ACTIVITY REPORT 2016

ACTIVITY REPORT 2016

Review Investigations, Control of Special Intelligence Methods and Recommendations

Belgian Standing Intelligence Agencies
Review Committee

Belgian Standing Intelligence Agencies Review Committee

intersentia
Cambridge – Antwerp – Portland

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

Activity Report 2016. Review Investigations, Control of Special Intelligence Methods and Recommendations
Belgian Standing Intelligence Agencies Review Committee

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

Cambridge – Antwerp – Portland
www.intersentia.com

ISBN 978-1-78068-642-4
D/2018/7849/27
NUR 823

CONTENTS

LIST OF ABBREVIATIONS

BCC	Belgian Criminal Code
BCCP	Belgian Code of Civil Procedure
BICS	Belgacom International Carrier Services
BOJ	Belgian Official Journal
CCB	Centre for Cybersecurity Belgium *(Centrum voor Cybersecurity België – Centre pour la cybersécurité Belgique)*
CCIRM	Collection coordination and intelligence requirements management
CHOD	Chief of Defence
C.O.C.	Control Agency for Management of Police Information *(Controleorgaan voor politionele informatie – Organe de contrôle de l'information policière)*
COPPRA	Community Policing and Prevention of Radicalisation
CTG	Counter Terrorist Group
CUTA	Coordination Unit for Threat Assessment
Data Protection Act	Act of 8 December 1992 on privacy protection in relation to the processing of personal data *(Wet tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens – Loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel*)
EU	European Union
FCCU	Federal Computer Crime Unit
FTF	Foreign Terrorist Fighters
GCCR	Governmental Coordination and Crisis Centre
GCHQ	General Communications Headquarters (UK)
GISS	General Intelligence and Security Service of the Armed Forces (*Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht – Service Général du Renseignement et de la Sécurité des Forces armées*)
HUMINT	Human Intelligence
ICT	Information and Communication Technology

IMINT	Image Intelligence
Intelligence Services Act	Act of 30 November 1998 governing the intelligence and security services *(Wet houdende regeling van de inlichtingen- en veiligheidsdienst – Loi organique des services de renseignement et de sécurité)*
IO	Immigration Office
IOB	Intelligence Outlook Bulletin
IS	Islamic State
JIB	Joint Information Box
LTF	Local task forces
NSA	National Security Agency (US)
NSC	National Security Council
NTF	National Task Force
OSINT	Open Source Intelligence
OVG	Operation Vigilant Guardian
Parl. doc	Parliamentary Document
PNR	Passenger Name Record
POC	Point of contact
Review Act	Act of 18 July 1991 governing the review of police and intelligence services and of the Coordination Unit for Threat Assessment *(Wet tot regeling van het toezicht op politie- en inlichtingendiensten en op het coördinatieorgaan voor de dreigingsanalyse – Loi organique du contrôle des services de police et de renseignement et de l'organe de coordination pour l'analyse de la menace*)
RFI	Request for information
SEP	Scientific and Economic Potential
SIGINT	Signals Intelligence
SIM	Special Intelligence Methods
SIM Act	Act of 4 February 2010 governing the intelligence collection methods used by the intelligence and security services (*Wet betreffende de methoden voor het verzamelen van gegevens door de inlichtingen- en veiligheidsdiensten – Loi relative aux méthodes de recueil de données par les services de renseignement et de sécurité)*
SIM Commission	Administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services
SLA	Service Level Agreement

SOCMINT	Social Media Intelligence
Standing Committee I	Standing Intelligence Agencies Review Committee *(Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten – Comité permanent de contrôle des services de renseignement et de sécurité)*
Standing Committee P	Standing Police Monitoring Committee *(Vast Comité van Toezicht op de politiediensten – Comité permanent de contrôle des services de police)*
State Security	*Veiligheid van de Staat – Sûreté de l'État*
Threat Assessment Act	Act of 10 July 2006 on Threat Assessment *(Wet betreffende de analyse van de dreiging – Loi relative à l'analyse de la menace)*
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.[1]

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

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

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

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

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

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

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

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

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

Pursuant to Article 35 of the Review Act of 18 July 1991, the Standing Committee I annually draws up a general activity report. These activity reports are drawn up in Belgium's national languages Dutch and French and can be found on the website of the Committee (see www.comiteri.be). With increased globalisation in mind, the Standing Committee I wishes to meet the expectations of a broader public. The sections of the Activity Report 2016 that are most relevant to the international intelligence community (the review investigations, the control of special intelligence methods, the recommendations and the table of contents of the complete activity report), have therefore been translated into English. This book is the sixth to be published in English by the Standing Committee I, after the *Activity Report 2006-2007,* the *Activity Report 2008-2009,* the *Activity Report 2010-2011, the Activity Report 2012-2013* and the *Activity Report 2014-2015* (see www.comiteri.be). The Standing Committee I has now opted for an annual publication of its reports translated into English.

