission (Art. 18/9 §2, second paragraph of the Intelligence Services Act). This SIM Commission had not yet been set up at that time. Hence, it was ordered that the measure be discontinued and any intelligence already gathered, destroyed.

III.2.4.2.6. Surveillance of an individual with a protected status

The intelligence service in question wanted to put a non-EU national under surveillance who, however, enjoyed a protected status. Pursuant to Article 18/3 §1 of the Intelligence Services Act, specific methods may be used in connection with individuals belonging to these professional categories or with respect to the means of communication used by them only after the SIM Commission has given its assent on the motion of the Head of Service. Naturally, such an assent could not be presented for this dossier.

III.2.5. SOME INITIAL CONCLUSIONS

It is evident that, rather than the absence of the required implementation decrees, it is mainly the failure to appoint the members of the SIM Commission that has been a key factor during the first four months of SIM operations. Yet it cannot be said that the services had fewer powers during these months than they had before: they could continue using the specific methods which they were using previously without an adequate legal basis. However, in this short period of time, they have been denied the possibility of using the new exceptional methods.

The intelligence services were far from accustomed to justifying the use of special intelligence methods in writing and taking the principles of proportionality and subsidiarity explicitly into consideration. In addition, their decision on this matter can now be reviewed and if necessary, sanctioned by third parties. In this area, the SIM Act has certainly implied both a change in mentality as well as additional (administrative) work for State Security and the GISS. But on the other hand, the rationalisation of the use of resources and a greater accountability of the services have been made possible.

In the initial phase, the Standing Committee I has chosen to enter into discussions with the services, in order to optimise the quality of the authorisations. The intelligence services have responded positively to this invitation and have always provided the necessary information. Naturally, this does not mean that there will be no ambiguities or points of improvement henceforth. These elements will undoubtedly form the subject of subsequent reports.

CHAPTER IX
RECOMMENDATIONS

Based on the investigations concluded in 2010, the Standing Committee I has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred to individuals by the Constitution and the law (IX.1), the coordination and efficiency of the intelligence services, the 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 THOSE RIGHTS WHICH THE CONSTITUTION AND THE LAW CONFER ON INDIVIDUALS

IX.1.1. PROTECTION OF PERSONAL DATA OUTSIDE OF SECURE SITES

The GISS has made a great deal of effort to protect classified information that leaves secure sites.[97] However, it is recommended that the same efforts be devoted to the protection of personal data that are not necessarily classified. Since, Article 16 §4 of the Data Protection Act of 8 December 1992 stipulates that the person responsible for processing this data must take the appropriate technical and organisational measures to protect personal data against accidental loss.

Additionally, the Standing Committee I recommends that rules be developed for communicating a security incident to the persons whose information has been lost. In doing this, the risks to the service must, of course, be weighed against the interests of the individual concerned.

The Committee will question the GISS in 2011 regarding the actions (proposed) taken in this regard.

97 See Chapter II.3.

IX.1.2. STATE SECURITY AND PROCEDURES FOR OBTAINING BELGIAN NATIONALITY

The Standing Committee I is of the opinion that the role assigned to State Security in the context of procedures for obtaining Belgian nationality must be further defined by the legislator. For this, the regulation with regard to security verifications and investigations can serve as an example.

In addition, the legislator should also make it explicitly possible for the Public Prosecutor to receive, process and use classified information in the context of nationality declaration procedures. The rights of the individual concerned must, of course, always be taken into account.

Finally, the short period allowed to State Security to formulate its remarks should be reconsidered. Since it is not always possible to collect, analyse and deliver accurate and relevant information to the Public Prosecutor within this limited period of time.

IX.1.3. A LEGAL BASE FOR THE COLLECTION OF INFORMATION THROUGH INFORMANTS

The Standing Committee I is pleased to note that, pursuant to the SIM Act, Article 18 of the Intelligence Services Act now provides that the Ministerial Committee for Intelligence and Security must develop guidelines for gathering information with the help of human sources. But the Standing Committee I continues to believe that certain conditions concerning the application of this method should be defined at the level of the legislator.[98] More specifically, the Committee recommends an explicit ban on gathering information through informants when this implies circumventing provisions implying an obligation of confidentiality or setting aside the guarantees provided under the SIM Act.

Pending such legislation and the issuance of a guideline by the Ministerial Committee, the Committee recommends that the Ministers of Justice and Defence should forbid the use of such circumvention tactics.

---

98 See also STANDING COMMITTEE I, *Rapport d'activités 2006,* 75; *Rapport d'activités 2008,* 108; *Rapport d'activités 2009,* 83–84.

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

IX.2.1. ADMINISTRATIVE COORDINATION CELL AND MONITORING OF SECTARIAN ORGANISATIONS BY STATE SECURITY

In order for the members of the Administrative Coordination Cell for the fight against harmful sectarian organisations to be informed of the classified information in the possession of State Security, it is advisable that they be subjected to a security screening and if necessary, obtain a security clearance.[99]

Furthermore, the Committee recommends that State Security should no longer serve as the secretariat of the Administrative Coordination Cell. This will allow the official in question to devote himself fully to his assessment work.

IX.2.2. MONITORING OF THE ECONOMIC AND FINANCIAL OPERATIONS OF SECTARIAN ORGANISATIONS

It is desirable that State Security pays more attention to the economic and financial operations of sectarian movements and networks. For this, the relevant sections of the Operational Departments and Analysis Departments should have sufficient staff who are familiar with this field.

IX.2.3. TRANSPORT OF CLASSIFIED MATERIAL

The Standing Committee I recommends that the intelligence services should equip their service vehicles with a device to protect sensitive and/or classified information and materials. In the event of a security incident, this will prevent such data or materials being easily consulted or stolen by third parties.

[99] See Chapter II.2.

IX.2.4. HANDLING OF INCIDENTS INVOLVING THE LOSS OF DATA

In case of loss of sensitive and/or classified (personal) data, any decision to undertake (or not) specific actions (such as reporting crimes in accordance with Article 29 of the Penal Code, withdrawal of a security clearance, notifying the persons whose data is lost) must be properly motivated and communicated to the competent ministers.

IX.2.5. COOPERATION IN THE CONTEXT OF THE FIGHT AGAINST PROLIFERATION

The Committee is of the opinion that, despite the improvements observed, it is desirable that the cooperation between the authorities involved in the fight against proliferation be further strengthened through cooperation agreements. For this, the Committee specifically refers to agreements concluded by the intelligence services with the CANVEK/CANPAN and the three Regions.[100] These agreements, which are based on Article 14 of the Intelligence Services Act, should clearly indicate the channels through which classified information can be exchanged. Before the end of 2011, the Committee intends to examine the actions taken in this regard.

However, the Standing Committee I wants to stress that the absence of such agreements does not, in itself, form an obstacle to the communication of information to the Ministers and the competent authorities and bodies.

IX.2.6. GUARANTEED REPRESENTATION IN THE CANVEK/CANPAN

The Committee stresses the importance of the presence of a member of the GISS at the CANVEK/CANPAN meetings, as this is not always the case. The contribution of the military intelligence service in this advisory body must be guaranteed. Indeed, this is one of the consequences of a more structural problem: the GISS does not deploy sufficient analysis resources for monitoring proliferation.

---

100 On 17 July 2007, pursuant to the Special Act of 12 August 2003, a cooperation agreement was concluded between the Federal State and the three Regions with regard to the import, export and transit of weapons, munitions and equipment and related technology specifically for use by military or law enforcement forces as well as dual-use products and technologies and the granting of permits in connection therewith (*Belgian Official Gazette* 20 December 2007). But in addition to this, the two intelligence services also have information that may be useful for the regional governments.

IX.2.7. HOUSING OF THE PROVINCIAL POSTS OF STATE SECURITY

The Standing Committee I found a positive change in 2010 with respect to the long-standing and sometimes harrowing manner of dealing with the housing problem of certain State Security Provincial Posts. It recommends that this new approach should be extended to include the Provincial Post in Mons, where the renovation works have been suspended for years, and that the efforts already made for the other posts should be sustained until their completion. This is not only to ensure a safe workplace, but also to bring about the revaluation of the Provincial Posts as envisaged in the 'Strategic Plan 2008–2012'.

IX.2.8. COMPLIANCE WITH THE SCOPE OF COMPETENCE

Based on its investigation of certain surveillance operations[101], the Standing Committee I was pleased to note that State Security has incorporated the Committee's earlier recommendations (in the Erdal and Kimyongur cases) in its organisational culture. Indeed, the investigation had shown the concern of the State Security leadership regarding a correct and legal interpretation of its tasks. This had translated itself into a sustained and well-founded opinion addressed to the competent minister.

Since the Standing Committee I is not competent to express an opinion on actions or instructions of the competent ministers, it limits its recommendation to calling on the intelligence services to continue paying attention in future to the correct interpretation of their tasks.

IX.2.9. MONITORING OF THE RIOTS IN BRUSSELS BY STATE SECURITY

Based on its investigation into the monitoring of the riots that broke out in Autumn 2009 in the Brussels conurbation[102], the Standing Committee I was of the opinion that State Security did not have a leading role to play in combating this phenomenon.

However, the Standing Committee I recommends that, e.g. in the context of the responsibilities of the Board for Intelligence and Security, the necessary agreements should be made between the intelligence services and the (federal and local) police services in order to systematically monitor the evolution of this problem and exchange the necessary information in time.

---

101 See Chapter II.4.
102 See Chapter II.7.

IX.2.10. ENSURING THE PROPER FUNCTIONING OF COUNTER-ESPIONAGE SERVICES

The presence of international institutions such as the NATO, the SHAPE and the European Union on Belgian territory makes our country a favourite target of international espionage. It is therefore necessary that Belgium has properly functioning counter-espionage services.

Based on the investigation into the espionage in the *Justus Lipsius* building[103], the Committee reiterates its recommendation that adequate human, technical and legal[104] resources should be assigned to State Security and the GISS so as to ensure that both services perform this task efficiently.

More specifically, the Standing Committee I recommends that State Security should sign a protocol agreement with the Brussels-based EU institutions to clearly define the cooperation and information exchange in this regard.[105]

Furthermore, the Committee recommends that the GISS should draw up reports of the sweepings it carries out at the request of various bodies, especially since at present these are usually occurring independent of any protocol.

IX.2.11. SCREENING OF EXTERNAL SERVICE PROVIDERS

Based on the same investigation, the Standing Committee I emphasised that it is absolutely imperative to take into account the numerous warnings issued by the intelligence services regarding the need for protecting critical information systems against interceptions and cyber-attacks.

In this context, the Committee also recommends that the greatest care should be taken in selecting (the suppliers of) technical equipment intended for processing sensitive and classified information. This recommendation is especially applicable to information relating to or arising out of the SIM methods.

IX.2.12. AN EFFECTIVE INFORMATION MANAGEMENT SYSTEM FOR THE GISS

The Committee concluded that five years after the discovery of a significant lacuna in the information management system of the GISS, budgetary

---

103 See Chapter II.1.

104 With the introduction of the SIM Act, the intelligence services now have access to the necessary legal options for taking effective action with respect to counter-espionage activities.

105 In its response to the investigation, State Security informed the Committee that they had contacted the EU institutions with a view to concluding a protocol agreement, but that neither the Council nor the Commission had acted upon this.

considerations and internal resistance have prevented this problem from being remedied. This situation is certainly such that it compromises the proper execution of the tasks of the GISS. Therefore, the Standing Committee I strongly recommends that the solution developed by the GISS at that time, should be examined, re-assessed and incorporated as soon as possible in the budgets of the coming years.

The Committee will re-examine this issue in the context of the audit of the military intelligence service initiated in 2010.[106]

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

IX.3.1. FINALISATION OF THE SIGINT PROCESS DESCRIPTIONS BY THE GISS

The Committee regrets the fact that the SIGINT process descriptions of the interceptions have not yet been finalised by the GISS.[107] The Standing Committee I emphasises the importance of these process descriptions because they allow legal verifications to be carried out in a more efficient manner. It therefore recommends that the GISS finalise these process descriptions in 2011.

IX.3.2. TIMELY COMMUNICATION OF RELEVANT SECURITY INTERCEPTIONS

Before 31 December each year, the GISS is required to provide the Minister of Defence with a reasoned list of organisations or institutions whose communication may be the subject of a security interception during the coming year. This is done so as to secure ministerial approval for these interceptions.[108]

To ensure that the power of supervision can be executed, the Standing Committee I urges that this legal period be scrupulously respected.

IX.3.3. HEARING OF FORMER MEMBERS OF THE INTELLIGENCE SERVICES

Until 2010, it was only possible for the Standing Committee I to summon the presently serving members of the intelligence services for questioning. It was

106 See Chapter II.12.11.
107 See Chapter III.
108 See Chapter III.

impossible to force a former member of State Security or the GISS to testify under oath.

The Standing Committee I therefore reiterates its recommendation from 2009 that it should be possible to issue summons against former members of the reviewed services.[109] Article 48 of the Review Act has since been amended in this regard by the Act of 9 February 2011.[110]

109 STANDING COMMITTEE I, *Rapport d'activités 2009*, 88.
110 *Belgian Official Gazette* 29 March 2011.

ACTIVITY REPORT 2011

TABLE OF CONTENTS OF THE COMPLETE ACTIVITY REPORT 2011

PREFACE

The writing of an annual report provides an ideal opportunity to reflect on our operations: What did we achieve? What were the key focus areas? Did we meet our goals? Looking back at 2011, there are several areas that merit special attention. We have selected four of these in this preface.

The first was the audit of the General Intelligence and Security Service (GISS). Having thoroughly screened State Security in 2009, the Standing Committee I turned its attention to the military intelligence service in 2011. Since such an audit is a very labour-intensive process, the Committee has had to dedicate a great deal of its resources to this task. The Monitoring Committee of the Senate, the Minister of Defence as well as the GISS have recognised the added value of the audit results in terms of improving effectiveness and efficiency (see II.1 and IX.2.1).

Rome was not built in a day and the same is true for the *European Network of National Intelligence Reviewers* (ENNIR), an initiative of the Committee and the Monitoring Commission of the Senate. Progress was made, however, on this web-based knowledge-sharing platform for European review bodies of intelligence and security services. The website is now online (www.ennir.be) and several countries have already pledged their full cooperation. This network designed to facilitate the exchange of interesting information and best practices will be further developed in 2012.

On a completely different note, the Standing Committee I relocated to the new Forum building. Thorough preparation allowed for a successful and efficient relocation. And even though the investment of people and resources associated with this relocation did not directly yield benefits in terms of the 'review of the intelligence services', there is no doubt that the new work environment and the close proximity of the main partner of the Committee (i.e. the Parliament) will positively influence our future operations.

Above all, however, 2011 was the first year in which the Special Intelligence Methods Act was in full effect (see III). For the first time, State Security and the General Intelligence and Security Service could exercise specific and exceptional powers. Moreover, the appointment of the members of the SIM Commission meant that, in addition to the judicial monitoring by the Standing Committee I, the administrative review process also became operational. Naturally, a preface is not the appropriate place to assess such complex legislation. However, we feel that the past year has demonstrated that the SIM Act actually works and is

effective: the intelligence services have applied the methods without lapsing into excesses and the dual external monitoring has proved its worth as a guarantee for the rights and freedoms of individuals. In fact, this stringent supervision was one of the main reasons why the Constitutional Court upheld the complete SIM Act (barring one provision) in its judgement of 22 September 2011. However, this does not mean that the current regulation is perfect. Further improvements and refinements may be warranted. The Committee will not fail to formulate recommendations to this effect, where necessary. In addition, it will continue investing further in its new jurisdictional assignment in this extremely important matter.

Guy Rapaille,
Chairman of the Standing Intelligence Agencies
Review Committee

1 June 2012

CHAPTER II
INVESTIGATIONS

In 2011, the Standing Committee I received 25 new complaints or reports from private individuals. After verifying a number of objective data, the Committee dismissed 19 complaints or reports either because they proved to be manifestly unfounded (Art. 34 of the Review Act) or because the Committee was not competent for the matter in question. In the latter cases, the complainants were referred, wherever possible, to the competent authority. The two complaints that were still pending at the end of 2010 also did not result in an investigation. An investigation was opened with regard to three new complaints or reports; for the remaining three complaints from 2011, it was still being examined whether there are sufficient grounds for initiating an investigation.

Besides the three investigations resulting from a complaint, the Standing Committee I also opened an investigation in 2011 at the initiative of the President of the Senate.

Ten investigations were completed in 2011. These will be discussed below (II.1 to II.10). This will be followed by a summary and brief description of the investigations that are still ongoing (II.11).

II.1. AUDIT OF THE MILITARY INTELLIGENCE SERVICE

II.1.1. INTRODUCTION

The Belgian military intelligence service has been assigned four tasks by the legislator:

- an intelligence assignment with respect to any activity that threatens or could threaten the inviolability of the national territory, the military defence plans, the scientific and economic potential, the performance of the assignments of the armed forces or the safety of Belgian nationals abroad;
- ensuring the military security of personnel and military installations;

– an assignment to protect secrets related to military installations and intelligence;
– and finally, carrying out security investigations (Art. 11 of the Intelligence Services Act).

Of course, these tasks can only be carried out properly if the GISS deploys its resources efficiently and effectively. To determine whether this is the case, the Standing Committee I decided – with the backing of the Monitoring Committee of the Senate – to carry out an audit.[111]

The Committee not only carried out a 'performance audit'[112] in order to gain insight into the situation within the service in question, but it also wanted to create a dynamic which would lead to real change and improvement, where necessary. With a view to the creation of this dynamic, the Committee formulated a number of detailed recommendations.[113] To place these recommendations in context, the structure of the audited service and the progress and results of the audit are explained briefly in this chapter.

II.1.2. KEY THEMES

Since the Committee had allowed itself only a relatively short period of time – i.e. six months – a selection had to be made among the areas to be investigated. This selection was done based on criteria such as added value[114], materiality[115] and the degrees of risk and uncertainty.[116]

The first two selected areas of investigation were related to 'human resources' and 'information management'. Since, both the deployment of personnel and the use of available information are crucial elements within an intelligence service. This is not only the case with regard to investments[117] but also from a strategic point of view, since intelligence work is entirely dependent on human effort and having access to the right information. The so-called 'organisational management system' (an internal monitoring of the audited service) was also

111 '*Audit with a view to identifying and verifying the conditions necessary for the effective use of resources at the General Intelligence and Security Service (GISS), with particular attention paid to the management and supervision of staff, information flows and risk management*' (free translation).

112 In this respect, also refer to the audit of State Security: STANDING COMMITTEE I, *Activity Report 2009*, 5–23.

113 See Chapter IX. Recommendations (in particular IX.2.1). The considerations formulated in the audit were also presented by the Committee in the form of a 'roadmap' for a better deployment of resources at the GISS.

114 'The less known about a particular area, the greater the added value of an audit into this area'.

115 'Importance of the area in terms of investments, strategic importance, public impact, etc.'

116 'Areas about which little is known (e.g. because they have never been audited) or areas in which incidents have occurred in the past are, in principle, areas involving risk or uncertainty.

117 The HR budget represents the major part of the budget of the GISS.

studied. Internal monitoring is based on the risk management process within an organisation; this is why this topic was included for detailed study as a third area of investigation.

II.1.3. PHASING AND METHODOLOGY

The Standing Committee I has invested extensively in this investigation, both in terms of people and resources.

Naturally, the actual audit was preceded by the preparation of an audit plan and the development of a well-founded methodological basis, in conformity with internationally applicable standards.

Work was carried out in phases. The first phase involved forming an idea regarding the matter at hand based on the requested documentation and exploratory interviews (December 2010).

In a second phase, information was collected on issues prevalent at all levels of the organisation (such as internal communications, training, cooperation), which was then converted into 'hard' numerical data. Possible areas for improvement were also studied, based on the experience and suggestions of staff members of the service. Staff members were invited to give their opinion via a written questionnaire (January–February 2011).[118] In a personal and confidential interview, the respondents could contribute additional information, if any. In addition, all (sub-)divisions of the GISS were visited and both the managers and their employees were given the opportunity to discuss their activities and working conditions.

The information gathered was fed back in a third phase: based on interviews with managers and domain experts, the identified issues were verified and analysed in depth. An attempt was also made to develop more detailed suggestions for improvement. Cross-divisional 'focus groups' were set up for this task (March–May 2011).

A final phase involved reporting (June 2011). The audit resulted in a voluminous report (198 p.), which was classified as secret.

II.1.4. STRUCTURE OF THE MILITARY INTELLIGENCE SERVICE

The GISS is managed by the Command (GISS/C), which is assisted by a small staff and a secretariat. The GISS – which employs both civilian and military personnel – is sub-divided into four divisions operating mainly from Brussels.

[118] The gross response rate to this questionnaire was 71.5%, while the net response, i.e. without blank answers, was 67.3%. These results are definitely representative.

The Support Division (A – *Appui*) combines all services responsible for providing general assistance to the GISS, i.e. HR and budgetary management, ICT, logistics aspects managed within the GISS, etc.

The Counter-Intelligence Division (CI) monitors phenomena which are mainly located on Belgian territory and which could threaten military security. This division has a number of provincial detachments that communicate the data gathered to analysts within the division.

The Intelligence Division (I), the largest division within the GISS, also performs a collection and analysis task. It focuses on phenomena occurring abroad that constitute a threat falling within the area of operations of the GISS. The Analysis Departments of this division are mostly organised by geographical region, while there are also offices for *Naval, Air* and *Land Intelligence* and transnational issues. The I/Ops Division is active abroad and provides assistance to Belgian troops. It gathers local information, both for military personnel in the field and for the GISS in general.

The Security Division (S) has two main tasks. Firstly, it conducts security investigations with respect to persons or companies that have requested a security clearance or certificate that is required for carrying out certain tasks or assignments within or for the Defence department (S/Habilitations). This division may also call upon the assistance of provincial detachments. Secondly, the division monitors military security (areas, persons, IT systems), i.e. it formulates guidelines to be followed by the various Defence entities and it is entitled to carry out inspections in certain cases (S/Security, MIS[119] and S/Infosec).

II.1.5. KEY PRINCIPLES OF THE AUDIT

The results of the audit per selected area are explained briefly below.

II.1.5.1. Deployment, management and motivation of staff members

In the area of human resource management[120] and staff motivation, the GISS still faces many challenges.

The strengths of the service are, undoubtedly, the interesting job content and the opportunity given to staff members to develop their own initiatives, where necessary. These are extremely important elements and form the basis for staff motivation and commitment.

---

119 Military and Industrial Security.

120 These include various human resource topics such as recruitment, management of natural attrition, career planning, remuneration, etc.

At the same time, its staff members could be deployed more effectively and efficiently. There is also room for improvement in the way in which objectives are formulated internally and subsequently translated with respect to the employees in the field. In fact, it appeared from the audit that the employees themselves were pressing for this.

The audit further revealed that the Personnel & Organisation function (P&O) must be reinforced to enable the service to invest in job descriptions, previsional HR management, coaching, etc. The organisational development capacity of the service, which every organisation needs in order to continually analyse, improve and change its operations (learning capacity), must also be strengthened.

The staff members were rather moderately satisfied with the career opportunities and remuneration. But these are aspects for which the GISS is not (solely) responsible. Since, for such matters, the intelligence service depends on the cooperation of other entities such as the Directorate-General for *Human Resources* within Defence. But here too, the invested resources appeared to be rather scarce. Active cooperation and consultation among all partners, both within and outside the GISS, remain essential.

Another thorny issue was the equal treatment (with regard to career opportunities, allowances, etc.) of the various categories of staff within the GISS. In particular, the situation of the civilian personnel drew the Committee's attention. It was not clear what kind of position they had within the military structures and what they could expect from their careers within the GISS. A number of factors have led to a serious disruption in the balance between civilian and military personnel. Although (legal) inequalities transcend the GISS, they have become a problem now that the number of civilians in the entire workforce of the GISS appeared to be relatively high in proportion to the military personnel. In addition, the civilian personnel play a central role in the intelligence cycle and more specifically, in the assessment phase. However, the Standing Committee I believes that this issue must be approached with caution. Since, any measure taken in favour of a particular category may be regarded as unfair by the other members of staff.

But the audit showed that there were inequalities not only in one but in several categories, regardless of whether this involved civilian or military personnel. Since the Committee feels that the service should try to accommodate the ambitions of all members of staff, it was of the opinion that the prevalent 'group logic' should make way for a 'functional logic'. It is better not to think in terms of 'staff categories' (military personnel *vs* civilians, contractual *vs* statutory staff, level X *vs* level Y, etc.) but rather in terms of 'positions' (e.g. a line[121], analysis or data collection function). Within these functions, one can strive towards an equal treatment of all members of staff, regardless of status or rank.

[121] This is a hierarchical position.

The Committee felt that the analysis function, employing staff members with different statuses, deserved priority. But this does not mean that other 'inequalities' – e.g. within the collection services – should therefore deserve less attention.

Another problem was that the military personnel of the GISS are drawn from other units of the Armed Forces and are deployed by the GISS only for a short period of time. The relatively high level of rotation created problems with regard to their induction, training and knowledge management. The Standing Committee I was of the opinion that this could be remedied by creating an 'intelligence section', where the focus could be laid on career and knowledge development. The recruitment of staff, preparation of consistent job profiles, development of competency management, career planning and training could be organised by and from within this division. Civilian personnel would also have a clearer position within such an 'intelligence section' and they would be able to develop their careers better.

II.1.5.2. Information management

With regard to information management, the Standing Committee I found that the staff members of the GISS are trying to master the ever-increasing volume of information and documentation with great 'industry' but with limited resources. A *Request for Information* system (RFI)[122], intended to provide an answer to the findings of a previous investigation[123], had been implemented in autumn 2011.

Despite the efforts made, the Committee was forced to conclude that it will not be possible to implement an integrated ICT system that allows staff members to easily and quickly enter and retrieve data, within the short term. The necessary investments appear to be continually postponed. However, a number of innovations have been made, though these were delayed by the postponement of the planned investments (at the time of the audit, postponed to 2016). The Committee concluded that the intelligence activities were not (or no longer) sufficiently supported by the ICT system. Due to the large volume, it was difficult to access or process particular information or there was a risk that this information would escape the attention of the GISS. In this sense, the conditions for proper information management were not (or no longer) being fully met.

The Standing Committee I pointed to the obvious risks entailed by this. Since, there is no guarantee that information – which would later prove to be

---

122 The *Request for Information system* is based on a standardised document that describes what kind of intelligence is required.

123 Investigation with regard to information management by the military intelligence service. The initial reason for opening this investigation was the fact that, in an actual case, there had been a lack of information flow between the Intelligence and Counter-Intelligence Divisions. See STANDING COMMITTEE I, *Rapport d'activités 2010*, 41–42.

crucial in a dossier – will be received, retrieved and/or processed by the service (in time). These risks must be mitigated by investments in ICT.

However, just as in the case of human resource management, the GISS depends on other Defence entities for its material and budgetary needs. This led the Committee to conclude that the cooperation between the GISS and the Defence entities of all the relevant parties needed to be conducted with a new form of openness, ensuring that the often 'secret' nature of the activities of the GISS does not hinder communications.

II.1.5.3. Organisational management systems and risk management

A final area of investigation concerned the organisational management and the associated risk management processes. The Standing Committee I pointed out that, due to the rotation and outflow of staff, the GISS faced a number of risks[124] related to discontinuity and loss of knowledge. There was a need to further identify and manage these risks. Here again, a strong P&O function, adequate ICT resources and a thorough knowledge management process are necessary for making progress. Recently, the GISS has implemented a risk management tool. But the risk management process can only be initiated in practice after the objectives of the GISS have been clearly defined (*supra*) and the organisational processes have been optimised.

II.1.5.4. Other findings

During the audit, a number of observations were made that fell outside the scope of the investigation.

For example, the physical security of the infrastructure and the monitoring resources of the GISS were not always up to a level expected from a military intelligence service.

Regarding staffing needs[125], the Committee noted that some assessment and collection offices had fallen back on a minimum staffing level. This also implied risks with regard to the continuity of the service.

Finally, the Committee also concluded that the cooperation between the GISS and other sections of Defence – particularly the Directorates-General *Human Resources* and *Material Resources* as well as the Internal Audit of Defence – needed to be reinforced.

---

124 The term 'risk' refers to any uncertainty having an impact on the objectives of the organisation. 'Risks' are all incidents and circumstances that could affect the achievement of these objectives.

125 The audit could not deliver any further opinion in this matter. The staffing needs can only be determined after the objectives and Service Levels of the GISS have been defined in detail.

II.1.6. GENERAL ASSESSMENT

To the question regarding whether the conditions for a proper human resources management are being met, the answer was positive; although, of course, improvements and changes are possible and necessary.

In contrast, with regard to the access and use of the available information (the actual intelligence work), the answer appeared to be rather negative. The Standing Committee I established that the military intelligence service – certainly in the area of ICT – lacked the necessary resources, as a result of which there was a risk that certain information escapes the attention of the GISS or is not used.

Finally, the GISS has started focusing on organisational and risk management since only very recently and a lot of work still needs to be done in this area.

The fact that the GISS has been able, so far, to deliver thorough work is largely due to the hard work and dedication of its staff. The commitment of its many employees is such that the genuine problems and risks faced by the organisation become less visible.

But the precarious situation of the GISS as at the time of the audit cannot be expected to be tenable in the long term. The Committee concluded that either ambitions should be set to a more modest level or the resources (and the organisation) must be adapted. If not, the risks arising due to the situation will have to be accepted. One of these risks is that it will no longer be possible to fulfil the (high) expectations of the principals of the GISS.

II.2. PROTECTION OF COMMUNICATION SYSTEMS AGAINST POSSIBLE FOREIGN INTERCEPTIONS AND CYBER-ATTACKS

In an information society, ensuring the security of communications systems managed via information technologies is crucial. Various superpowers view mass attacks against these systems as one of the main threats to the security, military interests and economy of a country, as well as to the fundamental rights and freedoms of citizens. Therefore, the Monitoring Committee of the Senate has expressed its desire to be kept informed by the Standing Committee I about the manner in which the intelligence services are monitoring this matter.[126]

Successively, an overview is provided of the federal institutions entrusted at present with the task of ensuring the security of ICT systems and the roles of

[126] The Committee also wanted an update of the Echelon Rapport presented by the Standing Committee I in 2000 (STANDING COMMITTEE I, *Rapport d'activités 2000*, 27 ff.).

State Security and the GISS are explained. Finally a number of conclusions are drawn.

II.2.1. FEDERAL INSTITUTIONS RESPONSIBLE FOR THIS MATTER

Unlike its neighbouring countries[127], Belgium does not have a body that is specifically entrusted with the task of protecting information systems. This task is distributed over several federal public services, which, moreover, do not always have access to adequate resources. Which are these services?

First, the (intelligence) policy for combating threats against information systems falls under the Ministerial Committee for Intelligence and Security (MCI&S). However, the MCI&S has not developed any specific guideline *in casu*.

The FPS Information and Communication Technology (FEDICT) has the task of developing and implementing a policy with a view to ensuring the security of the information systems of the federal administrations. FEDICT is entrusted with the task of developing a structure for the online services of the government (e-government) and for promoting the computerisation of society. It has also been assigned the task of drawing up an inventory of the critical IT infrastructure.

The National Security Authority (ANS/NVO) was designated as the homologation authority for the systems and networks of the federal public services that process, communicate or store national or international (EU, NATO) classified information. The ANS/NVO has the task of ensuring the security of information systems and this task is carried out in three phases: evaluation, certification and the actual homologation. However, due to a lack of resources, the ANS/NVO was not fully capable of executing this task.

In 2000, BELNET[128] was set up. This service was entrusted with the development, introduction and management of the communication network between the federal public services and the internet. Some of the connections within this so-called 'FEDMAN' network (Federal Metropolitan Area Network) are protected. A part of FEDMAN – named 'BINII'[129] – is reserved for the exchange of classified information. This functionality is managed by the GISS. The task of setting up a Computer Emergency Response Team (CERT)[130] at the

127 See, for example, the *Agence Nationale de la Sécurité des Systèmes d'Information* (France), the *Bundesamt für Sicherheit in der Informationstechnik* (Germany) or the *Office of Cyber Security* (United Kingdom).

128 BELNET is a public service, separately managed within the FPS Science Policy.

129 Also see STANDING COMMITTEE I, *Rapport d'activités 2007*, 48.

130 A CERT is usually entrusted with the following tasks:
- centralised identification of incidents (attacks) on information networks and systems and centralisation of requests for assistance as a result of these security incidents (receipt of requests, analysis of symptoms and possible correlation between incidents);

federal level was also entrusted to BELNET.[131] This is a warning and response centre for assisting public bodies and companies if they have become the target of an electronic attack. The public service CERT.be was launched in September 2009.[132]

Previously, the Federal Consultation Platform on Information Security, better known as the Belgian Network Information Security (BELNIS) platform, had been already set up. In addition to State Security and the GISS, this platform brings together representatives of federal authorities such as the ANS/NVO, the Governmental Crisis Centre, the Federal Computer Crime Unit, the Board of Prosecutors-General, the Privacy Commission, etc. The BELNIS platform formulated proposals with regard to the protection of critical ICT infrastructure and the approval of systems for processing classified information. In the course of 2007, BELNIS drew up the White Paper '*Towards a national policy in information security*' (free translation). This revealed that, in Belgium, this problem is being handled only in a fragmentary manner. The White Paper formulated a number of proposals to eliminate the shortcomings.[133] The recommendations below were considered essential by the Standing Committee I[134]:

- approval of an enabling legislation laying down the general national objectives with respect to information security;
- designation of institutions entrusted with the task of achieving these objectives;
- establishment of a national authority for the certification and homologation of sensitive systems, which acts in consultation with the ANS/NVO and the GISS

- processing of warnings and responding to computer attacks: technical analysis, exchange of information with other CERTs, contribution to specific technical studies;
- preparing and maintaining a database of vulnerable locations;
- prevention by disseminating information about precautions to be taken to minimise the risk or, in the worst case, the consequences of the incidents;
- possible coordination with other entities (outside the scope of action): network competence centres, operators and providers of Internet access, national and international CERTs.

131 BELNET performed these tasks in collaboration with the Belgian Institute for Postal Services and Telecommunications (BIPT).

132 A CERT was also set up within Defence with the task of analysing suspicious activities and handling security incidents occurring on the computers in its networks. The team was originally called Computer Security Incident Response Capability (CSIRC) and its task was limited to processing information security incidents.

133 The Standing Committee I noted that the White Paper does not make any reference to the possible role to be performed by State Security in this matter.

134 Meanwhile, a number of recommendations have been implemented: the creation of a national CERT (called CERT.be), the creation of a system for inventorying of critical ICT infrastructure, the appointment of information security advisors in federal administrations, etc.

– improvement and coordination of the Belgian representation in international working groups[135];
– preparation of an inventory of the – both public and private – critical ICT infrastructure in Belgium.

II.2.2. STATE SECURITY

II.2.2.1. Powers and resources

State Security only has a limited role within the framework of public services described (*supra*). The legislator did not assign the service the legal task of 'protecting' ICT networks; neither does State Security have the legal and technical capacity to take electronic countermeasures.

With the resources available to them and taking into account the initiatives of the various relevant bodies and services, State Security limits itself to its 'intelligence task'. This consists in gathering information on (impending) attacks and interceptions of communications originating from '*state*' and '*non-state*' *actors*.

With regard to any detected (whether or not successful) attacks, the only relevant sources of information are IT investigations (*computer forensics*). These refer to the legal and technical capacity of e.g. being able to identify e-mail addresses and the holders of these addresses. Until the implementation of the SIM Act, State Security did not have this option. Since then, the service can, by means of a specific method, proceed to take '*measures for identifying the subscriber or regular user of an electronic communications service or of the used means of electronic communication*', and '*measures for tracing call-associated data of electronic means of communication and the localisation of the origin or destination of electronic communications*' (free translation).[136]

II.2.2.2. IT section of State Security

Within State Security, an IT section has been assigned the task of providing operational ICT support to the field services and managing the IT systems of State Security. But this section also has the task of monitoring threats to ICT systems, developing documentation on observed trends, carrying out awareness-

135 For example, it appears that the BIPT, the GISS and a number of individual experts – often volunteers – represent Belgium in numerous international working groups without any actual coordination with other concerned authorities.

136 Article 18/2 §1, 4° and 5° of the Intelligence Services Act.

raising campaigns, issuing security recommendations as well as conducting investigations in response to observed incidents.[137]

The Strategic Plan of State Security provided for the appointment of an ICT Director and the expansion of the staff of this section. However, the service was not granted the authorisation, required for carrying out these measures, by the Staff Service P&O of the FPS Justice and the Inspectorate of Finance. The Standing Committee I concluded that this situation was highly problematic and recommended that the necessary qualified staff should be made available.

II.2.2.3. INFOSEC equipment[138]

Information originating from foreign services may only be processed if internationally applicable security standards are complied with. Therefore, State Security only makes use of certified and homologated equipment. But due to the lack of (technical) resources at the ANS/NVO (*supra*), State Security is still obliged to make use of systems and procedures certified by foreign authorities. The Standing Committee I feels that this is a problem.

II.2.2.4. Threat assessment

Given the number of potential targets (European institutions, headquarters of the NATO and SHAPE, Belgian public institutions, research institutes and high-tech companies), State Security believes that the threat of cyber attacks must be taken seriously. Cyber attacks that could threaten Belgian interests and security originate from foreign powers, independent individuals and groups, cyber pirates as well as from the organised crime sector. Hence, State Security requests Belgian authorities to urgently take appropriate protective and investigative measures[139], which may include awareness-raising campaigns, preventive measures and an emergency plan in case of a large-scale cyber attack.

---

137 The members of the IT section also take part in the activities of the Working Group on Electronic Attack (WGEA) of the Club of Bern. This working group meets to exchange information on trends and observed incidents related to cyber attacks against ICT systems as well as to coordinate joint campaigns, if required.

138 INFOSEC refers to the application of security measures aimed at protecting information that is processed, stored or forwarded by communication and information systems or other electronic systems, against infringements of the confidentiality, integrity, or availability of this information (whether accidental or deliberate infringements as well as to prevent infringements of the integrity and availability of the systems themselves).

139 In November 2007, State Security did not hesitate in labelling the attitude adopted by the government at that time as being 'near blind' with regard to this matter.

II.2.2.5. Awareness-raising campaigns and targeted interventions

State Security has focused a lot of attention on raising awareness regarding general or specific threats. For example, it warned the Belgian authorities that the confidentiality and integrity of communications via a *Blackberry* can be risky. In the same context, the service notified numerous authorities (for example, the Minister of Justice, the Board for Intelligence and Security, the management committee of the FPS Justice, and the FPS Foreign Affairs) about the threats of cyber attacks. State Security has also participated in organising an awareness-raising campaign for European Members of Parliament and a briefing was organised for Belgian Members of Parliament and representatives of other government bodies.

Today, the INFOSEC activities of State Security are focused on targeted interventions with regard to incidents notified to the service by the victims themselves, where these victims cooperated spontaneously with the service. The IT department of State Security participated e.g. in an investigation involving security officers of Foreign Affairs. The aim of this was two-fold: to find digital proof of an attack and to verify whether and to what extent the cyber attacks had harmed the integrity of the IT infrastructure.

II.2.3. GENERAL INTELLIGENCE AND SECURITY SERVICE

II.2.3.1. Threats

The GISS monitors the increasing number of attacks against information networks of federal authorities (such as Defence[140]) and also collects information from open sources about cyber attacks detected abroad. Such penetrations appear to be increasingly complex, more difficult to trace and the source and precise reasons for such attacks are often difficult to identify.

With regard to the strengthening of the American legislation on the interception of communications (cf. *Echelon*), the Committee found that the actions of the American intelligence services do not appear in the Intelligence Steering Plan. In fact, the GISS relies on the loyalty of the partner services within the NATO, since the application of the *Patriot Act* is targeted against the enemies of the United States.[141] But the GISS recognises that the risk of interception has

[140] One of the attacks involved the so-called 'Conficker' virus and its variants. But the GISS could not detect any infections in its classified IT systems. However, at the end of 2008, cases of infection were identified in the unclassified administrative network of Defence.

[141] In 2000, the GISS informed the Standing Committee I that any military espionage originating from Belgian's allies was not a high-priority assignment for them (see STANDING COMMITTEE I, *Rapport d'activités 2000*, 55). In this regard, State Security stated that if the implementation of the *Patriot Act* should entail an act constituting an infringement of one of

increased and therefore requires classified information to be encrypted during transmission.

II.2.3.2. INFOSEC section

Within the Security (S) Division of the GISS, the INFOSEC section is active in the area of electronic protection and investigative measures. In other words, the section is active in the area of prevention and detection and recently it has been made responsible for providing a response (see II.2.3.4). In recent years, it has conducted investigations into various incidents. The GISS analysed the *modi operandi*, assessed the damage incurred and informed the military authorities regarding this.

This section, however, encountered serious difficulties in recruiting and retaining qualified personnel. Many of them switched over to the private sector, where salaries are much more attractive. The 2009 recruitment plan provided for additional IT specialists for the GISS, who were eventually recruited in 2010. However, based on the investigation, the Committee warned that this might not be sufficient to meet the chronic staff deficit.

II.2.3.3. Raising awareness, support and management

On the advice of the GISS, the Ministry of Defence took various measures to cope with information attacks. For example, staff were routinely informed about the threats and security rules to be applied, an internal security regulation was drawn up, security audits and controls were performed in the units and new technical means were applied (improvement of the software, configuration of the '*Intrusion Prevention and Detection System*', etc.).