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

1 December 2017

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

ACTIVITY REPORT 2016

TABLE OF CONTENTS

Chapter XI.
Recommendations

Appendices

PREFACE

The terror attacks that have plagued Europe over the last few years have had a significant impact. It is therefore not surprising that the theme of 'security' has become a priority concern. Radicalism and terrorism are now a daily reality. The same applies to espionage and foreign political interference. As they could disrupt our society, they must be resisted. After all, being able to live in safety is a fundamental human right. And the government is obliged to guarantee that safety.

The large number of new regulatory initiatives that have been taken in this regard have a profound effect on the precarious balance between citizens' rights and freedoms and their restriction, temporarily or otherwise, for security reasons.

The Standing Committee I too is faced with the quest for this balance. The Committee – just like other institutions entitled to appropriations[4] – was established to carry out monitoring tasks independently and impartially, in part to assure citizens that the rights granted them under the Constitution and other laws are and will remain guaranteed. In the relationship within the *trias politica* of a democracy based on the rule of law, it is essential that checks and balances can be performed correctly and efficiently. This undoubtedly includes a Parliament that can also actively perform its review duties, including via the Standing Committee I. The quality of the work that these institutions entitled to appropriations can deliver is essential not only to guarantee citizens' rights, but is also a vital factor in the trust that citizens must be able to place in various state institutions.

However, in a changing society in which both security risks and funding restrictions are on the rise, the task to protect the fundamental rights of every citizen is becoming more and more difficult. The executive and legislative powers have moreover assigned increasingly more monitoring tasks to the Standing Committee I over recent years. However, additional funding has not been made available for these tasks.[5]

---

4 This includes the Standing Police Monitoring Committee, the Data Protection Commission, the Control Agency for Management of Police Information (C.O.C.), the Federal Ombudsman, the High Council of Justice, the SIM Commission and the United Appointment Commissions for the Notarial Profession. In 2017, these institutions jointly informed the President of the Chamber of Representatives of the consequences of budgetary restraints.

5 In October 2016, the Committee raised its concerns in this regard with the Justice Parliamentary Committee, following the discussion of the legislative amendments to the

Institutions that are entitled to appropriations must deal with this acute lack of funding and the Standing Committee I is no exception. It goes without saying that more cuts versus more powers will affect the quality of the Standing Committee I's operations. The Committee is adamant that the scant resources must be debated. However, such a debate should be held not only within the context of applying a number of budgetary standards, but also within the context of the indispensable balances that must be maintained in a democracy based on the rule of law.

Guy Rapaille,
Chairman of the Standing
Intelligence Agencies Review Committee

26 September 2017

Intelligence Act by which the intelligence services will receive new powers that will have to be monitored by the Standing Committee I.

CHAPTER II
REVIEW INVESTIGATIONS

In 2016, the Standing Committee I finalised fourteen review investigations, three of which were in conjunction with the Standing Committee P (II.1 to II.14). In the same year, the Standing Committee I also opened three new review investigations, one of which is a joint investigation with the Standing Committee P. This latter investigation was initiated at the request of the Monitoring Committee; the other two investigations were started officially at the Committee's own initiative. One of these investigations – namely the investigation into the Zaventem (Brussels Airport) and Maalbeek (metro station in Brussels) attacks (II.4) – was completed in 2016. A brief description of the other two investigations that were opened follows in II.15.

The Committee received a total of 29 complaints or reports in 2016. This year also marked the start of efforts to relax, deformalise and standardise the 'complaints and reports' work process.[6] After verifying some objective information, the Committee rejected all of these complaints or reports because they were manifestly unfounded (Article 34 of the Review Act) or because the Committee did not have jurisdiction for the matter in question. In the latter cases, the complainants were referred, wherever possible, to the competent authorities (the Standing Committee P, Federal Police and Public Prosecutor). None of the complaints from 2016 resulted in an investigation being opened; one complaint was added to an existing intelligence file.