Furthermore, the GISS also provides assistance to other federal services. Hence, the service is active within the BELNIS platform, it works together with State Security for analysing spyware, provides support for CERT.be and raises awareness among the Federal Public Services and advises these services in implementing secure networks.

Finally, the GISS also manages a secure intranet service on the FEDMAN network (see II.2.1). This network was created to exchange classified information between the CUTA, the intelligence services and the Federal Police on the one hand and, on the other hand, in order to be able to disseminate classified information from the CUTA to the relevant Federal Public Services. The network can also be used for exchanging classified information between all federal administrations connected to the network.

---

the interests State Security is obliged to protect under the law, it would not refrain from communicating its intelligence to the competent bodies.

II.2.3.4. A new assignment for the GISS

Until recently, due to the lack of a legal framework, the GISS could not take any electronic countermeasures in the event of a cyber attack, since there was no legal provision permitting this. In the course of the investigation, the SIM Act introduced changes in this respect: '*In the context of cyber attacks on military computer and communication systems or systems controlled by the Minister of Defence,* [the task of the GISS is to] *neutralise the attack and identify the perpetrators, without prejudice to the right to immediately respond with its own cyber attack, in accordance with the provisions related to the law on armed conflicts*' (free translation).[142]

The Standing Committee I expressed its satisfaction with this new assignment. However, it wondered why such a possibility was not provided in case of attacks against the IT system of other public services or ICT systems that are considered part of the national critical IT infrastructure.

II.2.4. CONCLUSIONS

Both State Security and the GISS are aware of the seriousness of the threats posed by cyber attacks to the critical (civilian and military) information systems of the country. The two intelligence services have therefore taken initiatives to raise awareness regarding this issue among their 'clients' and they continuously point out the need for taking protective measures.

To the extent permitted by the limited resources at their disposal, the services also carry out investigations into specific attacks against information systems. This is a mostly defensive approach based on detection and evaluation. Recently, a reactive approach was also included as an option for the GISS.

Despite everything, it had to be concluded that the lack of an overall federal policy on information security makes our country very vulnerable to attacks against its critical information systems and networks.[143]

Moreover, there is a lack of a central service to ensure the security of ICT systems. None of the institutions currently competent in this area appear to have a complete view of the problem. Given this high level of fragmentation, the Standing Committee I supported the decisions of the White Paper '*Towards a national policy in information security*' (free translation). The Standing Committee I also recommended that a federal strategy be developed in this matter and that a single agency be set up soon with the task of coordinating

142 Article 11 of the Intelligence Services Act.

143 As early as in 1995, the Standing Committee I drew attention to the importance of the security of information systems and the need to develop an overall security policy in this regard (see STANDING COMMITTEE I, *Rapport d'activités 1995*, 114–118).

activities related to information security. The experience and know-how of the Belgian intelligence services can be used within or for the benefit of this agency.

It could be established that the members of the GISS and State Security – without real coordination with other authorities – represent Belgium in certain international working groups. It is necessary to clearly define the role assigned to the intelligence services with regard to the protection of information systems. The Standing Committee I recommended that the Ministerial Committee for Intelligence and Security takes the necessary steps to this end.

Finally, it must be ensured that the Belgian intelligence services have access to the required (technical and human) resources in order to fulfil their assignment in this matter. In particular, they must be able to recruit and retain qualified staff members.

II.3. INFORMATION POSITION AND ACTIONS OF THE INTELLIGENCE SERVICES WITH REGARD TO LORS DOUKAEV

On 10 September 2010, an explosion took place in a hotel in the Danish capital, Copenhagen. In this explosion, a certain Lors Doukaev was slightly injured. The explosives he was carrying, intended for launching an attack on the Danish newspaper 'Jyllands Posten', had exploded prematurely.[144]

Doukaev was of Belgian nationality and hence, the Standing Committee I opened an investigation into the information position and the actions, if any, of the Belgian intelligence services prior to the failed attack.

II.3.1. FACTS

II.3.1.1. Who is Lors Doukaev?

Doukaev was born in 1986 in Chechnya. At the age of 10, he became the victim of a grenade explosion, as a result of which his right leg had to be partially amputated. In 2000, he fled with his mother and sister to Belgium. They were granted the status of political refugee. Later, in March 2006, Doukaev acquired the Belgian nationality. As required, State Security was asked if there were any possible contraindications. However, the person was not known to the service at that time.

144 Based on these charges, Doukaev was sentenced in mid-2011 by a Danish court to twelve years in prison.

II.3.1.2. Information position and actions of the GISS

In 2007, Doukaev was accidentally spotted by an agent of the field services of the GISS. He had noticed a man with a beard and an amputated leg on the street in the company of a veiled woman and he wanted to check whether the person was possibly a member of a radical movement. But verifications within his service, with the Federal Police and with the Immigration Service[145] did not reveal anything suspicious. Therefore, the intelligence officer did not prepare a report on this for his service.[146] However, he did record the information in his own documentation.

II.3.1.3. Information position and actions of State Security

In a 'routine message' from a foreign partner service at the end of January 2010, State Security was informed that, during a roadside check in October 2009, some participants of a meeting of a radical Islamist movement had been identified. Lors Doukaev was one of them. Prior to this date, he had never attracted the attention of State Security.

Within State Security, the message from the partner service was simply forwarded to the relevant operational departments and the competent Analysis Department. The message received a 'routine treatment' for three reasons: a lot of time had elapsed between the findings (October 2009) and the communication of the message (January 2010); the partner service had not asked any specific question; and Doukaev did not appear in the State Security database.

Thereupon, one of the operational departments consulted the elements in the possession of the Immigration Service and sent the message from the partner service and the results of its investigation to the competent provincial post. The message and the results of the investigation were sent labelled 'FYI'; no specific questions were formulated.

The very same day, the head of the provincial post assigned the case 'for investigation' to the intelligence officer charged with monitoring the Chechen milieu. The important thing was, therefore, that the initial status of the message had been changed. The State Security officer contacted the police inspector of the district where Doukaev lived and learned that the person was only known to the police for old charges of assault and battery and that he had left the area a few months ago, without further information. The officer also contacted his informants, but without result. However, he did not contact either the GISS or the Federal Police.

145 State Security was not consulted in the matter.

146 As a consequence, no information was passed on to other services, such as State Security or the CUTA.

The State Security officer did not think it useful to draw up a report or notify other services regarding this matter. He thought that he had too few elements in his possession to justify this. State Security subsequently concluded that this was anything but professional and took measures to prevent a recurrence (see below). The Committee also decided that the dossier deserved greater attention, given the message from the partner service, Doukaev's 'disappearance' and his origin. On the other hand, the Committee emphasised that the initial message from the central services of State Security had only been sent labelled 'for your information'.

II.3.1.4. Police information

In May 2010, the police services of a neighbouring country requested information about a certain 'Lors' from the federal judicial police of Liège. The Liège police replied that this concerned Lors Doukaev, that he was known for charges of assault and battery, and that an arrest warrant had also been issued against him as a result of a criminal conviction in February 2010. Finally, the police reported that Lors Doukaev '*was not known at that time to* '*Terro*' *and that they had never heard any mention of him among the Islamic community in Liège*' (free translation).

Furthermore, the Federal Police had also obtained information from a source. In short, it appeared that a fundamentalist Islamist organisation had allegedly recruited Lors Doukaev. He had apparently let his beard grow and had been looking for weapons and explosives. But the Standing Committee I could not determine whether this information dated from before or after the failed attack.

II.3.2. CONCLUSIONS

The Committee emphasised that it is difficult for the security services to identify a so-called '*lone wolf*', especially if the radicalisation process proceeds as swiftly as it possibly did in the case of Doukaev. Whether or not the person actually meets this profile will, however, only become apparent after viewing the information available with the Federal Police.

Regardless of this, the Committee reached the conclusion that both intelligence services had separately possessed partial information regarding Doukaev.

Regarding the GISS, the Committee questioned the relevance of the information possessed by the officer and its significance for any database. The inclusion of information in a file, simply on the basis of elements such as clothing and physical characteristics, not only seems excessive but even contrary to privacy legislation.

Regarding State Security, the Committee noted that information from a friendly service had not been exploited. The investigation at a provincial post was carried out '*a minima*' and was not followed up with a suitable report. Nevertheless, State Security drew lessons from this shortcoming and took structural measures to avoid such mistakes in the future.

The Committee further determined that no information had been exchanged either between the intelligence services or between the intelligence services and police. In this context, the Committee was specifically referring to the available police information. It therefore requested the Standing Committee P to open an investigation into the intelligence possessed by the police services prior to Doukaev's arrest in Copenhagen. The report of the Standing Committee I will, if necessary, be supplemented and updated based on the findings from this investigation.

The Committee emphasised that if the partial information had been shared, it would have become clear that the intelligence and police services should have devoted special attention to the person in question. Naturally, this does not mean that if this had been done, the attempted attack could have been prevented with certainty.

In general, the Committee pointed out the importance of the direct exchange of concrete information between the intelligence services and the police services. It emphasised the fact that the exchange of information should not be limited to the exchange of (general or specific) assessments at, for example, CUTA level. Since, the lack of a direct flow of information can cause the services to miss opportunities for tracing persons who are a threat to society and citizens.

II.4. INFORMATION FLOWS BETWEEN THE CUTA AND ITS SUPPORTING SERVICES

The core task of the CUTA is to carry out, at its own initiative or at the request of certain authorities, ad hoc or strategic assessments of threats related to terrorism and extremism.[147] This task is entrusted to (externally recruited) analysts and to experts (seconded from the so-called 'supporting services'). These supporting services form the most important sources of information for the CUTA. They include State Security, the GISS, the Integrated Police (both the Federal as well as Local Police forces), the Administration of Customs and Excise of the FPS Finance, the Immigration Service of the FPS Home Affairs, the FPS Mobility and Transport and the FPS Foreign Affairs.[148] Each of these services should, in

147 This task is defined in the Threat Assessment Act of 10 July 2006 and its implementation decree of 28 November 2006 (Threat Assessment Decree).

148 The Act allows the number of supporting services to be increased. The CUTA feels that there is currently no need for this. However, this does not mean that it does not maintain any

principle, have a single point of contact through which the exchange of information, intelligence and assessments from and to the CUTA should be carried out.

With this joint investigation, the Standing Committees P and I wanted to draw up a *status quaestionis* of the information flows between the CUTA and the supporting services, based on an extensive survey. Moreover, the actual exchange of information was studied through a concrete test case. This test case concerned the threat assessment of a possible escape attempt during the terrorism trial of Malika El Aroud.[149] The general findings of the two phases of the investigation are explained below in brief.

II.4.1. INFORMATION FLOWS FROM A QUANTITATIVE PERSPECTIVE

The Committees wanted to gain an overall view of the number of elements of information, reports and analyses that were exchanged between the services. This was almost impossible, since each stakeholder seemed to have its own method of counting and because certain single points of contact were not aware of all the exchanged intelligence and documents. This was because the CUTA often communicated directly with certain key figures within the supporting services. The Committees did not feel that this was a problem in itself, provided that these contacts are 'traceable' and the single point of contact has an overall view of matters.

Other notable conclusion of this section of the investigation was that the figures communicated by the CUTA to the Committees differed from those published by it elsewhere subsequently.

Notwithstanding these findings, it became clear that the flow of information to and from State Security, the GISS, the police and the FPS Foreign Affairs was

---

contacts with other services. For example, the Governmental Crisis Centre (for threat assessments during visits), the Directorate-General for Prevention and Security of the FPS Home Affairs (in the area of supporting social initiatives focused on radicalisation), the Federal Prosecutor's Office, the Belgian Financial Intelligence Processing Unit (with regard to suspicious transactions), the FPS Justice (in the area of international cooperation), the Criminal Policy Service and the Office of the Commissioner General for Refugees and Stateless Persons (CGRS/CGVS) are considered as 'partners' by the CUTA. These services were outside the scope of this investigation.

149 Afterwards it appeared that, for several reasons, this test case was not representative of the findings from the general part of the investigation: it concerned an ongoing criminal investigation under an embargo procedure, the information was provided on the basis of a very specific question, the threat assessment was primarily based on elements from another criminal dossier, the short period between the request for an assessment and the start of the trial and only a limited number of supporting services played a role in this threat assessment.

substantial[150] and showed an increasing trend. However, the same did not apply to the Administration of Customs and Excise, the Immigration Service and the FPS Mobility: the information that reached the CUTA from these services was limited to a few (dozen) messages annually.

II.4.2. SINGLE POINTS OF CONTACT (SPOC)

Each supporting service must organise a single point of contact (SPOC) within its organisation through which information is exchanged with the CUTA (Art. 11 of the Threat Assessment Decree).

The SPOC of State Security, the GISS and the FPS Foreign Affairs (i.e. the Terrorism Coordinator) were described very positively by the CUTA.

However, the Administration of Customs and Excise[151], the Immigration Service[152] and the FPS Mobility[153] lacked a clearly designated and recognised point of contact. Although this shortcoming was partially made up for by the seconded experts, the Committees felt this should be remedied in the short term.

Neither was the CUTA entirely positive about the 'police contact point'. A SPOC for the Integrated Police has never been properly designated as such. There is a contact point for the Federal Police, the National Contact Point (NCP), but apparently the NCP merely operates as an intermediary for, on the one hand, the DGA (DAO)[154] with respect to administrative information and, on the other hand, for the DJP/TERRO[155] with respect to judicial information.[156] Furthermore, the Local Police have a limited involvement. Given the organisation of information flows within the Integrated Police, all relevant information should, in theory, reach the DJP/TERRO and via this route, the

150 However, see the findings of the investigation into 'A planned mission abroad by the CUTA' (Chapter II. 5).

151 The contact person designated by the Administration of Customs and Excise stated during the first hearing that he was unaware of his appointment.

152 The Immigration Service had designated the Bureau of Investigations within the Inspection Directorate as the single point of contact. But the CUTA believed that the point of contact was the Administrator-General of the service.

153 The contact person designated at the FPS Mobility was not at all visible within the structure of the organisation. The fact that this FPS is composed of three independent pillars (land, water and air transport) complicates the work of this contact person. His contribution is therefore very limited. The CUTA also acknowledges this and therefore, usually directly contacts certain individuals within the organisation.

154 Directorate of Operations and Information Management of the General Directorate of Administrative Police of the Federal Police.

155 Directorate of Crime against Persons/Terrorism.

156 The CUTA argued that the DGA should become the main channel. The Committees question the feasibility of this option, in view of the confidentiality of certain judicial information. Since, it can hardly be assumed that the judicial authorities would agree to simply allow this information to be handled via the information channels of the administrative police.

CUTA. However, the direction of the CUTA doubted whether this is actually happening and wanted a greater involvement of the Local Police in this matter.[157]

II.4.3. CONCEPTS OF 'INTELLIGENCE' AND 'RELEVANT'

Pursuant to Article 6 of the Threat Assessment Act, the supporting services are obliged to communicate to this body all 'intelligence' available to them in the context of their legal assignments and which is 'relevant' for the operations of the CUTA. With regard to this obligation, the Committees reached two conclusions.

On the one hand, unlike the police, the two intelligence services interpret this rule such that they do not, in principle, send any raw information but only processed information (also see II.10.10 and II.10.11).

On the other hand, it seemed that it was not always clear to all the supporting services when the information is 'relevant' or not. This was applicable to e.g. the FPS Foreign Affairs, which tried to remedy this through regular consultations with the CUTA. But the integrated police also appeared to have had some problems in the past, especially regarding the 'extremism' component. To solve this problem, a working group was set up with members from the CUTA, the Federal judicial and administrative Police and the Permanent Commission for the Local Police.

II.4.4. ACKNOWLEDGEMENTS OF RECEIPT AND MONITORING OF RESPONSE TIMES

Article 11 §§2 and 3 of the Threat Assessment Decree require that every request for information should be the subject of an automatic confirmation or acknowledgement of receipt which trigger the regulatory response times. However, this regulation does not appear to be put into practice, since neither the CUTA nor the supporting services work with a well-developed monitoring system. It is assumed that if the service does not respond to a request, it does not have the relevant information.[158]

Furthermore, it was not always clear whether messages from the CUTA were being sent labelled 'for your information' or 'for action'.

---

157 Given the structure of the Integrated Police, the Federal Police have no authority over the Local Police. Therefore, the CUTA defended the fact that it had to maintain direct contacts with the main forces of the Local Police. The Committees can endorse this method provided the point of contact for the Integrated Police retains an overview of the information flow from and to the police.

158 This method was also followed in the test case.

II.4.5. TWO EMBARGO PROCEDURES

To prevent the uncontrolled dissemination of certain sensitive information, the Threat Assessment Act has implemented two so-called 'embargo procedures': one with respect to judicial information obtained from the police services (Art. 11 of the Threat Assessment Act) and the other with respect to intelligence obtained from State Security, the GISS, the Administration of Customs and Excise and the FPS Foreign Affairs (Art. 12 of the Threat Assessment Act). Both procedures should make it possible that this intelligence is not mentioned as such in assessments or ensure that not all authorities receive assessments mentioning this information.

In both cases, in principle, the service providing the sensitive intelligence only communicates this to the Director of the CUTA. In practice however, the direction of the CUTA interprets this regulation in such a way that not only the Director personally, but also the staff members working on the case in question are notified of the sensitive data.[159]

In recent years, the embargo procedure *ex* Art. 12 of the Threat Assessment Act has no longer been availed of. However, embargo dossiers under Article 11 of the Threat Assessment Act have been applied. Such an application did not give rise to any problems.

In addition to Articles 11 and 12 of the Threat Assessment Act, an embargo procedure is also defined in Articles 44/1 ff. of the Police Function Act. But the Committees noted that the term 'embargo' is often used without it being clear as to which procedure is being referred to. Such confusion regarding concepts should be avoided.

II.4.6. THIRD PARTY RULE OR THIRD COUNTRY RULE

According to the CUTA, the 'third party rule' in (international) practice is evolving towards a 'third country rule'. This is reflected in the fact that information from abroad is now forwarded with the message '*for Belgian eyes only*'. This has led the CUTA to believe that the original mistrust towards the CUTA in this area is gradually disappearing.

For State Security and the GISS too, the third party rule did not present any problems in practice. Since the CUTA has become better known abroad, most countries appear to send information at present '*for Belgian eyes only*', whereby the use of this information is no longer limited to a particular service.

---

159 In this context, also see STANDING COMMITTEE I, *Rapport d'activités 2008*, 108–109.

II.4.7. A SECURE COMMUNICATION AND INFORMATION PLATFORM

Most of the supporting services emphasised the fact that the existing communication and information system is very expensive and not very efficient. It also appeared that a lot of necessary connections were still missing. This is not only with reference to some of the supporting services (such as the FPS Mobility), but also other recipients of the CUTA assessments, such as the members of the Ministerial Committee for Intelligence and Security and the various 'partners'. Finally, not all supporting services had provided for a permanent monitoring of the system and certain documents are still sent via other channels (e.g. by fax or bearer).

II.4.8. DEALING WITH CLASSIFIED INFORMATION

Although all the supporting services have a security officer, all of them could not guarantee that all provisions of the Classification Act are being respected. Therefore, a security incident involving classified information cannot be ruled out in these services.

As far as the use of classified information is concerned, there were only some exceptional issues: if necessary, information can be (partially) declassified and disseminated within the supporting service. It is obviously different if it is not permitted to declassify the information. In this context, the police noted that it is sometimes difficult to work optimally with such information, since there is no ICT system within the police services (such as, for example, the National General Database) that meets the applicable regulatory standards and hence, a paper dissemination must be relied on.

II.4.9. SOME SPECIFIC COMMENTS BY AND ABOUT THE CUTA

In general, the direction of the CUTA stated that its operations were up to speed. There were no significant problems in the exchange of information and the CUTA was convinced that it is receiving all the relevant information[160] and that this information flow is growing. The Coordination Unit felt that there was an improved working relationship with the supporting services. While in the early years, some services regarded the CUTA more as a competitor, today they seem

[160] Also as regards the test case, the CUTA was of the opinion that it had received all the relevant information at that time.

to be aware of the value added by it, thanks to its assessments, which provide a more overall picture of certain threats.

At the time of the investigation, the direction of the CUTA was almost fully staffed[161]: ten of the twelve analysts and nine of the eleven experts were operational. As for the experts, it appears that all the supporting services have accepted the principle that they need to second an employee. However, they do not make this a real priority: it can take quite a while before a new expert is deputed. As a result of this, an expert from State Security and one from the FPS Foreign Affairs were missing a long time. The CUTA appeared to be very satisfied with the level of the available persons, notwithstanding the fact that it is difficult for some services to identify a person who is familiar with all aspects of its administration. For instance, this is the case with the FPS Mobility, which consists of three totally different entities[162], and the Administration of Customs and Excise, which consists of fourteen separately operating divisions. As far as the police is concerned, it appears difficult to represent the 'Integrated Police' because this includes not only the Federal Police but also every local police zone.

Finally, the Standing Committees P and I concluded that the future objectives formulated by the CUTA for its own organisation appeared to be very general and not easily measurable. Also, it was not clear whether these objectives were in line with the expectations of the various authorities involved.

II.4.10. SOME SPECIFIC COMMENTS BY AND ABOUT STATE SECURITY

In general, State Security described its relationship with the CUTA as being a positive one.

The flow of information from and to State Security[163] shows not only an increase in absolute numbers, but the content seems to have also improved significantly. However, State Security categorises the quality of the intelligence as being extremely variable. Moreover, the service is urging for a refinement of the threat assessment level and an improved reporting of the source. For example, it is not always clear from where certain information is derived. This can lead to State Security reading a confirmation of its own findings in an assessment made by the CUTA, while the work of the CUTA is based solely on information from State Security itself. Or sometimes the information on which the CUTA relies is derived purely from open sources, while this is not explicitly mentioned.

---

161 Despite this workforce, the CUTA is still not able to organise a 24-hour on-call service. Outside working hours, only a call-back system is provided.

162 Transport by land, sea and air.

163 State Security only passes on assessments and intelligence to the CUTA. It is only in case of imminent danger that the raw information is also provided.

Another thorny issue are the contacts maintained by the CUTA with homologous foreign services, pursuant to Article 8, 3° of the Threat Assessment Act. If these services are themselves part of an operational intelligence service[164], this is seen as a problem by State Security. Since, State Security considers its sister services to be its natural correspondents and fears that the contacts of the CUTA are not limited to the department responsible for drawing up threat assessments.

II.4.11. SOME SPECIFIC COMMENTS BY AND ABOUT THE GISS

The CUTA and the GISS describe their mutual relationship as being a positive one. No serious problems seemed to have occurred until now.

Just like State Security, the GISS assumes that the CUTA primarily requires contextualised information, as a result of which finished products (assessments) are usually sent. In exceptional cases (imminent danger), raw information is provided by the GISS. This approach was developed in agreement with the CUTA and has been in effect since 2007.

Several times in the past, the GISS had already availed of the opportunity to request the CUTA for an assessment regarding a specific threat. One of the reasons for this was that the GISS was experiencing a lack of assessment capacity, since a number of its analysts had been assigned jobs within the CUTA.

A sensitive point for the GISS continues to be the role played by the CUTA with regard to threat assessments related to Belgian interests abroad. In particular, Intelligence Division of the GISS is not convinced of the CUTA's competence to carry out threat assessments abroad. Moreover, this division questions the quality of the assessments produced.

The GISS is urging for the development of broader and more prospective threat assessments. At present, the assessments apparently focus too much on the aspect of 'public order'.

Unlike State Security, the GISS felt that the CUTA had made sufficient mention of its sources in its assessments.

II.4.12. GENERAL CONCLUSION

The two Committees concluded that the information flows showed an upward trend, both in terms of quantity and quality. However, a number of supporting services had some serious catching up to do in order to operate at a certain level.

---

[164] For similar examples, see: STANDING COMMITTEE I (ed.), *Fusion Centres Throughout Europe. All-source Threat Assessments in the Fight Against Terrorism*, Antwerp, Intersentia, 2009, 220 p.

In general, the supporting services are positive about the operations of the CUTA[165] and this Coordination Unit is seen as an added value. Despite this, the Committees felt that there are further opportunities for improvement, e.g. by responding to the specific needs of certain supporting services.

II.5. A PLANNED MISSION ABROAD BY THE CUTA

In early 2009, the Coordination Unit for Threat Assessment (CUTA) planned a short mission to the Democratic Republic of Congo (DRC). However, this plan was abandoned at the very last moment.

The purpose of this mission would have been to allow the CUTA to gain a better idea of the security situation in the DRC and the possible presence of radical, extremist or terrorist groups. Meetings had been planned with many public and private bodies and individuals.

According to the CUTA, one of the underlying reasons for the mission was that the FPS Foreign Affairs had failed to pass on intelligence concerning Central Africa for a long time now, despite its obligation to do so and despite concrete initiatives taken thereto by the CUTA. When, unexpectedly, the opportunity arose to visit the DRC and, by doing so, to gain more information about this region, the CUTA seized this opportunity: there was place on-board a military flight that was to leave within the week. As a result, the preparation time for the mission was very short.

The management of the CUTA designated an analyst and an expert from within its organisation to carry out this mission and contacted the FPS Foreign Affairs, the Ministry of Defence and the Defence cabinet.[166]

Although the concerned bodies initially extended their cooperation, the cabinet of the Minister of Foreign Affairs suddenly announced that the mission could not take place at that particular time, because it was too delicate. But the Director of the CUTA was of the opinion that the real reason lay elsewhere: a supporting service was thought to be annoyed with the initiative taken by the CUTA to operate independently.

Even though the foreign mission had been cancelled, the Standing Committees P and I still decided to open a joint investigation. They wanted to verify whether such missions fell, in general, within the scope of or arose out of the tasks entrusted to the CUTA by or pursuant to the Threat Assessment Act. Specifically with regard to the cancelled mission and from the point of view of its effectiveness, the question asked was whether the CUTA had taken all the

165 All the respondents issued a very positive to a rather moderately positive report regarding the evolution of information flows. Nevertheless, there was also an occasional mention of certain isolated incidents.

166 Apparently, the CUTA had also informed the Head of the GISS regarding this mission.

necessary preparations and precautions. Finally, a third aspect was also discussed in the context of this investigation. This is explained below.

II.5.1. LACK OF INFORMATION ON CENTRAL AFRICA

The study visit was organised – according to the CUTA – because the Coordination Unit had not received any information from the FPS Foreign Affairs since 2008. From mid-2009, this supporting service had started providing considerably more information, though not with respect to the situation in Central Africa, despite specific questions in this regard. Therefore, the CUTA wanted to increase its knowledge of the region through this mission, so that it could provide accurate assessments. According to the Director, the fact that the mission could not be carried out, prevented the CUTA from improving its current information position with regard to the DRC.

However, the Committees concluded that the mission had been triggered solely by an opportunity (i.e. the imminent military mission to the DRC). In view of this, the allegedly essential nature of the proposed mission did not appear to be very convincing.

Regardless of this, the Committees decided that the attitude of the FPS Foreign Affairs was inadmissible. As a result of this investigation, the Minister of Foreign Affairs even intervened to remedy the situation. In consultation with the CUTA, it was decided to hold regular information meetings regarding Central Africa. The Minister also agreed to a mandatory secondment of an expert from the FPS Foreign Affairs to the CUTA.

The Committees also criticised the fact that they had become aware of the malaise between the CUTA and one of its supporting services only in a rather coincidental and indirect manner. The CUTA claimed that its operations with regard to Central Africa had been hindered for more than a year due to the inadequate flow of information about this region from the FPS Foreign Affairs. Although this might point to a structural dysfunction, the Committees – whose precise task is to make recommendations, where appropriate, for improving efficiency – had not been spontaneously informed of regarding this.

II.5.2. PREPARATION FOR THE MISSION

The Standing Committees P and I also noted that the mission appeared to have been planned rather poorly. The preparation consisted of a limited correspondence and a general identification of the *desiderata*. No substantive programme had been developed, no security briefing was held and the Ministers of Justice and Home Affairs were not informed in advance.

The Committees were of the opinion that the delicate nature of official missions in the Central African region requires maximum diplomacy and prudence, especially on the part of a body such as the CUTA.

Therefore, there was definitely room for improvement with regard to the preparation for this mission, in terms of content, communication and organisation. Besides a detailed planning, attention should also have been given to developing appropriate and specific precautionary measures. A consultation with the intelligence services was also advised. Finally, the politically responsible Ministers in charge should have been informed in advance.

II.5.3. THE VARIOUS ASPECTS OF THE MISSION AND THE LEGAL AND REGULATORY FRAMEWORK

The CUTA is responsible for drafting ad hoc and strategic assessments with regard to potential extremist and terrorist threats targeted against not only the security of the State but also against '*Belgian interests and the safety of Belgian nationals abroad*' (Art. 3 and 8, 1° and 2° of the Threat Assessment Act) (free translation). In addition, the CUTA also has the task of '*ensuring specific international contacts with similar foreign or international services in accordance with the guidelines of the Ministerial Committee*' (Article 8, 3° of the Threat Assessment Act) (free translation).

Besides this, no other tasks have been assigned to the CUTA under the Threat Assessment Act of 10 July 2006. Hence, a mission can never be regarded as a task, but only as a possible added value for carrying out the tasks listed under Article 8 of the Threat Assessment Act.

Does the proposed mission fit within this legal and regulatory framework? The mission had a three-fold purpose. Each aspect is discussed separately below.

II.5.3.1. A study tour

One part of the mission could certainly be regarded as a study tour. Insofar as the purpose of such trips is to enable experts and analysts to build their professional relationships and further develop their expertise at national and international forums, the attempt of the Director of the CUTA to encourage this to the maximum extent must be applauded. This can only improve the quality of the assessments.

II.5.3.2. Specific contacts with homologous services

The planned mission also included a meeting with the Congolese representative of the *Centre Africain d'Etude et de Recherche sur Ie Terrorisme* (CAERT). Given

the mission of the CAERT, the CUTA considers this centre to be a homologous foreign service within the meaning of Article 8 §3 of the Threat Assessment Act.

Although the task described in this article needs further interpretation by the Ministerial Committee for Intelligence and Security, the CUTA has justifiably not waited in undertaking this task. However, such a guideline should be issued soon. This should lead to a better understanding of the concepts of 'specific contacts' and 'similar services'. In this context, the Committees pointed out that the legislator did not, under any circumstances, want the CUTA to gather its own information in the field, on top of and in addition to the information gathered by the supporting services (see II.5.3.3): '*If it should appear that [the CUTA] would gain knowledge of information or data through these contacts, it is required to communicate this to the competent Belgian services or authorities, in order for them to handle this information or data in accordance with their legal tasks.*'(free translation)[167]

II.5.3.3. Gathering intelligence in the field

The Committees concluded that the mission was mainly intended to gain a better insight into and obtain more intelligence regarding the actual situation in the DRC. Both Committees stressed, however, that the CUTA is neither competent nor responsible for filling in *in situ* for the incidental gaps in the information.[168] This is clearly what was intended by the legislator. The parliamentary proceedings with respect to the Act of 10 July 2006 leave no doubts on this matter: the CUTA '*is not a new intelligence or police service, it does not collect first-line information, but assesses the threat based on the intelligence produced or delivered by the participating services*' (free translation).[169] This implies that the CUTA occupies a special position in the Belgian security landscape. Its assessments are essentially the processed product of intelligence and information supplied by the supporting services. These products should themselves be considered as 'intelligence'. However, this does not make the CUTA an intelligence service. Therefore, the Coordination Unit should ensure that there is no misconception regarding its task and statute, in order to avoid causing diplomatic incidents or tensions with the intelligence services. If the CUTA feels that certain supporting services are not fulfilling their obligations fully, they are advised to refer to the Standing Committees and P and I.

---

167 *Parl. Doc*. House of Representatives, 2005–06, no. 51 2032/001, 20.

168 In fact, the CUTA does not have either the necessary *know-how* or resources to operate in the field.

169 *Parl. Doc.* House of Representatives, 2005–06, no. 51 2032/001, 4. In the same context, see *Parl. Doc*. Senate, 2005–06, 3–1611/3, 3 and 12.

II.6. STATE SECURITY, THE FIGHT AGAINST PROLIFERATION AND THE PROTECTION OF THE SEP

II.6.1. FOLLOW-UP INVESTIGATION BASED ON AN ACTUAL CASE

The Standing Committee I had already conducted various investigations into the manner in which the intelligence services carry out the fight against proliferation[170] and the protection of the scientific and economic potential (SEP).[171] State Security[172] has an important role to play in both matters. The intelligence passed on by the service to various public services and the manner in which these services subsequently use the information, can sometimes have far-reaching (adverse) consequences for the companies involved. Moreover, the interests in the fight against proliferation and those related to the protection of the SEP, do not always coincide.

Earlier investigations had revealed that the approach taken by State Security in this matter was sometimes surrounded by a hint of nonchalance. For example, the competent authorities and the Minister in charge were not (always) properly informed. For this reason, the Committee wanted a closer cooperation between the intelligence services and the other relevant authorities.

With the present investigation, the Standing Committee I wanted to verify, based on an actual case, how State Security had in recent years (2006–2011) performed the task of monitoring a Belgian company specialised in the manufacture of high-tech equipment. It also wanted to ascertain whether State Security had taken into account the previous recommendations in the context of the fight against proliferation and the protection of the SEP. Anyway, the investigation did not allow the Committee to conclude that the previously identified deficiencies had been remedied in a meaningful manner.

---

170 See for example STANDING COMMITTEE I, *Rapport d'activités 2005*, 16–35 and *Rapport d'activités 2008*, 40–54.

171 See for example STANDING COMMITTEE I, *Rapport d'activités 2005*, 73 and 102–146 and *Rapport d'activités 2008*, 58–63.

172 Recently, the SIM Act also extended the intelligence assignment of the GISS to include *'the scientific and economic potential with regard to the players, being both natural and legal persons, which are active in the economic and industrial sectors which are related to defence'* (Art. 11 of the Intelligence Services Act) (free translation).

II.6.2. INVESTIGATION FINDINGS

II.6.2.1. Approach taken by State Security on this subject

II.6.2.1.1. Reactive *versus* proactive action against proliferation

Given the regionalisation of the power to grant licenses for arms exports, State Security believes that its role in the area of proliferation is limited.[173] According to State Security, the services responsible for issuing the licenses must carry out the initial verifications and decide for themselves which license applications are to be submitted to State Security. Moreover, State Security believes that it is not competent to give advice to the authorities, but only provide them with information. The Committee did not share this opinion.

But the Committee found that recently – i.e. in its 2011 Action Plan – State Security had assigned an 'active high-priority monitoring' status to the (intermediate) trade in raw materials, tools and technologies that can contribute to the proliferation of weapons of mass destruction. In addition, State Security had assigned an 'active monitoring' status to the study of some 'high-risk countries', targeted awareness-raising within the scientific, industrial and academic environments and to the task of profiling potential targets.

But Committee emphasised the fact that State Security[174] still lacks the material and human resources to enable it to cope with the increase in and the urgency of the activities in the fight against proliferation.

In addition, State Security was of the opinion that an agreement with the Administration of Customs and Excise is absolutely necessary in order to arrive at a comprehensive strategic analysis of proliferation in Belgium. Such an agreement should define clear and practical procedures for the exchange of information between these two administrations.[175]

II.6.2.1.2. Economic *versus* security interests

State Security is well aware of the fact that the fight *against* proliferation and therefore, *for* security also has a downside: since economic interests are also

---

173 State Security is certainly not competent to *materially* verify and obstruct sensitive export transactions, as sometimes requested to do so by some foreign services. Only the Administration of Customs and Excise is competent for this.

174 Regarding the GISS, the Standing Committee I had already expressed regret in its *Activity Report 2008* (p. 51) that only one analyst was assigned within the service to the section responsible for the fight against the '*proliferation of weapons of mass destruction and their carriers*' (free translation). This situation did not appear to have evolved favourably in any way.

175 A meeting that took place in February 2010 for this purpose missed the mark. The aim was to breathe a new lease of life into the 'Working Group on Proliferation' (with representatives from both bodies). The customs services seem no longer interested in signing a protocol with State Security now that they have concluded an agreement with the Regions.

involved, in the sense that the competitive position of a company must be taken into account.[176] In this context, State Security pointed to the risks accompanying the regionalisation of the granting of export licenses: the various competent authorities use different criteria for assessing applications. In addition, the regional administrations sometimes tend to give priority to commercial interests, while the CANVEK/CANPAN emphasises security interests.

In any case, the position of State Security in this matter is clear: in such dossiers, security should always be given priority, even if the economic interest of a company is more concrete and direct. The Standing Committee I shares this point of view.

However, the Committee noted that a proposal had been circulating for some time for a better reconciliation between the two opposing interests: a procedure for '*prior advice*' could be implemented within the CANVEK/CANPAN. This would limit the commercial loss that a company might incur as a result of negative advisory opinions that are issued only after a long time (and sometimes after the materials have already been produced). This course of action was investigated, but the discussion has not (yet) been completed.

II.6.2.1.3. The fight against proliferation *versus* the protection of the SEP against interference

The Committee was able to establish that State Security had paid attention to possible attempts to 'interfere in decision-making processes' by foreign powers in the context of the fight against proliferation. Such interference can be a threat to the SEP.

To properly assess this threat, a good information position is extremely important. However, it appears that State Security is (still) too dependent on the (classified) information they receive from foreign services, even with regard to suspicious transactions taking place in Belgium.

Another important element in this context is the need to 'link' the two matters. Earlier, the Committee had proposed that the analysts and operational agents working in the two domains should be brought together in the same team. They should define a common methodology with the intention of adopting, on behalf of State Security, a clear standpoint with respect to the competent political bodies. Due to insufficient resources, this proposal was not put into practice.

---

[176] For example, State Security found that the enhanced control measures and international sanctions against a particular proliferation country have led to a decrease in the number of (sensitive) export transactions of the company that served as a case study in the investigation.

II.6.2.1.4. Cooperation within the CANVEK/CANPAN

There is still no internal guideline regarding the mandate of the representative of State Security at the CANVEK/CANPAN. Consequently, the content of the information provided to this commission and the manner of its communication (written or oral), are left entirely to the discretion of the concerned individual.

Moreover, there is no cooperation protocol specifying the conditions for the communication and protection of classified information supplied to the CANVEK/CANPAN.

II.6.2.2. Monitoring of the company in question

The Committee was able to establish that State Security had carefully monitored, until mid-2008, a number of transactions of the company with one or more of the so-called 'proliferation countries.

Only after an interruption of almost two years had the company aroused its interest again. This is because foreign intelligence services had informed State Security of new plans for transactions with 'sensitive countries'. During the subsequent, intensive bilateral cooperation, pressure was placed on State Security to use all its resources to oppose the export of certain materials. The transactions were, however, only monitored depending on the information spontaneously supplied by foreign intelligence services. The ministers and the federal[177] and regional services involved were fully and regularly informed by State Security. But this was sometimes hindered by the application of the 'third party rule'.

The Committee concluded that the monitoring of the company in question had been primarily of a 'reactive' and ad hoc nature. Probably, the lack of necessary resources was the main reason for this.

It was not until the end of 2010 that State Security finally turned its attention, in a more general way, to the company itself, its production and its customers and with this, initiated the first 'proactive' search for intelligence.

---

177 '*In order to optimise the efficiency of our work (…), we have intensified the exchange of information with the Belgian authorities which are competent in the fight against proliferation, and we have systematically kept the Minister of Justice informed of any relevant facts that had come to our attention*' according to the Administrator-General of State Security. On several occasions, the State Security representative at the CANVEK/CANPAN also brought into discussion the transactions of the company with some 'sensitive' countries. Information on suspicious orders was communicated to the Commission.

II.7. COMPLAINT FROM A MEMBER OF STATE SECURITY AND HIS SPOUSE

In mid-2010, the Standing Committee I received a complaint from a member of State Security and his spouse. The complaint consisted of four different aspects.

The complainant had received a 'written warning' because he had allegedly revealed his position as a member of State Security to a third party. He found it unacceptable that this notice was stored in his personnel file.

The second aspect was with respect to the fact that the Security Investigations service of State Security appeared to have been aware of statements supposedly made by the complainant during a confidential interview with a psychologist from State Security.

During the same security investigation, old charges, of which his spouse had been the victim, had apparently been brought into question in a slanderous and defamatory manner.

Finally, the complainant claimed that a climate of anti-Semitism had prevailed in the department in which he worked. Symptomatic for this were – according to the complainant – a newspaper cutting and a flyer displayed in an office of State Security.

The Committee examined every aspect of the complaint[178] but also made sure that it did not cross the limits of its legal mandate. Since, certain parts of the complaint did not fall under its jurisdiction. For example, the complainants had labelled the words of the State Security investigators as being 'slanderous and defamatory'. This is a criminal qualification, over which only a court can pronounce a judgement. But the Standing Committee I is always entitled to establish the materiality of the facts and to assess these in the context of its own powers. The same was applicable to the written warning in the complainant's personnel file: although the Committee is not an appeal body in disciplinary proceedings, it may investigate whether State Security is infringing upon the rights granted by the Constitution or the law to its staff members and whether a certain practice can have an impact on the efficiency of the service. Based on the same two points of view, the Committee may also analyse the progress of security investigations, without thereby taking the place of the Appeal Body for security clearances, certificates and advice.

[178] However, pursuant to Article 3, third paragraph of the Classification Act of 11 December 1998, the investigation was temporarily suspended following the appeal lodged by the concerned staff member against the withdrawal of his security clearance.

II.7.1. THE 'WRITTEN WARNING' IN THE PERSONNEL FILE

Despite the fact that the complainant disputed the allegation that he had revealed his position as a member of State Security to a third party without any valid professional reason to do so and despite the discontinuation of the disciplinary proceedings, State Security decided to issue him a 'written warning'. This was included in the personal file of the complainant.

The Committee was of the opinion that such a method was not acceptable given the current regulatory status. Since, this possibility is not provided for in the Staff Regulations of 13 December 2006. In fact, storing notices containing negative elements for unlimited periods of time can cause serious harm to the further career developments of the individuals.

II.7.2. THE OBLIGATION OF PROFESSIONAL SECRECY AND THE SECURITY INVESTIGATION

In the presence of his head of department, the complainant had made certain statements to a psychologist from State Security.[179] Later, this information – which was related to a serious performance problem within his service – was used in a security investigation involving the complainant. This is because the complainant's head of department had informed his hierarchical superior of these statements. The Committee emphasised that though the psychologist is bound by the obligation of professional secrecy[180], the concerned head of department is not bound by such an obligation. Hence, the head of department was entitled to pass on the statements to his hierarchical superior, thereby placing the general interest of his service before the specific interest of his staff member.

---

179 This psychologist was part of the psychological and social support counselling team of State Security. Taking into account the impact of the responsibilities and the psychological and social burdens faced by State Security officials, the Royal Decree of 13 December 2006 has set up such a team.

180 Article 143 of the Royal Decree of 13 December 2006 reads as follows: '*The counselling team intervenes either at the request of the staff member or at the request of the hierarchical superior or a colleague and in the last case, with the consent of the concerned staff member. The members of the counselling team are bound by the obligation of professional secrecy. They work outside the scope of each separate personnel file and guarantee anonymity. They do not, in any way, share the content of their conversations with the management, except with the written consent of the staff member.*' (free translation).

II.7.3. THE INTERVIEW AS A RESULT OF THE SECURITY INVESTIGATION

In order to ascertain the reliability of the complainant, the security investigators examined the old charges of aggression towards his spouse. When the complainant got the impression that the investigators were minimising these charges, he refused to cooperate further in the interview.

The Standing Committee I emphasised that the main purpose of the security investigation was to verify the authenticity of the statements made by the complainant. For this, the investigators were forced to verify whether and for what reason his spouse had filed the complaint at that time. However, there had been no need for them to go any deeper into the criminal qualification which the victim wanted to give to the charges.

II.7.4. THE CONTESTED DOCUMENTS

A newspaper cutting and a flyer were displayed in an office of the service conveying a standpoint in the Israeli-Palestinian conflict. The head of department was not aware of this.

The Committee was of the opinion that the documents were not indicative of the alleged anti-Semitic climate. However, the Committee felt that these did not belong in an office of State Security, given the obligations of discretion and neutrality to be respected by the officials of this service.

In principle, field service officials of State Security have the freedom to express their opinions. But they must refrain, under all circumstances, from publicly expressing their political beliefs and engaging in political activities in public.[181] The officials in question are regularly reminded of these principles, which have been incorporated in a draft of an administrative handbook/code of ethics, which was still being prepared at the time of the conclusion of this investigation.

II.8. BELGIAN REPRESENTATION AT INTERNATIONAL MEETINGS ON TERRORISM

The Standing Committees P and I observed that the Belgian police and intelligence services and the CUTA regularly participated together in international meetings on the fight against terrorism. The question arose whether there was any coordination between these services and whether, in other words, the requirements of effectiveness and efficiency were being

[181] Article 12 of the Royal Decree of 13 December 2006.

observed. Naturally, the CUTA, the Federal Police, State Security and the GISS, as the principal players in the fight against terrorism and extremism, were involved in the investigation. But other supporting services of the CUTA were also interviewed: the local police forces, the Administration of Customs and Excise of the FPS Finance, the Immigration Service of the FPS Home Affairs, the FPS Mobility & Transport and the FPS Foreign Affairs.[182] The Federal Prosecutor's Office and the Governmental Crisis Centre are also regularly represented at international meetings. However, they were not the subject of investigation since the Committees have no supervisory jurisdiction with respect to these bodies.

The investigation examined the subject of international (strategic or operational) meetings, conferences or working groups in the context of the fight against terrorism and extremism, and the Belgian bodies taking part in these. It was also investigated whether there was any prior consultation between the Belgian bodies regarding the agenda and the standpoints that would or should be taken on behalf of Belgium. Furthermore, it was also studied how the results, reports, agreements or standpoints emerging from the meeting were disseminated among participating and/or non-participating services. Finally, the concerned bodies were given the opportunity to express their views on the composition of the delegation at specific forums.

The investigation confirmed that not only the Belgian police and intelligence services and the CUTA but also the FPS Foreign Affairs participate in many international meetings on the fight against terrorism and/or extremism. The information revealed a somewhat kaleidoscopic picture of which body is present at which meeting. Sometimes several services are simultaneously represented within a single forum or meeting.[183] It is also not always clear whether the present services represent Belgium or their own organisations at these forums. Finally, it appeared that not a single service had a complete view of the existing international forums.

Although all the bodies performed some form of prior consultations in order to prepare for international meetings – including with services that did not participate in the meetings – it was found that there was no clearly defined method of preparation for the meetings and for determining the standpoint of Belgium, if necessary.[184] The Committees noted that this process was rather

182 Some services and ministers responded only after several reminders. Even the Ministers of Finance and Home Affairs failed to send any response to the Committees.

183 Of course, there are forums reserved for a single player. For example, State Security found that there are two types of meetings: meetings of intelligence services governed by the basic rules of the intelligence community (i.e. the 'need to know' rule and the 'third party rule') and joint meetings with both intelligence services and other services competent for matters related to terrorism and extremism. The latter type occurs primarily within the context of the European Union.

184 In this respect, the Federal Police stated that there were few or no specific structural mechanisms for discussing the participation in the meetings and the standpoints to be taken.

informal and unstructured, so that there was no guarantee that the relevant services had been able to set forth their standpoint prior to the meetings and that a common 'Belgian standpoint' had been presented at the meetings.

The same was applicable to the dissemination of the results of the meetings: this also occurred in an informal and unstructured manner, so it was not certain whether all the relevant services had received the necessary feedback.

II.9. COMPLAINT REGARDING THE COMMUNICATION OF INFORMATION BY THE GISS TO THE FEDERAL POLICE

When a prospective professional volunteer to the Armed Forces failed to pass his basic training, he made concrete threats against the Belgian army to his colleagues. His superior notified the GISS of this. The military intelligence service conducted an investigation into this matter and came to the conclusion that there was a potential threat. Subsequently, this information was communicated to the police.

When the individual in question later presented himself as a candidate for a position with the Federal Police, he failed to pass the personality test. According to him, this was because of the information communicated by the GISS to the police. He claims to have been the victim of discrimination because of his ethnic origins.

However, the Standing Committee I came to the conclusion that the GISS had acted in accordance with its legal assignment (Article 11 of the Intelligence Services Act) and that the police, given its areas of competence, was entitled to receive this information (Article 19 of the Intelligence Services Act and 44/1 of the Police Function Act). It was clear that the information had not been passed on with the intention of providing the police an element for assessing the personality of the complainant in the context of a selection procedure. Therefore, the actions of the GISS did not constitute an infringement of the rights of the

---

Usually, attempts are made at establishing ad hoc agreements only if this appears essential. In many cases, a certain amount of harmonisation takes place within national forums, such as the Board for Intelligence and Security.

State Security stated that not just the Belgian participants, but also the services that do not participate in the meetings, meet each other and exchange information regarding their standpoints prior to the meetings. For example, the programme for the fight against terrorism and extremism with a view to the Belgian Presidency of the Justice and Home Affairs Council of the European Union (JHA) was drawn up in consultation with all the relevant bodies.

For meetings at UN or EU level, prior meetings are held within the FPS Foreign Affairs, where there is a continuous discussion regarding the position to be taken by Belgium. The FPS Justice, the FPS Home Affairs, the Federal Police, State Security, the GISS and the CUTA take part in these meetings.

individual in question and no evidence of discriminatory treatment was found by the Standing Committee I.

II.10. THE ABILITY TO ENTER PRIVATE PREMISES FOR PROTECTION ASSIGNMENTS

Protection officers of State Security entered the private garden of an apartment building in order to inspect a specific escape route. This garden was adjacent to a location where they had been assigned to protect a dignitary. The checking of these premises occurred in the presence of employees of the private security service of the location in question, but without the owners of the apartment being informed of this. Two residents questioned whether the security agents were entitled to enter their private premises at all times.[185]

The Intelligence Services Act of 30 November 1998 states that State Security agents may only enter private premises without the knowledge and consent of the owner under certain conditions.[186] But this specific or exceptional power is only applicable when performing their intelligence assignments. This option may not be used in the context of protection assignments. Protection officers of State Security do have certain powers of administrative police which are similar to those of the police services (i.e. they are armed and may resort to violence if the life or physical integrity of the person under protection is in danger), but they may not enter private premises unless they are abandoned premises.[187]

As a result of this incident, the private security service involved and the representative of the apartment's residents reached an agreement stating that the latter will be informed in advance of any inspection conducted by State Security of their premises.

II.11. REVIEW INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2011 AND REVIEW INVESTIGATIONS OPENED IN 2011

This section contains a list and brief description of all review investigations opened in 2011 and those review investigations continued during the operating year 2011 but which have not been completed as yet.

---

185 The garden of the apartment building was encumbered by an easement of passage for emergency situations and for the evacuation of the neighbouring building. This easement, however, was not related to any prior inspections of the escape route.

186 See Art. 18/2, 18/4 and 18/5 of the Intelligence Services Act.

187 Article 24 of the Intelligence Services Act.

II.11.1. INVESTIGATION WITH REGARD TO THE ACTIVITIES OF THE GISS IN AFGHANISTAN

The Belgian troops in Afghanistan are part of the International Security Assistance Force (ISAF). The major part of the Belgian troops is posted in the Afghan capital of Kabul and consists of a protection company for the international airport. In Kunduz, Belgium provides support to the provincial reconstruction teams and provides *Operational Mentoring and Liaison Teams*. In Kandahar, Belgium contributes to the military effort with F-16s.[188]

A briefing of the 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 (and possibly develop a frame of reference), the Committee decided to open an investigation into '*the role of the GISS in monitoring the situation in Afghanistan*' (free translation). This investigation included topics such as the deployed personnel, intelligence methods used, cooperation with foreign intelligence services as well as the transmission of intelligence.

The Standing Committee I intends to close this investigation in the autumn of 2012.

II.11.2. MONITORING OF A CONVICTED TERRORIST DURING AND AFTER HIS DETENTION IN BELGIUM

According to a press article from the British newspaper *The Independent*[189], a terrorist who was convicted in Belgium and who was serving his sentence in the prison of Forest, had allegedly been put under pressure by an agent of the British secret service to start working for them. This news report was extensively covered in the Belgian press. It was alleged that the man had been illegally transferred to the United Kingdom and 'imprisoned' at a secret base. Here, he was apparently interrogated and forced to cooperate.

According to his lawyer, this operation could not have taken place without the approval or knowledge of the Belgian intelligence services.

The Standing Committee I thereupon decided to open an investigation into *'the possible monitoring of a person (M.J.) by State Security and the GISS during and after his detention in Belgium*' (free translation). The results of this investigation were sent to the Monitoring Committee of the Senate and the competent ministers in the spring of 2012.

---

188 At the end of 2011, the Belgian government decided to begin with the withdrawal of Belgian troops as from 2012. The last soldiers should have left Afghanistan by 2014.

189 *The Independent*, 23 July 2010.

II.11.3. AD HOC ASSESSMENTS BY THE CUTA IN THE CONTEXT OF VISITS OF FOREIGN INDIVIDUALS

In October 2010, the Standing Committee I, together with the Standing Committee P, opened an investigation into '*the threat assessment performed by the CUTA with respect to the visit of foreign individuals to Belgium* '(free translation). The figures cited by the CUTA in its annual reports suggested that such ad hoc assessments imply a huge investment in time and resources for this service.

The final report was provided in 2011. However, the late response of the CUTA meant that the investigative actions could not be finalised. The results of the investigation are expected in 2012.

II.11.4. ADVICE ISSUED BY STATE SECURITY IN THE CONTEXT OF NATURALISATION APPLICATIONS

One of the questions that came up in the so-called Belliraj case[190] was how State Security might have intervened in the naturalisation of this person. This was an item which the members of the Monitoring Committee of the Senate returned to in detail when discussing the investigation in November 2010.

In line with this discussion, the then President of the Senate requested the Standing Committee I to open an investigation '*into the manner in which and the circumstances under which State Security investigates and handles requests for information regarding procedures for obtaining Belgian nationality*' (free translation). The results of this investigation, which includes a legal, descriptive and quantitative section, were sent to the Monitoring Committee in the spring of 2012.

II.11.5. MONITORING OF CERTAIN FOREIGN INTELLIGENCE SERVICES IN CONNECTION WITH THEIR DIASPORA IN BELGIUM

Belgium appears to have an attraction for foreign intelligence services. The presence of the European institutions and the NATO on our territories is one of the reasons for this. Moreover, foreign intelligence services show great interest in Belgian high-tech research in space programmes, arms industry and energy policy. However, some foreign intelligence services also closely monitor the activities of their own immigrant communities – i.e. their diaspora – in Belgium.

190 STANDING COMMITTEE I, *Activity Report 2009*, 30–40.

At the request of the then President of the Senate, an investigation was opened in July 2011, '*into the manner in which Belgian intelligence services monitor the possible activities developed on Belgian territories by intelligence services from major immigration countries outside the European Union*' (free translation).

During 2011, various questions were put to State Security and the GISS in this regard. The results of this investigation are expected in the course of 2012.

II.11.6. THE RIGHT TO TRADE UNION ASSISTANCE IN THE CONTEXT OF SECURITY INVESTIGATIONS

In October 2011, the Standing Committee I received a question regarding whether a trade union representative has the right to assist a soldier during an interview in the context of a security investigation. The Standing Committee I thereupon opened an investigation into this.

But the soldier in question lodged an appeal in December 2011 with the Appeal Body for security clearances, certificates and advice. In application of Article 3 of the Appeal Body Act, the Standing Committee I suspended the investigation. In the beginning of 2012, the Appeal Body issued its judgement and the investigation could be resumed.

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS

Article 35 §1, 1° of the Review Act specifies that, in its annual Activity Report, the Committee '*[must devote] particular attention to the specific and exceptional methods of data collection methods, as intended in Article 18/2 of the Intelligence Services Act of 30 November 1998 [and] to the implementation of Chapter IV/2 of the same Act*'[191] (free translation). This chapter therefore deals with the use of special intelligence methods by both intelligence services and the manner in which the Standing Committee I performs its jurisdictional role in this matter. It is a brief summary of the two half-yearly reports drawn up by the Committee on behalf of the Monitoring Committee of the Senate.[192]

III.1. SOME SPECIFIC POINTS OF ATTENTION

III.1.1. INFORMAL CONSULTATIONS WITH THE PARTIES INVOLVED

The Standing Committee I regularly consulted State Security, the GISS and the SIM Commission regarding the application of the SIM Act.

With the SIM Commission, it discussed the following items:

- flow of information and documents from the SIM Commission to the Standing Committee I;
- on-call service of the SIM Commission during holiday periods, given the absence of substitute members;

---

191 For an analysis of the special intelligence methods and how they are monitored, see: STANDING COMMITTEE I, *Activity Report 2010*, 51–63 and W. VAN LAETHEM, D. VAN DAELE en B. VANGEEBERGEN (eds.), *De Wet op de bijzondere inlichtingenmethoden*, Antwerpen, Intersentia, 2010, 299 p.

192 Art. 35 §2 and 66*bis* §2, third paragraph of the Review Act. The two reports were forwarded to the Monitoring Committee in, respectively, mid-September 2011 and early February 2012.

– delay in sending authorisations to the Committee for the use of specific methods in those cases where the SIM Commission has requested additional information from the intelligence services;
– issue regarding the use of specific methods for the identification of users of means of communication, in light of the subsidiarity requirement (see III.2.2.1 and III.3.2.6);
– method of notifying the members of the Commission in case a method is authorised after obtaining the assent of the Chairman of the SIM Commission, referred to in urgent matters.

The following points were raised with the intelligence services:

– conditions under which the Investigation Service of the Standing Committee I may obtain additional information informally from the intelligence services before the Committee is officially referred to, if at all;
– possible consequences for the operations of the two services or their response when the Committee finds that State Security and the GISS are independently using (a) special method(s) with respect to the same target.

III.1.2. 'RESULTS OBTAINED' VIA SPECIAL METHODS

Article 35 §2 of the Review Act states that '*where appropriate, the results obtained*' (free translation) must be included in the half-yearly report sent by the Committee to the Monitoring Committee. Given the complexity and sensitivity of such reports in an intelligence context, the Committee is currently developing a methodology for randomly evaluating how the intelligence services value the results they obtain. This tool should make it possible to prepare (depending on recommendations regarding the effectiveness and legitimacy of the actions of the services) useful reports regarding the use of special methods.

III.1.3. JUDGEMENT OF THE CONSTITUTIONAL COURT

The Constitutional Court delivered its judgement on 22 September 2011 with regard to two requests for the annulment of various provisions of the SIM Act.[193] Based on this, only one Article was annulled. The judgement stated that Article 2 §3 of the Intelligence Services Act, which introduces a passive notification obligation, should be adjusted with respect to two points. On the one hand, legal

[193] By the Flemish bar association (*Belgian Official Journal* 16 August 2010) and the Human Rights League (*Belgian Official Journal* 27 October 2010). An extract from the judgment was published in the Belgian Official Journal of 12 December 2011.

persons must also be notified if they are the subject of a special method. On the other hand, it must be ensured that the intelligence service involved notifies a (legal) person at its own initiative as soon as the SIM Commission deems this to be possible.

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

In 2011, for the two intelligence services, a total of 831 permissions or authorisations (referred to further as 'authorisation'[194]) were granted for the use of special intelligence methods: 764 for State Security (of which 731 were for specific and 33 for exceptional methods) and 67 for the GISS (of which 60 were for specific and 7 for exceptional methods). When interpreting these figures, two things need to be kept in mind:

- in principle, only one special method is allowed for each 'authorisation' (an observation assignment *or* a search, but not both). In only one case may this be deviated from: a single authorisation may allow an intelligence service to obtain call or localisation data and subsequently proceed to the identification of the information thus obtained (see III.2.2.1.);
- however, for each authorised method, multiple targets (such as persons, organisations, places, subjects, means of communication, etc.) may be permitted. Some authorisations may therefore have a more substantial impact than others on the workload of the intelligence services and on the privacy of citizens.

The figures for the two services are displayed separately below. While both services have the same powers, their assignments are so different that very few lessons can be drawn based on a comparison of the figures related to the two services.

For each service, three major categories have been distinguished: figures on specific methods, figures on exceptional methods and figures on threats and the interests to be defended with the help of the various methods.

194 In the Act, the French and Dutch terms for 'permission', 'authorisation' and 'decision' are sometimes used interchangeably. In the interests of the readability of this report, the term 'authorisation' shall be used for all special methods authorised by the head of service or the Minister, while the term 'decision' shall be used in the context of the jurisdictional monitoring by the Standing Committee I.

III.2.1. AUTHORISATIONS WITH REGARD TO THE GISS

III.2.1.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER
Entry into and observation of or in places accessible to the public using a technical device	7
Entry into and searching of places accessible to the public using a technical device	0
Inspection of localisation data of postal traffic and requesting the cooperation of a postal operator	0
Inspection of identification data of electronic communication, requesting the cooperation of an operator or direct access to data files	23
Inspection of call-associated data of electronic communication and requesting the cooperation of an operator	17
Inspection of localisation data of electronic communication and requesting the cooperation of an operator	13
TOTAL	60[196]

III.2.1.2. Exceptional methods

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

III.2.1.3. Interests and threats justifying the deployment of special methods

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

– intelligence task 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 (Art. 11, 1° of the Intelligence Services Act);

195 In three cases, the authorisation was related to a protected professional category, namely that of a lawyer, doctor or professional journalist.

– military security task focused on, for example, preserving the military security of defence personnel, military installations and military IT and network systems (Art. 11, 2° of the Intelligence Services Act);
– protection of military secrets (Art. 11, 3° of the Intelligence Services Act).

NATURE OF INTEREST	NUMBER
Intelligence task	38
Military security	8
Protection of secrets	19

Unlike for State Security, the Act does not lay down which threats the GISS may or must pay attention to. But despite this, in its authorisations, the service systematically mentions the threat being targeted. Such transparency is to be recommended. The figures show that, as regards the use of special methods, the fight against espionage is the first priority of the military intelligence service.

NATURE OF THREAT	NUMBER
Espionage	54
Terrorism	10
Extremism	3

III.2.2. AUTHORISATIONS WITH REGARD TO STATE SECURITY

III.2.2.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER
Entry into and observation of or in places accessible to the public using a technical device	89
Entry into and searching of places accessible to the public using a technical device	0
Inspection of localisation data of postal traffic and requesting the cooperation of a postal operator	4
Inspection of identification data of electronic communication, requesting the cooperation of an operator or direct access to data files	355
Inspection of call-associated data of electronic communication and requesting the cooperation of an operator	237
Inspection of localisation data of electronic communication and requesting the cooperation of an operator	46
TOTAL	731[197]

196 In nine cases, the authorisation was related to a protected professional category, namely that of a lawyer, doctor or professional journalist.

The above table clearly shows that the majority of the methods used by State Security are related to the (not very intrusive) identification of the subscriber or user of a telephone or mobile number. This includes 355 authorisations for identifications, where one authorisation usually includes several numbers. In fact, the 355 authorisations involved 1892 numbers. However, the actual number of identifications carried out is even higher. Since, the Standing Committee I, in consultation with the SIM Commission, has agreed to the method by which the head of service of an intelligence service may authorise both the tracing and identification of call-associated data in the same authorisation. This prevents the head of service from having to issue two consecutive and virtually identical authorisations in the same dossier. This is because both methods are strongly related to one another: call-associated details are only useful if they can be attributed to a particular individual or organisation. On the other hand, this method implies that the Committee does not automatically have an idea of the number of identifications carried out.

However, the Committee requires that the intelligence service should only authorise the identification, via an operator, of those numbers that cannot be identified via an ordinary method and which are necessary in the context of the intelligence investigation. This ensures compliance with the principles of proportionality and subsidiarity. The services have accordingly adapted their authorisations in which they want to consecutively inspect call and identification data. The Committee has randomly verified whether the services have respected this agreement.

III.2.2.2. Exceptional methods

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

This table shows that State Security, as compared to the GISS, makes a more extensive use of the option of using special intelligence methods.

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

State Security may only take action in order to safeguard the following interests:
- internal security of the State and maintenance of democratic and constitutional order;
- external security of the State and international relations;
- safeguarding of the key elements of the scientific or economic potential.

NATURE OF INTEREST	NUMBER[198]
Internal security of the State and maintenance of democratic and constitutional order	694
External security of the State and international relations	571
Safeguarding of the key elements of the scientific or economic potential	24

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 (Art. 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 leading to terrorism (Art. 3, 15° of the Intelligence Services Act).

NATURE OF THREAT	NUMBER[199]
Espionage	193
Terrorism (and radicalisation process)	371
Extremism	319
Proliferation	17
Harmful sectarian organisations	4
Interference	3
Criminal organisations	3

With regard to the use of special methods, terrorism and extremism are clearly the top priorities for State Security. It is also notable that – just as for the GISS – the threat of espionage accounts for a considerable share of the use of specific and exceptional methods.

197 Each authorisation may involve multiple interests.
198 Each authorisation may involve multiple threats.

III.3. ACTIVITIES OF THE STANDING COMMITTEE I AS A JURISDICTIONAL BODY

III.3.1. STATISTICS

The Standing Committee I may be referred to in five ways to deliver a decision regarding the legality of special intelligence methods (Art. 43/4 of the Intelligence Services Act):
- at its own initiative;
- at the request of the Privacy Commission;
- as a result of a complaint from a citizen;
- automatically, whenever the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and prohibited the exploitation of the data;
- automatically, if the competent Minister has issued an authorisation based on Article 18/10, §3 of the Intelligence Services Act.

In addition, the Committee may also be referred to in its capacity as a 'pre-judicial advisory body' (Art. 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure). When requested, the Committee gives its opinion about 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
At its own initiative	28
Privacy Commission	0
Complaint	0
Suspension by SIM Commission	9[200]
Authorisation Minister	0
Pre-judicial advisory body	0
TOTAL	37

Of a total of 831 authorisations for the use of special methods, the Committee was referred to in 37 cases.[200] Once it has been referred to, the Committee may

199 In two dossiers, the SIM Commission suspended an authorization after the Standing Committee I had already been referred to in this matter. These suspensions have not been taken into account here.

200 The Committee is always 'referred to' in connection with an 'authorization' by the head of the intelligence service.

take various kinds of (interim) decisions. However, in the first two cases, a decision is taken before the Committee is actually referred to:

- decision to declare the complaint as null and void due to a formal defect or the absence of a personal and legitimate interest (Art. 43/4, first paragraph of the Intelligence Services Act);
- decision not to take any action with regard to a complaint that is manifestly unfounded (Art. 43/4, first paragraph of the Intelligence Services Act);
- suspension of the disputed method pending a final decision (Art. 43/4, last paragraph of the Intelligence Services Act);
- request for additional information from the SIM Commission (43/5 §1, first to third paragraph of the Intelligence Services Act);
- request for additional information from the relevant intelligence service (43/5 §1, third paragraph of the Intelligence Services Act);
- investigation assignment for the Investigation Service I (Art. 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 Committee has been actually referred to and which is, therefore, obtained in a more informal way;
- hearing the members of the SIM Commission (Art. 43/5 §4, first paragraph of the Intelligence Services Act);
- hearing the head of service or the members of the relevant intelligence service (Art. 43/5 §4, first paragraph of the Intelligence Services Act);
- decision about secrets relating to an ongoing criminal investigation or judicial inquiry to which the members of the intelligence services are privy, after consultation with the competent magistrate (Art. 43/5 §4, second paragraph of the Intelligence Services Act);
- decision of the Chairman of the Standing Committee I, after having heard the head of service, in case 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 (Art. 43/5 §4, third paragraph of the Intelligence Services Act);
- discontinuation of a method if it is still in use or has been suspended by the SIM Commission and order stating that the information obtained through this method may not be exploited and must be destroyed (Art. 43/6 §1, first paragraph of the Intelligence Services Act);
- partial discontinuation of an authorised method.[201] This refers to a situation in which, for example, the use of a method is limited in time and not to the

[201] This decision is not described as such in the Intelligence Service Act.

situation in which several methods are approved in a single authorisation by a head of service and the Committee discontinues only one of them.
- total or partial lifting of the suspension and prohibition imposed by the SIM Commission (Art. 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, proportional and subsidiary by the Committee.
- no competence of the Standing Committee I;
- pending case is unfounded and no discontinuation of the method;
- advice given as a pre-judicial advisory body (Art. 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure).

NATURE OF DECISION	NUMBER	NUMBER OF FINAL DECISIONS
Invalid complaint	0	
Manifestly unfounded complaint	1	
Suspension of method	3	
Additional information from SIM Commission	4	
Additional information from the intelligence service	9	
Investigation assignment of Investigation Service	17	
Hearing of members of the SIM Commission	0	
Hearing of members of the intelligence services	1	
Decision regarding investigative secrecy	0	
Sensitive information during hearing	0	
Discontinuation of method	12	39
Partial discontinuation of method	7	
(Partial) lifting of prohibition imposed by SIM Commission	5[203]	
No competence	0	
Lawful authorisation/ No discontinuation of method/ Unfounded	15	
Pre-judicial advice	0	

202 This count includes two decisions of the Committee which were also included in the section on 'Partial discontinuation of a method' because the SIM Commission had suspended the authorizations completely after the Committee had been referred to, while this suspension had to be partially lifted.

In 2011, the Committee delivered 39 final decisions.[203, 204] It should not be forgotten that these decisions only constitute the final part of the activities of the SIM Commission and in this sense, represent only a fraction of the real effort. Since, *each* SIM authorisation by State Security and the GISS is subjected to a substantive verification based on a standardised procedure and a detailed checklist. If need be, the intelligence services are also asked additional questions before referring the case to the Committee. Therefore, the verification of the authorisations issued by the SIM Commission represents a significant portion of the Committee's time budget.

Five of the nine suspensions imposed by the SIM Commission were fully or partially lifted. Moreover, the Committee fully or partially discontinued 13 authorisations, without these having been previously suspended by the SIM Commission.

Of the 19 partial or complete discontinuations, five were related to dossiers of the GISS and 14 to State Security dossiers.

III.3.2. DECISIONS

The 39 final decisions delivered by the Standing Committee I in 2011 are briefly presented below. The summaries have been stripped of all operational information. Only those elements relevant to the legal issue have been included.

The decisions are grouped into six sections:

- legal (procedural) requirements prior to the implementation of a method;
- justification for the authorisation;
- legal (procedural) requirements during the implementation of a method;
- legality of the method in terms of the applied techniques, data collected, duration of the measure and nature of the threat;
- proportionality requirement;
- subsidiarity requirement.

Where relevant, some decisions are included under multiple sections.

---

203 The number of times the Committee is referred to and the number of final decisions are not necessarily the same. This is possible, for example, because the final decision is not delivered in the reference period within which the Committee was referred to or because one referral can result in several final decisions.

204 The Standing Committee I must deliver a final decision within one month following the day on which it was referred to in this matter (Art. 43/4 of the Intelligence Services Act). This period was respected in all dossiers.

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 as well as the assent of the SIM Commission must be presented. If such methods are used without the above-mentioned written authorisation or assent (if necessary), the Committee will, of course, have to intervene.

III.3.2.1.1. No written authorisation

The Committee found that an intelligence service had proceeded to the inspection of call-associated data of a mobile and a landline number, while the authorisation granted was solely related to the mobile number (Dossier 2011/501a). Therefore, information gathered from the 'surveillance' of the landline was nullified on the grounds of illegality, since no written authorisation from the head of service could be presented for this.

In another dossier, a head of service had granted the authorisation to trace the call-associated data of a mobile number for a period of six months (Dossier 2011/748). In implementing this authorisation, the intelligence service requested one telecom operator to provide the relevant call-associated data and all telecom operators to identify the holders of the numbers thus obtained. But this kind of identification falls under a separate method. No authorisation had been granted for this: '*That the mentioned request, insofar as it seeks to identify the subscriber or regular user of the traced numbers (call-associated data), does not fall under the scope of a (lawful) decision and is, consequently, illegal*' (free translation).

The same problem also occurred in a third dossier. The head of service of the intelligence service had granted an authorisation to proceed to the identification of '*all telephone numbers held by X*' (free translation) (Dossier 2011/830). However, the subsequent request to the operators revealed that the request was related not only to the identification of the telephone numbers in X's name, but also to the identification of the means of communication used by various other subscribers. Therefore, the method applied was not entirely covered by a written and reasoned authorisation and owing to this, the part of the method falling outside the scope of the authorisation was illegal. '*That, consequently, targets (people, places, etc.) not mentioned at all in an authorisation may not be the legitimate subject of a request for information.*' (free translation). Moreover, it appeared that, while the authorisation only mentioned the identification of all telephone numbers held by X., the request sent to the operators also asked for the identification of *all* electronic communications services used by X: *'That, here too, there is no correspondence between the authorisation (limited to telephone services) and the final request for information*' (free translation).

III.3.2.1.2. Authorisation by the acting head of service

The Standing Committee I decided to intervene in a dossier (2011/406) in which a specific method had been signed '*For the Administrator-General, absent, [name], Advisor*' (free translation). At that time, the Advisor in question had assumed the responsibility for the general management of the service.

The question was whether this was compliant with the provisions of Article 18/3 §1, second paragraph of the Intelligence Services Act, which states that a specific method may be used only after a written and reasoned authorisation from the head of service, being '*the Administrator-General of State Security or, in his absence, the acting Administrator-General*' (free translation). Through this provision, the legislator wanted to ensure that the management of the intelligence services is always notified of the use of a specific method and its implementation. Though it had been a mistake on the part of the concerned Advisor to officially sign '*for the Administrator-General*' (free translation) (since he was the acting Administrator-General at this time), the final objective of the Act had indeed been met. Moreover, it was clear that the Administrator-General was absent: hence, in the context of the SIM Act, he could justifiably delegate this authority. In addition, the Committee established that neither the Royal Decree of 14 January 1994 on the statute of the Administrator-General and Deputy Administrator-General of State Security nor the Royal Decree on State Security of 5 December 2006 make any mention of mandatory rules related to the replacement of the head of service. Hence, no illegality was found.

III.3.2.1.3. Prior notification to the SIM Commission in case of a specific method

An intelligence service was authorised to conduct camera surveillance of the entrance to private premises for a defined period of time. Since the head of service wanted to 'extend' the measure[205], he issued a new authorisation for a period beginning immediately after the previous period (Dossier 2011/667). However, the notable aspect in this case was that the SIM Commission was only notified of the 'extension' during the morning of the first day of the new period. Article 18/3 §1 of the Intelligence Services Act states that a specific method may only be used after notification of the authorisation to the SIM Commission. As a result, any surveillance of the premises from midnight (the original authorisation for surveillance of the premises expired at that time) until the notification of the new authorisation was not covered by a valid mandate. Any pictures taken during that short period therefore needed to be destroyed.

---

[205] Unlike for exceptional methods, the Act does not strictly offer the possibility of 'extending' a specific method. Upon expiry, a new method must be authorized.

III.3.2.1.4. Absence of an assent

An intelligence service wanted to intercept certain communications (Art. 18/17 §1 of the Intelligence Services Act) and enter private premises to install monitoring equipment (Art. 18/17 §2 of the Intelligence Services Act) (Dossier 2011/300). Since this involved an exceptional method, the assent of the SIM Commission was required. However, in the opinion of the Standing Committee I, the advice concerned the powers defined in Article 18/17 §2 of the Intelligence Services Act (and not to the actual monitoring). Also, based on the period during which the exceptional method could be used according to the SIM Commission, the Committee felt that the concurrent advice was only related to the installation and removal of the monitoring equipment, and not to the actual interception.

Therefore, the Standing Committee I decided to declare as illegal the '*authorisation for the implementation of the method as intended in Art. 8/17 §1 of the Intelligence Services Act*' (free translation).

III.3.2.1.5. (No) assent in the case of an alleged journalist?

The intelligence service in question wanted to find out the identity of an anonymous blogger who was spreading extremist opinions on his website (Dossier 2011/204). This individual was, moreover, presenting himself as a journalist. The question was whether the intelligence service needed the assent of the SIM Commission for this method without having more details about the alleged capacity of the blogger. Since, Article 18/3 §1, third paragraph of the Intelligence Services Act states the following: '*The specific methods may only be used with respect to a lawyer, doctor or journalist or the means of communication used by them for professional purposes, provided that the intelligence and security service has prior, serious evidence that the lawyer, doctor or journalist personally and actively participates or has participated in the origin or development of the potential threat and after the Commission, pursuant to Article 18/10, has given its assent on a motion of the head of service.*' (free translation).

Just like the SIM Commission, the Committee was of the opinion that the specific method could be used in this case without prior assent in order to verify the identity of the blogger and to subsequently check whether the person was actually a journalist within the meaning of the Act. If this verification confirmed his status as a journalist, the provisions contained in Articles 18/2 §3 and 18/3 §1, third paragraph of the Intelligence Services Act have to be observed from that moment on.

A similar question was raised in another dossier. An intelligence service wished to find out the identity of the holders of mobile numbers who were suspected of intelligence activities, but who were possibly operating under the cover of being journalists (Dossier 2011/264). Here too, the Committee was of

the opinion that the specific method could be used to verify the user's identity and whether he was acting in the capacity of a journalist.

III.3.2.1.6. Assent and scope of the concept of 'IT system'

A head of service wanted to authorise the identification of the PUK codes of certain SIM card numbers owned by an individual who had drawn the attention of his service (Dossier 2011/721). He considered this to be a specific method, i.e. '*identifying the subscriber or regular user of an electronic communications service or of the means of electronic communication used*' (free translation) as described in Article 18/7 of the Intelligence Services Act. Under the scope of the same authorisation, the PUK codes obtained would be used to create a new PIN code, in order to subsequently '*make it possible to read the cards through additional SIM methods*' (free translation).

The Standing Committee I suspended the method in question and investigated its legitimacy. It found that the method did not, in reality, lead to the identification of the subscriber or user of the SIM cards in question since he had been known in advance. The final objective of the method had been to change the PIN code with the help of the PUK code (to be retrieved) of the SIM card.

A SIM card contains a *S(ubscriber) I(dentity of identification) M(odule)*, an integrated circuit on which data is programmed and stored in a secure manner. Such a SIM card should be regarded as an 'IT system' within the meaning of Article 18/16 of the Intelligence Services Act. This is because the legislator intended to interpret this term in the same way as in the Computer Crime Act of 28 November 2000.[206] During the creation of the Computer Crime Act, IT systems were described as '*all systems used for storing, processing or transferring data. This refers not only to computers, cash cards, etc., but also networks and parts thereof, as well as telecommunications systems or components thereof that rely on IT*'[207] (free translation). Therefore, obtaining and using the PUK code to change and enter the PIN code constitutes an exceptional method as defined in Article 18/16 §1, 1° and 2° of the Intelligence Services Act ('*to 1° gain access to an IT system and 2° neutralise any security features of this system, whether or not with the help of technical resources, false signals, false keys or false capacities*') (free translation). Since the legal requirements for the authorisation of an exceptional method had not been respected, the Committee decided to discontinue the method.

206 *Parl. Doc.* Senate 2008–2009, 4–1053/1, 54.
207 *Parl. Doc.* House of Representatives 1999–2000, no 50–213/1 and no. 50–214/1, 12.

III.3.2.1.7. Assent in case of an emergency

As part of an ongoing operation, the head of service of the relevant intelligence service authorised a search of private premises (Dossier 2011/331). For this, the procedure in case of emergencies, as defined in Article 18/10 §4 of the Intelligence Services Act, was applied. This provision allows the head of service to authorise the exceptional method in writing after obtaining the assent of the Chairman of the SIM Commission (and therefore, not of the entire Commission). The issue revolved around this assent. The written authorisation of the head of service only mentioned that this assent had been obtained; however, this was only a verbal assent. Neither was there any written draft authorisation, nor any written (confirmation of the actual content of the verbal) assent available.

Pursuant to Article 18/10 §1 of the Intelligence Services Act, making an authorisation dependent on the assent of the SIM Commission implies an investigation of compliance with the legal provisions for the use of exceptional methods, the principles of proportionality and subsidiarity as well as a verification of the requirements defined in Article 18/10 §2 of the Intelligence Services Act. There was no verifiable written evidence of such an investigation and evident proof of conformity, apart from the mere mention in the authorisation of the presence of an assent. The Committee considered this to be insufficient. Since, such an approach does not allow the Standing Committee I to verify the legality of the method in all its aspects (especially *in casu*, the verification of the conformity between the (draft) authorisation on the one hand and, on the other hand, the assent given). For the reason alone that this undermines the control by the Standing Committee I, this approach could not be regarded as legal.

Moreover, the Committee noted that the current legal and regulatory provisions neither explicitly nor implicitly refer to any verbal draft authorisation from the head of service or any verbal assent from the SIM Commission. Furthermore, Article 43/3 of the Intelligence Services Act states that *all* decisions, opinions and authorisations must immediately be brought to the notice of the Standing Committee I, *ter fine* the verification of the legitimacy. This means that these decisions, opinions and authorisations should be in the form of a document.

The Committee derived an additional argument based on the fact that the legislator has only allowed a very limited exception to the written nature of an authorisation, i.e. for the request made by the intelligence officer to apply the specific methods referred to in Articles 18/6 §2, 18/7 §2 and 18/8 §2 of the Intelligence Services Act in extremely urgent cases. However, the Act states that even such a request must be confirmed in writing as soon as possible. The Committee also felt that it could not reasonably be assumed that, for the more intrusive exceptional methods, the legislator would have wanted to implicitly

deviate from the written nature of an authorisation in one or more of the various stages.

This is the reason why the Standing Committee I decided that the verbal nature of the initial request and the assent were not in keeping with the letter and the spirit of the Act.

III.3.2.2. Justification for the authorisation

III.3.2.2.1. Insufficient justification

In six dossiers, the SIM Commission decided to suspend a method because the authorisation of the head of service was not sufficiently reasoned in order to adequately assess the legality, proportionality and subsidiarity aspects. In the first five cases, the Standing Committee I – which is officially referred to when the SIM Commission suspends a method – endorsed this decision and ordered the discontinuation of the method. In the sixth case, the suspension was lifted because the relevant intelligence service provided additional information after the (correct) decision of the SIM Commission. In a seventh dossier, in which the justification of the authorisation was under discussion, the Committee had decided to intervene at its own initiative.

In the first dossier (2011/84), an authorisation to proceed to the identification of the subscriber or user of a mobile number was suspended by the SIM Commission because the authorisation of the head of service '*contains only a brief description of the factual elements justifying the authorisation and therefore, prevents the SIM Commission from proceeding to a verification of the principles of subsidiarity and proportionality*' (free translation). The Committee decided that the authorisation did not reveal any link between the monitored mobile phone number and the threat: '*The authorisation provides no proof whatsoever of its legality. In addition, such wording does not, in any way, allow to assess whether the principles of proportionality and subsidiarity have been respected*' (free translation).

When a mobile phone belonging to a Belgian Member of Parliament was stolen or misplaced abroad, an intelligence service wanted to locate the device by using a specific method (Dossier 2011/192). Here, the potential threat was referred to as 'interference'. In this case, the SIM Commission suspended the method because '*the authorisation did not contain any description, not even a brief one, of the factual elements justifying the authorisation*' (free translation). The Committee reached the same conclusion: the authorisation '*does not justify* in concreto *the source of the potential threat of interference and does not contain any description, not even a brief one, of the factual elements justifying the authorisation*' (free translation).

A third authorisation was suspended because it '*does not allow to sufficiently determine whether the principle of subsidiarity has been respected* in concreto *and*

because the link with the internal security of the state raised therein is not a convincing one' (free translation) (Dossier 2011/307). The Committee added the following reason to this: '*Where an authorisation, as* in casu*, does not indicate any real or at least any reasonably plausible link between the target of a method and a potential threat, as defined in Art. 18/1 of the Intelligence Services Act, but is based on allusions, is poorly reasoned and therefore, is not adequately justified from the legal perspective. Considering that this does not allow an adequate assessment of the principles of proportionality and subsidiarity.*' (free translation)

In a fourth dossier (2011/355), the intelligence service wished to proceed, at the request of a foreign correspondent, to the identification of the user of a Belgian telephone number that had appeared in a terrorism dossier. The authorisation was suspended because it was not sufficiently clear on certain points: '*the interest to be defended is not sufficiently defined; the identity of the foreign service is also insufficiently defined; there is no information about the ongoing terrorism investigation; the principles of proportionality and subsidiarity are not sufficiently justified*' (free translation). The Committee also found too few elements in the authorisation to be able to assess the legality, proportionality and subsidiarity *in concreto*.

In a fifth dossier (2011/442) – in which the intelligence service wanted to identify the users of two mobile numbers – the SIM Commission again found '*no description, not even a brief one, of the factual elements justifying this authorization*' (free translation). The Committee reached the same conclusion: conformity with the principles of proportionality and subsidiarity could not be verified.

In the last dossier suspended by the SIM Commission, the head of service wanted to authorise an observation assignment to be conducted using a technical device (Dossier 2011/724). However, the Commission decided that the authorisation '*as it was drafted, and particularly since the degree of seriousness of the potential threat described in it, is not sufficiently detailed and justified*' (free translation). The Standing Committee I could only agree with the rationale provided by the SIM Commission at the time when it took its decision. However, additional verbal and written information revealed that '*based on documented elements, the target poses a genuine threat to one of the interests referred to in Art. 7 of the Intelligence Services Act*' and that '*the method which has been decided on is in proportion to the seriousness of the above-mentioned threat and meets the requirements of proportionality and subsidiarity*' (free translations). However the Committee stated that '*it would have been appropriate, however, that* ab initio*, more detailed mention had been made in the decision itself of the elements – which were actually available – that were reasonably required for being able to adequately assess the threat and the proportionality and subsidiarity. That a decision to use a method must be adequately self-supporting in this aspect, under*

penalty of failing to meet the obligation to provide justification, consequently leading to a loss of time and resources' (free translation).

Finally, the intelligence service wanted to obtain the call-associated data from mobile phone numbers of three separate persons, as well as the e-mail addresses of one of them (Dossier 2011/522). The authorisation was sufficiently justified with respect to one of the mobile numbers and the e-mail addresses linked to this. But this was not the case with regard to the mobile numbers of the other two persons. Hence, the authorisation was unclear with regard to the threat that should have justified the method, to the extent that it raised questions regarding the competence of the relevant intelligence service. Likewise, no link could be established between the user of the first mobile number and the users of the other two numbers. Based on the initial information, the Standing Committee I could not verify the legality. However, the intelligence service in question sent additional documentation proving that the legal conditions that determine the competence and the threat had indeed been met. Therefore, the Committee decided that the method was legal but again noted that '*it would have been appropriate, however, for the authorisation itself to have mentioned* ab initio*, those elements demonstrating* in concreto *the competence and the threat with regard to each of the means of electronic communication included under the method*' (free translation).

III.3.2.2.2. Contradiction in the justification

According to the written authorisation of the head of service, the relevant intelligence service wished to proceed to the identification of the user of a telephone number (Dossier 2011/72). This method is described in Article 18/7 §1, 1° of the Intelligence Services Act ('*identifying the subscriber or regular user of an electronic communications service or of the means of electronic communication used*'). This same authorisation showed, however, that the intention was to identify the holder of an anonymous telephone number based on communications via this number. In reality, the service intended to '*trace the call-associated data of the means of electronic communication from which or to which calls are being or have been sent*' (Art. 18/8 §1, 1° of the Intelligence Services Act).

The Committee decided that the reasons cited in the authorisation of the head of service must support the use of the chosen method. Given the internal contradiction in the authorisation, it was not properly reasoned and as a result, the Committee recommended that the method be discontinued.

III.3.2.3. Legal (procedural) requirements during the implementation of a method

Once a method has been properly authorised and if necessary, brought to the notice of the SIM Commission, it may be implemented. But sometimes, this implementation must take into account certain special rules.

III.3.2.3.1. Emergency procedure when requesting information from an operator

Article 18/8 §2 of the Intelligence Services Act states that, in case of very urgent and adequately justified emergencies, the intelligence officer may verbally request an operator to immediately supply the required call-associated data, provided he has the prior verbal approval of the head of service (Dossier 2011/227). As required, the head of service subsequently confirmed this verbal approval in writing. However, this confirmation did not make it clear which intelligence officer had actually made the request; it gave no indication of the date and time when the operator had been requested for the information and did not indicate when the verbal consent of the head of service had been given. Neither could this information be found in any other document initially in the possession of the Committee, so it was impossible to verify the legality of the method.

But, during the procedure, the intelligence service in question provided additional documentation proving that all the legal conditions had been met. Therefore, the Standing Committee I concluded that the method was in accordance with the provisions of the Act. Nevertheless, the Committee emphasised the fact that the elements demonstrating *in concreto* that the statutory formalities have been fulfilled, should be included *ab initio* in the written authorisation.

III.3.2.3.2. Prior notice to the Chairman of the Association of Professional Journalists

Since the relevant service wanted to retrieve call-associated data of a means of communication used by a professional journalist, the service requested and obtained the assent of the SIM Commission (Dossier 2011/193). However, Article 18/2 §3 of the Intelligence Services Act states that '*this method may not be implemented without prior notification of this to […] the Chairman […] of the Association of Professional Journalists by the Chairman of the Commission*' (free translation). The assent of the SIM Commission did not clearly show whether this formality had been observed. Inquiries revealed that the SIM Commission had not informed the Chairman. This was done only later, after the Standing Committee I had made a remark on this matter.

Since Article 18/2 §3 of the Intelligence Services Act does not either specify the form of this notification or what is meant by '*the necessary information*', the Committee decided that '*the confirmation from the Chairman of the SIM Commission that prior notification has taken place, along with the clarification of the date and time of this prior notification and the statement that 'the necessary information' had been provided to the Chairman of the Association of Professional Journalists, are considered sufficient in the light of the statutory requirements*' (free translation).

The notification of the Chairman in question is an essential procedural requirement. Therefore, the Committee concluded that the possible implementation of the method, before the Chairman had been notified, was illegal. Any intelligence already collected had to be destroyed, although the information obtained after the notification could be exploited.

In a second, almost similar case (Dossier 2011/257), the assent of the SIM Commission did not show that the Chairman of the Association of Professional Journalists had been notified. Therefore, the Standing Committee I asked the SIM Commission for further explanation. Since the SIM Commission reported that the Chairman had received '*the necessary information*' at a certain point, the Committee decided that the implementation of the specific method was legal from that time onwards.

The notification issue also came up for discussion in two more cases (Dossiers 2011/761 and 2011/762): a head of service had granted authorisation to monitor the mobile phones of foreign journalists who were recognised in Belgium as professional journalists. In its assent, the SIM Commission specified that these specific methods could only be implemented after they had been notified to the Chairman of the Association of Professional Journalists. These notifications did not, however, take place immediately. The Standing Committee I checked certain aspects and came to the following decision: '*Since it is established that the [intelligence service] has implemented a specific method with respect to a professional journalist before the Chairman of the SIM Commission had notified the Chairman of the Association of Professional Journalists*' (free translation). Therefore, the information collected prior to the notification had to be destroyed.

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

Naturally, the intelligence services are not free to apply any method or technique whatsoever: these must be in accordance with the Act, are sometimes bound by time limits, may not be applied for any type of threat, may not be used outside Belgium, etc. These limits were specified by the Standing Committee I in some of its decisions.

III.3.2.4.1. Retroactive retrieval of bank details

The relevant intelligence service wanted to obtain various banking-related information both for the past and next six months (Dossier 2011/304).

This exceptional method was based on Article 18/15 of the Intelligence Services Act, which allows the intelligence services to request information on banking transactions '*carried out within a certain period of time*', without any maximum period being defined for this in the Act. However, Article 18/10 §1, second paragraph of the Intelligence Services Act states that '*the period during which the exceptional method for collecting data is used may not exceed two months*'.

The Standing Committee I examined the scope of these two provisions.

With regard to the real time retrieval of (future) bank data, the Committee stated that this could only be done for a period of maximum two months from the time of the authorisation. However, the SIM Act allows this period to be extended, subject to an evaluation.

With respect to the retroactive retrieval of bank data, the Committee came to the conclusion that no time limit had been indicated either in the Act or in the preparatory documents and "*that the period is therefore (only) limited by the proportionality principle*" (see III.3.2.5.1.).

This basic decision has subsequently been confirmed several times (Dossier 2011/378, 2011/435 and 2011/436).

III.3.2.4.2. No indication of the duration of a method

In two separate dossiers, an intelligence service wanted to inspect, via a telecom operator, the call-associated data of a particular individual (Dossiers 2011/493 and 2011/494). The authorisations indicated the period within which the request should be made to the operator, but not the period for which the call-associated data was requested. However, the investigation by the Standing Committee I showed that the legality of the method had been ensured.

III.3.2.4.3. Does the authorisation fall within the context of legal threats?

An intelligence service wanted to find out – retroactively and for a short period – which numbers had called a specific mobile phone, in order to then identify the various subscribers and holders (Dossier 2011/609). What was notable about this authorisation was that the mobile phone belonged to an intelligence officer of the relevant intelligence service and that he had granted his permission for this matter. The officer had been the victim of an incident and wanted a definitive answer about any, though not very probable, link between this incident and the dossiers handled by the officer. '*However, one cannot exclude the fact that the officer and the service could have been the*

victims of an act of intimidation by an organisation being monitored by the officer in the context of the tasks entrusted to him' (free translation), according to the relevant service. The Standing Committee I investigated whether the objective of the method actually fell within the scope of the legal task of the service as defined in the Act of 30 November 1998. The Committee presented the following argument: '*Considering that this shows that the objective of the intended specific method is, in the first place, to ensure that the safety of an intelligence officer was not compromised in the performance of one of his tasks; that such objective does not, in itself, fall under the scope of the tasks defined in the Intelligence Services Act; considering, however, that by wanting to verify whether one of its agents had been the victim of an act of intimidation, the service is also investigating evidence of any activity that might threaten the internal security of the country*' (free translation).

III.3.2.4.4. Scope of the concept of 'post'

An intelligence service wished to carry out the inspection, over a period of two months, of the post and mailbox identification data of sender(s) and recipient(s) of post packages, whether or not entrusted to postal operators (Dossier 2011/659). Article 3, 13° of the Intelligence Services Act describes '*post*' as '*postal matter as defined in Article 131, 6°, 7° and 11°, of the Act of 21 March 1991 on the reform of certain economic public sector companies*' (free translation). However, Article 131 of the Act of 21 March 1991 was amended after the implementation of the SIM Act of 4 February 2010. In Article 5 of the Act of 13 December 2010 (*Belgian Official Journal* 31 December 2010), both the sequence as well as the definition of various terms were amended. However, the Standing Committee I decided that the amendments are not applicable with respect to the contents of the term 'post' as it has been defined in the SIM Act of 4 February 2010. For this, the definitions in Article 131, 6°, 7° and 11° of the Act of 21 March 1991 remain applicable, just as they were at the time of the implementation of the SIM Act of 4 February 2010.

III.3.2.4.5. Identification of illegally obtained call-associated data

As stated above (see III.3.2.1.1), the Committee concluded that an intelligence service had proceeded to inspect the call-associated data of a mobile phone as well as a landline number, while the authorisation was only related to the mobile number. The 'surveillance' of the landline was therefore nullified, followed by a ban on using the information obtained. Hence, the relevant head of service should not have granted an authorisation for the identification of the call-associated data of the landline. However, the identification of the call-associated data of the mobile phone was allowed (Dossier 2011/501b).

III.3.2.5. Proportionality requirement

The Committee has expressed its opinion several times regarding whether or not an authorised method was in proportion to the seriousness of the threat.

III.3.2.5.1. Retroactive retrieval of bank details

As stated above, the Committee approved the retroactive request for bank data for a period of more than two months, provided that the period is proportional to the seriousness of the threat. The Committee has expressed its opinion on this issue in four separate dossiers, all of which were related to 'espionage'. In general, the Committee stated that '*verifying conformity with the principles of proportionality and subsidiarity requires, however, that the duration of the past period, related to the collection of bank data, is reasoned by the intelligence service in a manner such that the Standing Committee I is able to assess whether this period is justified in light of the seriousness of the threat; such an assessment should be performed for each dossier depending on the special circumstances justifying the implementation of the exceptional method*' (free translation).

Information was requested for a period of six months (Dossier 2011/403), eight months (Dossier 2011/378), more than five years (Dossier 2011/436) and more than 15 years (Dossier 2011/435). In addition, the Committee concluded that the reasons provided by the intelligence service became more detailed and accurate as the duration of the requested period increased. It was only in the first case that the choice of the period was not reasoned. However, the Committee decided that the necessary task of mapping the financial transactions and contacts of the account holders being investigated, with a view to exposing their network, required a sufficiently long and sustained effort. *In casu*, the period of half a year seemed acceptable.

III.3.2.5.2. Monitoring of as yet unknown numbers

The relevant service wanted to tap all the known telephonic devices owned by a target (Dossier 2011/322). In addition, it also wanted to grant this authorisation for '*numbers which are not yet known and, a fortiori, not yet identified and which would come to light in the context of the implementation of another specific method*' (free translation), but which were being used by the same target.

The Committee reviewed the authorisation for yet unknown numbers from the point of view of proportionality. It concluded that the intelligence service had formulated its reason for using this method in a very precise manner. From this it appeared that even the emergency procedure provided in the Act could not provide any solution for this exceptional case. For this reason, it decided that the method was legal.

III.3.2.5.3. Duration of the observation of private premises

The intelligence service wanted to proceed to the observation of a private place for a period of two months (Dossier 2011/434). The meeting of a group, which had drawn its attention, was expected to be held at these premises. But naturally, the duration of this meeting was limited in time: '*Considering, therefore, that an observation period of two months exceeds the period during which the event to be watched will take place*' (free translation), the measure was not proportional, as a result of which the method was partially declared null and void.

III.3.2.5.4. Inspection of call-associated data of an unknown number

The SIM Commission had suspended the inspection of call-associated data of a mobile phone and the subsequent identification of the holders in question (Dossier 2011/474). The reason was that though, at the time of authorising the specific method, the identity of the holder of the mobile phone was known, his number was still unknown. This number could only be identified after analysis of the results of two other specific methods. The SIM Commission decided that such an authorisation of the relevant intelligence service did not enable it to verify whether the requirement of proportionality and in particular, that of subsidiarity had been met. However, the Standing Committee I decided that, in this case, it was not required to know the number of the mobile phone in advance in order to assess the proportionality '*because the identity of the holder (i.e. the target) and the circumstances justifying the use of this method are known*' (free translation).

III.3.2.6. Subsidiarity requirement

Four decisions were related to the question of whether the objective aimed for in a method could also be achieved in a less invasive manner.

As already mentioned above, an intelligence service wanted to use a specific method to trace the misplaced mobile phone of a Belgian Member of Parliament. In the opinion of the Committee, not only was the authorisation insufficiently reasoned (see III.3.2.2.1) but the requirement of subsidiarity was also not satisfied: the objective, i.e. protecting the data on the mobile phone, could also have been achieved by a simple intervention of the operator and therefore, without the use of a specific method.

In the second case, which has also been discussed above (see III.3.2.5.1), the intelligence service in question wanted to check bank data relating to a very long period (more than 15 years). The targets were suspected of conducting espionage activities at home and abroad. Since, *in casu*, the only possibility of identifying the network and *modus operandi* of these persons was by investigating their

bank accounts from the time of their stay in Belgium, the subsidiarity requirement had been satisfied in this case.

In the third dossier, the relevant intelligence service wished to proceed to the inspection of call-associated data from and to a fax machine used by a research centre (Dossier 2011/484). The aim was to determine whether this centre had been invited to participate in an international conference on high technology in a country that is being monitored in the context of the fight against proliferation. The intelligence service stated that it was impossible to gain confirmation within the short term, using only ordinary methods, of whether the centre had actually received an invitation. Consequently, the intelligence service decided that the use of this specific method was essential. Although the Standing Committee I decided that the intelligence service had not acted outside its legal mandate (since *in casu* this concerned the fight against proliferation), it nevertheless concluded that the use of an ordinary method '*does not seem insurmountable in this case*' (free translation). This was also subsequently proved by the facts: since the specific method turned out to inconclusive, the intelligence service addressed its question directly to the centre. Taking into account the fact that the research centre is not a '*target*' of the intelligence service, but rather a possible victim of approaches from certain countries, the Committee decided that the subsidiarity principle had not been observed.

In a recent dossier, the head of service of the intelligence service had granted an authorisation to, in addition to the tracing of communication data, immediately proceed to the identification of certain phone numbers (Dossier 2011/830 – also see III.3.2.1.1). However, the SIM Commission had found that it could itself identify some of the numbers by dialling 1207 (especially certain landline telephone numbers). Hence, the requirement of subsidiarity had not been met. The Standing Committee I endorsed the view of the SIM Commission, but specified that the lack of subsidiarity of the authorisation was only applicable to the landline telephone numbers and not to the mobile numbers.

III.4. CONCLUSIONS

With regard to the first year of the SIM Act being fully operational, the Standing Committee I formulated the following general conclusions:

– the new monitoring task assigned to the Committee requires a significant investment of time and resources, but it clearly adds value in two areas. First, the Committee contributes to the legitimacy of the activities of State Security and the GISS and thus to the protection of the fundamental rights and freedoms. On the other hand, the monitoring by the SIM Commission provides a more complete picture of the operations of the intelligence services, which certainly benefits the general review task of the Committee;

- State Security seems to be applying the new opportunities for deploying special intelligence methods in a balanced manner. In conformity with the Act, it uses exceptional methods, which are highly intrusive, only 'in exceptional cases'. The service is also taking appropriate care when writing the authorisations (proper justification and contextualisation), although this entails a substantial administrative workload;
- however, the same conclusions cannot be drawn as yet regarding the GISS. Despite the limited number of authorisations, they are not uniformly accurate, although the service is making efforts to remedy this. In future, the Standing Committee I will pay particular attention to this finding;
- at present, it is not yet possible to draw up useful reports regarding the 'results obtained' through special methods;
- the Act does not provide any clear, uniform and feasible framework for the use of special methods in emergency situations (see III.1.1, III.2.1.1, III.3.2.1.7 and III.3.2.3.1).

CHAPTER IX
RECOMMENDATIONS

Based on the investigations concluded in 2011, the Standing Committee I has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred to individuals by the Constitution and the law (IX.1), the coordination and efficiency of the intelligence services, the 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 WITH REGARD TO THE PROTECTION OF THE RIGHTS CONFERRED TO INDIVIDUALS BY THE CONSTITUTION AND THE LAW

IX.1.1. DESTRUCTION AND ARCHIVING OF DOCUMENTS OF THE INTELLIGENCE SERVICES AND AUTOMATIC DECLASSIFICATION[208]

The decision regarding whether or not to destroy and/or archive documents of the intelligence services is closely related to '*the rights conferred on individuals by the Constitution and the law*' (free translation). This issue is governed by a number of legal provisions. The Standing Committee I came to the conclusion that the various interests at stake are perfectly reconcilable provided that the distinction between the so-called 'living' and 'dead' archives is taken into account. However, the Committee advocates a system that provides for classifications to automatically expire after a certain period – for example, 30 years for documents classified as 'secret' and 50 years for 'top secret' documents – unless they are explicitly renewed. This requires an amendment to the Classification Act.

[208] See Chapter V.1. Legislation on archiving and destruction of State Security and GISS data.

IX.1.2. RECOMMENDATION IN THE CONTEXT OF THE INTERCEPTION OF FOREIGN COMMUNICATIONS

The communication interception plan of the GISS may only target organisations and institutions, not phenomena. This is clearly stated in Article 44*bis* of the Intelligence Services Act.

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

IX.2.1. RECOMMENDATIONS WITH REGARD TO THE AUDIT OF THE GISS

In the context of the audit of the GISS, the Standing Committee I has formulated numerous recommendations regarding the organisational conditions required for a proper deployment of resources (IX.2.1.1), staff management (IX.2.1.2), information flows and ICT (IX.2.1.3) and finally, risk management (IX.2.1.4). A distinction has been made between 'recommendations for change' (i.e. recommendations that are essential for the proper functioning of the GISS and which imply a major change in the current method of working or for the organisation) and 'recommendations for improvement' (these concern more detailed subjects, where the methodology does not need to be fundamentally changed but rather refined and improved). Both forms of recommendations are complementary to one another and are described below in brief.

IX.2.1.1. Recommendations regarding organisational conditions required for a proper deployment of resources

- The Personnel & Organisation function (P&O) within the GISS must urgently be reinforced. This reinforcement is a recommendation for change and is, therefore, a *conditio sine qua non* for successfully implementing other recommendations;
- the Committee recommends that a recurrent process be initiated for defining clear and SMART objectives, in terms of products to be delivered and Service Level Agreements (SLA);
- the kind of cooperation between and within divisions, i.e. one which is opportune and necessary for achieving these objectives, must be defined. The

proposed products and SLA must, moreover, be checked with internal and external users and 'customers';
- in determining the products and the SLA, the necessary staff investments, in terms of time spent and competencies, must also be assessed;
- the management of competences within the GISS and the coordination of tasks, positions and competencies require a more professional approach;
- the Standing Committee I is of the opinion that creativity is a valuable asset for an intelligence service and must be encouraged;[209]
- for each objective, a schedule, the stakeholders involved and the method of monitoring progress must be defined. This is a recommendation for change;
- all data collection plans must specify the information required for delivering the products and who can supply this information. For this purpose, an information manager should be appointed and automated searches within the files must be facilitated;
- each division should regularly inform both its own staff members as well as those from other divisions regarding 'who' has 'which' information and 'what' can be made available to them;
- a feedback mechanism should be provided for all delivered products. Moreover, internal and external customers should be systematically interviewed on this matter, so that they have a better understanding of their needs and of what they can expect from the GISS;
- the GISS and the Directorate-General *Material Resources* of the Armed Forces must continually try, each within their budgetary constraints, to improve the resources and working conditions. Here, the focus should be on ICT resources, without compromising any security aspects (security of documents, infrastructure and persons).

IX.2.1.2. Recommendations regarding staff management at the GISS

- The Standing Committee I recommends that clear job descriptions be drawn up;
- the training process (life-long learning) should be modified. The current and required competencies should be identified, a training plan prepared and the internal and external training programmes inventoried;[210]

209 For example, via improvement circles or an 'intrapreneurship' (this is an entrepreneurship within the boundaries of the organisation).

210 With regard to the specific case of the certified training for statutory civilian personnel falling under the 'Camu' statute (Belgian statute applicable to federal officials), the DG HR and the FPS Personnel & Organisation must be consulted to examine whether it is possible to create 'positions' which are closely aligned to the intelligence and analysis activities and/or to develop targeted certified trainings.

- the Standing Committee I is of the opinion that creating an 'intelligence wing'[211] can (partially) help solve a number of the identified problems and bring about a genuine change;
- there is a need to resolve the many financial and administrative differences that exist between the various groups of staff within the GISS and between the staff of the GISS and other services in the intelligence sector (State Security and the CUTA). Since, these differences are not conducive to an effective human resource management;
- particular attention should be paid to the coaching, guidance and support of staff members of the GISS, taking into account their specific situation;
- in the context of the (reinforced) P&O function, the Standing Committee I recommends that a cell be set up to assist civilian personnel with the problems inherent to their statute and situation;
- the evaluation of the staff members of the GISS is currently based on a regulatory framework that goes beyond the scope of this service. The P&O function should help ensure that the evaluations are properly conducted and supervised. In addition, for each objective and deliverable, the method of evaluation should be defined;
- the Standing Committee I recommends that the inequalities in the statute of staff members within the GISS be addressed. For this, a 'functional logic' rather than a 'group logic' should be used. The analysis function deserves top priority in this regard. Since the biggest differences are with regard to this function, this can soon create a risk of discontinuity;
- the Committee recommends that a function be created within the GISS whose main task will be 'managing internal communication'.

IX.2.1.3. Recommendations regarding information flows and ICT

- The Standing Committee I is of the opinion that the new *Request for Information (RFI)* system will (greatly) improve the handling, follow-up and processing of requests for information. The Committee recommends that the GISS allow for a trial period before starting investigating whether there is an additional need for a reorganisation. In the meantime, the GISS can concentrate on the technical aspect of the RFI management system, without being immediately faced with organisational issues;
- the Committee recommends that the process of integrating the data collection and databases, which has been already initiated, be continued and if possible, sped up;

[211] Naturally, a question arises regarding the components to be combined in such an intelligence division. It was outside the scope of the audit to formulate a definitive answer to this question. This requires a separate study.

– in order to manage the large volume of data and documentation, the GISS must take a number of initiatives. Firstly, it must be determined what information is needed for achieving the objectives and the deliverables. In addition, an effective cooperation should be ensured between the data collection departments and the analysis offices. Finally, investments should be made to provide the absolutely necessary ICT and human resources;
– in general, the Committee recommends that sufficient resources should be invested in ICT technology, even more promptly than provided for in the investment plans.

IX.2.1.4. Recommendations regarding risk management

– the Committee recommends that actions be taken to mitigate the risks of discontinuity in the performance of a function and the consequent loss of knowledge. More specifically, the human resource management process should take into consideration future requirements, the creation of an 'intelligence wing' (reducing the loss of knowledge and allowing for a smoother replacement of staff members) should be considered and once again, investments must be made in ICT;
– it is recommended that explicit attention is paid to knowledge management within the GISS. Clear instructions should be developed to inventory the existing knowledge, assess its relevance and take measures to save, store and disseminate this knowledge. It is recommended that a knowledge manager be appointed within each division to support the knowledge management process;
– the Standing Committee I feels that the risk of 'pragmatic prioritisation'[212] is limited, but vigilance is nevertheless advised. Effective recruitment and a well-developed job description system can help curtail this risk;
– the Standing Committee I recommends that the GISS devote efforts to developing a risk management process.

IX.2.2. RECOMMENDATIONS REGARDING THE SIM ACT[213]

IX.2.2.1. Emergency procedure for specific and exceptional methods

For all specific and exceptional methods, there should be an emergency procedure which, on the one hand, allows the services to respond immediately to

212 For this, top priority should be given to matters that are well managed; therefore, areas of weakness receive less attention based on pragmatic reasons.
213 These recommendations originate from findings in the context of the jurisdictional control by the Standing Committee I of the special intelligence methods (see Chapter III).

acute threats and on the other hand, makes it possible to carry out a thorough control.

IX.2.2.2. Appointment of substitute members to the SIM Commission

Substitute members for the SIM Commission should be appointed as soon as possible. This is crucial for guaranteeing the continuity of the administrative monitoring of special intelligence methods.

IX.2.2.3. Identification of users of means of communication as a specific method

Regarding the identification of users of certain means of communications (such as a mobile phone), the Standing Committee I feels that the expediency of retaining this measure as a specific method should be reconsidered. While the intrusiveness of such a method is assessed as low to very low, this measure is nevertheless subject to the same stringent requirements as all other specific methods, which however may entail a more extreme infringement of privacy. Given the rather substantial use of such methods, this places a heavy administrative burden on these services.

IX.2.3. RECOMMENDATIONS REGARDING INFORMATION SECURITY[214]

IX.2.3.1. Security policy with regard to cyber-attacks

Both in Belgium as well as in the context of Europe and the NATO, a number of initiatives have been developed with regard to information security.[215] The Standing Committee I considers it not only important for our country to properly coordinate these initiatives, but to also actually include these in an integrated security policy on cyber-attacks against national interests. For this, it is essential to set up an agency that will coordinate the activities related to information security.

IX.2.3.2. Extension of powers of the GISS and State Security

The SIM Act assigned an additional task to the GISS to '*neutralise attacks in the context of cyber-attacks on military computer and communications systems or*

[214] See Chapter II.2. Protection of communication systems against possible foreign interceptions and cyber-attacks.

[215] For example, see the White Paper *Towards a national policy in information security*, the *NATO Cyber Defence Policy* and the *European Programme for Critical Infrastructure Protection* (free translation).

systems controlled by the Minister of Defence and to identify the perpetrators, without prejudice to the right to immediately respond with its own cyber-attack' (Art. 11 §1, 2° of the Intelligence Services Act) (free translation). However, the Standing Committee I recommends that the same option be provided in case of attacks against information systems of other public services or against national critical infrastructure. This task could be entrusted to State Security.

IX.2.3.3. Sufficiently qualified staff members

The Standing Committee I found that there was a serious shortage of qualified staff members in the intelligence services for performing the task related to information security. It recommends that these services finally acquire the means enabling them to recruit the necessary staff.

IX.2.3.4. Sufficiently secure equipment for processing sensitive and classified information

The Standing Committee I recommends that the greatest circumspection be exercised in choosing secure technical equipment for processing sensitive and classified information. The Committee adopts the recommendations of the *White Paper of the Federal Consultation Platform on Information Security* (free translation) and recommends that technical equipment be assessed, certified and approved (with regard to reliability and safety) in accordance with criteria and procedures compliant with EU standards.

In addition, the Standing Committee I recommends that contracts only be awarded to suppliers of technical equipment holding a security clearance. As part of the preliminary security investigation, special consideration must be given to possible ties between these suppliers and certain foreign intelligence services.

IX.2.3.5. Sufficient technical means of certification and approval

The lack of technical means of certification and homologation in the area of information security is also perceived to be a serious problem by the Standing Committee I. Therefore, it recommends that the necessary resources be provided, so that the certification and homologation of the systems used in Belgium to process classified information can finally take place without being dependent on foreign authorities and services.

IX.2.4. RECOMMENDATIONS WITH REGARD TO THE CUTA AND ITS SUPPORTING SERVICES[216]

IX.2.4.1. A clear single point of contact

Some supporting services of the CUTA do not have a known and recognised single point of contact (SPOC). Although experts from these services partially make up for this shortcoming, the fact remains that there are no guarantees for the traceability of the information flows or the organisation of the official communication of intelligence. In the opinion of the Standing Committees P and I, serious efforts must be made to resolve this issue in the short term.

IX.2.4.2. A clear insight into the information flows

The single point of contact within each supporting service of the CUTA should have a complete picture of the intelligence and/or assessments exchanged. Moreover, the traceability of the intelligence within each service must also be guaranteed.

IX.2.4.3. Acknowledgements of receipt and degrees of urgency

The investigation showed that the obligations under Article 11 §§2 and 3 of the Royal Decree implementing the Threat Assessment Act to acknowledge receipt and comply with the degrees of urgency were not respected at all times. The Committees were of the opinion that if these obligations did not provide any added value for the services, the regulations should be amended to that effect. Otherwise, the Royal Decree should be refined further, in the sense that a regulatory option should be incorporated stating that a response is not necessary if there is no information available. The Committees also felt that a clear distinction must be made between recipients of 'for your information' messages and recipients from whom an (a) (re)action is expected.

IX.2.4.4. Confusion regarding concepts related to various embargo procedures

Any confusion between concepts related to the embargo procedures *ex* Articles 11 and 12 of the Threat Assessment Act and similar procedures from e.g. the Police Function Act, should be completely eliminated.

---

216 The first six recommendations are the result of the findings made in the context of the investigation regarding 'Information flows between the CUTA and its supporting services' (see Chapter II.4). The seventh recommendation stems from the joint investigation into 'A planned mission abroad by the CUTA' (see Chapter II.5). The final recommendation is the result of both investigations.

IX.2.4.5. Operationalisation of the secure communication and information platform

The Standing Committees P and I recommend that a vision for the future be developed for a secure, encrypted communication and information platform and that in the short term, the existing obstacles be removed to ensure that the planned connections finally become operational.

IX.2.4.6. Explanation of the term 'relevant intelligence'

Some supporting services find it difficult to interpret the concept of 'relevant intelligence' in practice. The interpretation of this concept must be clearly explained, possibly in joint working groups.

IX.2.4.7. Confusion about the identity of the CUTA

It is recommended that the CUTA must always ensure that there is no confusion regarding its unique identity. In contrast to the GISS and State Security, the CUTA is not an intelligence service. It is essential to actively and consistently draw attention to this fact in its communication and operations, both in Belgium and abroad. In this context, it is recommended that the CUTA be extremely cautious in undertaking foreign missions and that its study tours should be strictly defined.

IX.2.4.8. The 'foreign assignment' of the CUTA

Regarding the relationship between the CUTA and the two intelligence services, the GISS questions the CUTA's mandate abroad and State Security has reservations regarding the contacts between the CUTA and foreign intelligence services. These aspects should be defined more clearly among the concerned services. However, even more importantly, the Ministerial Committee for Intelligence and Security should finally issue a guideline on this matter, in implementation of Article 8, 3° of the Threat Assessment Act.

IX.2.5. RECOMMENDATIONS WITH REGARD TO THE FIGHT AGAINST PROLIFERATION AND THE PROTECTION OF THE SEP[217]

The Standing Committee I recommends that State Security changes its approach in the fight against proliferation from one that is reactive and ad hoc to one which is more proactive and which focuses on more strategic assessments. Moreover, these assessments should not overlook aspects such as 'economic interests' and possible 'interference' by foreign (intelligence) services. Such assessments require a reliable information position, which can only be achieved by intensifying contacts with the Belgian administrations, companies, laboratories and research centres and through cooperation agreements with bodies involved in the fight against proliferation.[218] Based on the same concern, the Committee recommends that analysts and operational agents working in the area of the protection of the SEP and the fight against proliferation get together to draw up a common methodology. This should also help State Security take up an unambiguous position with respect to the competent political bodies.

Finally, the Committee reiterates the Senate's recommendation which aims to include a specific power in the Intelligence Services Act for monitoring the legitimacy of the activities of foreign intelligence services on our territories.[219]

IX.2.6. DIRECT EXCHANGE OF INFORMATION BETWEEN POLICE AND INTELLIGENCE SERVICES[220]

The Standing Committee I recommends that structured consultations take place between the intelligence services and the (federal and local) police services with a view to exchanging information via well-defined procedures. The absence of a cooperation agreement between these services is, undoubtedly, a shortcoming of our security system. The Standing Committee I has pointed this out on several occasions in the past.[221]

Before considering whether to create a database on terrorism and radicalism, the Standing Committee I recommends that a system of information exchange between the police and intelligence services be set up as soon as possible.

---

217 See Chapter II.2. Protection of communication systems against possible foreign interceptions and cyber-attacks.

218 Such as the FPS Foreign Affairs, the Administration of Customs and Excise, the CANVEK/CANPAN and regional authorities competent for these matters.

219 STANDING COMMITTEE I, *Rapport d'activités 2006*, 128.

220 See Chapter II.3. Information position and actions of the intelligence services with regard to Lors Doukaev.

221 STANDING COMMITTEE I, *Rapport d'activités 2006*, 131; *Rapport d'activités 2007*, 75 and *Rapport d'activités 2009*, 86–87.

IX.2.7. COORDINATION OF THE REPRESENTATION OF SECURITY SERVICES AT INTERNATIONAL FORUMS[222]

The Standing Committees P and I request that a feasibility study be conducted with regard to the establishment of a specific structure that can be entrusted with the task of coordinating and/or representing the various Belgian services participating at international forums and meetings in the context of the fight against terrorism and extremism. More specifically, the Ministerial Committee for Intelligence and Security could take the initiative in this regard and the Board for Intelligence and Security could, in turn, be designated to oversee its implementation.

Naturally, such a structure is not intended for forums that focus specifically on one or more well-defined services.

IX.2.8. A CODE OF ETHICS FOR STATE SECURITY AGENTS[223]

The Standing Committee I recommends that State Security, in implementation of Article 17 of the Royal Decree of 13 December 2006 on the statute of officials of the field services of State Security, draw up a (proposed) code of ethics and submit this for approval to the Minister of Justice.

This code must clearly define what is implied by the obligation of neutrality and discretion on the part of State Security officials. A strict compliance with this code of ethics must also be ensured through a quick and consistent application of the disciplinary procedure in case of non-compliance. This disciplinary procedure must certainly not be confused with a security investigation, which has its own objective.

IX.3. RECOMMENDATIONS WITH REGARD TO THE EFFECTIVENESS OF THE REVIEW

IX.3.1. SPONTANEOUS REPORTING OF PROBLEMS TO THE REVIEW BODIES

The CUTA and the supporting services must spontaneously inform the Standing Committees P and I if they observe any structural dysfunctions in their mutual relations with respect to legality, efficiency or coordination aspects.

---

222 See Chapter II.8. Belgian representation at international meetings on terrorism.

223 See Chapter II.7. Complaint from a member of State Security and his spouse.

IX.3.2. MONITORING THE LOGBOOK ON FOREIGN INTERCEPTIONS[224]

The Standing Committee I recommends that the pages of the logbook on interceptions be initialled in advance by the head of service or an officer designated by him.

224 See Chapter IV. Monitoring the interception of communications broadcast abroad.

ANNEX

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT

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 1 – THE STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE

Subsection 1 – Composition

Art. 28
The Standing Intelligence Agencies Review Committee, hereinafter referred to as the "Standing Committee I", shall consist of three full members, including a Chairman. Two substitutes shall be appointed for each of them. They shall all be

appointed by the Senate, 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 Senate, 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 Senate.

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 Senate 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 Senate 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 Senate.

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 House of Representatives, the Senate, the competent minister or the competent authority.

When the Standing Committee I acts on its own initiative, it shall forthwith inform the Senate 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 Senate with a report on each investigation assignment. This report shall be confidential until its communication to the Senate 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 House of Representatives, the Senate, 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 Senate 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 House 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 House 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 House of Representatives or the Senate 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 Senate 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 their conclusions of a general nature, the House of Representatives and the Senate 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 House of Representatives or the Senate;
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 the Standing Committee P shall be approved by the House of Representatives. The rules of procedure of the Standing Committee I shall be approved by the Senate.

The rules of procedure for the joint meetings shall be approved by the House of Representatives and by the Senate.

In accordance with paragraphs 2 and 3, the House of Representatives and the Senate 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 House of Representatives and the Senate shall each create a permanent committee responsible for monitoring the Standing Committee P and the Standing Committee I respectively.

The House of Representatives and the Senate shall stipulate in their respective regulations, the rules relating to the composition and functioning of each monitoring committee.

§2. Each monitoring committee shall supervise the operation of the Standing Committee concerned, and ensure observance of the provisions of this Act and the rules of procedure.

The monitoring committee of the House of Representatives shall also perform the assignments assigned to the House of Representatives by Articles 8, 9, 11, 1°bis, 2° and 3°, 12, 32, paragraph 1, 33, paragraph 7, 35, §1, 2° and 3°, 36 and 60.

The monitoring committee of the Senate shall also perform the assignments assigned to the Senate by Articles 8, paragraph 1, 9, paragraph 7, 11, 1°bis, 2° and 3°, 12, 32, 33, 35, §1, 2° and 3°, 36 and 60.

§3. The permanent committees shall sit together in order to:
1° Examine the annual reports of the Standing Committees before their publication, in the presence of their members. The conclusions of the monitoring committee shall be attached to the reports;
2° Examine the draft budget of the Standing Committees;
3° Supervise the operation of the Standing Committees in the cases referred to in Articles 52 to 55.

They may also sit together to analyse the results of an investigation requested by the House of Representatives to the Standing Committee I or by the Senate to the Standing Committee P.
§4. Each monitoring committee shall meet at least once per quarter with the Chairman or the members of the Standing Committee concerned. It may also meet at the request of the majority of the members of the monitoring committee, or at the request of the Chairman of the Standing Committee, or at the request of the majority of the members of the Standing Committee.

Every denunciation by a member of the Standing Committee concerned 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 the Standing Committee concerned, or to each of its members, relating to the functioning of the Standing Committee, the observance of this Act, or the rules of procedure.
§5. The members of the monitoring committees 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 they belong to.

ANNEX

30 NOVEMBER 1998 ACT GOVERNING THE INTELLIGENCE AND SECURITY SERVICES

(extract)

Only the chapter concerning the control by the Standing Committee I is reproduced.

[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.]
(…)