II.1. THE ISSUE OF FOREIGN TERRORIST FIGHTERS

Since 2013, the Syrian conflict had been a magnet for foreign (terrorist) fighters[7] from all over the world. And a proportionally large number of those fighters were from Belgium.

---

6 First the admissibility and validity of a complaint are studied, after which it is processed by the Investigation Service I. If a general problem arises, the Committee may decide to open a review investigation, otherwise the inquiry remains limited to the complaint *per se* (a complaint inquiry).

7 The Committee used to refer to the 'contingent of foreign fighters in Syria', referring to those who left for or returned (returnees) from Syria or neighbouring countries (jihadist conflict

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

At the start of 2015, a first, interim report was drawn up.[8] The final report is dated February 2016.

II.1.1. A CONSTANT EVOLUTION

The problem and approach of foreign terrorist fighters is constantly evolving. Intelligence services have adapted their priorities and implemented structural and organisational changes, the Parliament has outlined the general framework, and the government has specified the regulatory framework and taken various initiatives.[9]

State Security management already held out the prospect of significant changes to its strategy and organisation in 2014. Meanwhile, the government has taken a number of decisions to reinforce the service and additional

---

zones) and participate in the armed fight on the side of terrorist groups. The Circular of the Ministers of the Interior and Justice of 21 August 2015 and COL 10/2015 of the Board of Procurators General renamed these as foreign 'terrorist' fighters (FTFs). Both the Circular and COL 10/2015 have defined six categories in this regard, depending on the status of the person: (1) suspected to be in a jihadist conflict zone, (2) en route to a jihadist conflict zone, (3) in Belgium, after having been in a jihadist conflict zone (returnees), (4) in Belgium, after having been en route to a jihadist conflict zone, (5) serious indications that he will leave for a jihadist conflict zone and (6) support and recruitment.

8 In this regard, see: STANDING COMMITTEE I, *Activity Report 2015*, 120–124 ('II.4. The monitoring of Syria fighters by the two Belgian intelligence services: an interim report'). This explained the effect of this problem on the functioning of State Security and GISS and indicated which resources both services had deployed. Attention was also paid to the organisational problems and the risks confronting both intelligence services.

9 In that light, the Committee referred, inter alia, to the 'Circular on the exchange of information relating to and the monitoring of foreign terrorist fighters from Belgium' (free translation).

resources have been allocated. Within the intelligence assignment, 'the fight against jihadi combatants' has been brought forward as one of the three priorities in the 2015 Action Plan. The structure of the service has also been changed significantly.[10]

State Security memoranda showed the Federal Prosecutor's Office/Federal Prosecutor as the main addressee, followed by the Immigration Office and CUTA. Fairly little information was exchanged with GISS.[11] The number of strategic memoranda was relatively small. The theme of foreign fighters was strongly represented in the use of special intelligence methods: around 60% of all SIMs used by State Security – mainly identification, localisation, etc. – during the period from June to October 2015 was linked to this problem.

GISS too considered it its duty to provide, based on its own specialisms (mostly focused abroad) and given the specific collection resources, intelligence on both the threats concerning Belgians or Belgian interests abroad and the impact of foreign phenomena in Belgium to various bodies and in various consultation platforms (such as the local task forces). GISS deployed a range of collection resources for this purpose (HUMINT, SIGINT, IMINT, OSINT and SOCMINT).

Not only the organisation of the intelligence services but also the broader cooperation structures (e.g. the national and local task forces) were redesigned with a view to a more focused and streamlined approach. This meant that the 'Task force foreign fighters' and 'Platform returnees' ceased to exist as from 1 September 2015. Other structures from the Plan R – the National Task Force (NTF) and the local task force (LTF) – were updated. The National Task Force was expanded with representatives from the Regions and Communities and an 'FTF working group' was established under the NTF. Local task forces consist of a strategic component at district level and of an operational component at local level.

The FTF's concrete approach involved various aspects: determining the presence or absence of a foreign fighter, verifying and enriching the information, the individual threat evaluation and the standardised and personalised monitoring. All the services involved had clearly described duties to fulfil regarding those aspects. In order to manage and share the information, it was decided to install a 'dynamic database' in 2016.[12]

---

10 At the time of the investigation, it was still too premature to verify the extent to which the new structure has effectively contributed towards a better information position in relation to foreign terrorist fighters. However, it was clear that this theme seemed to be having a major effect on the functioning and workload of State Security.

11 Around 60% of the official memoranda to the Belgian authorities (*notes aux autorités (NA)*) had the Federal Prosecutor's Office or Federal Prosecutor as the addressee, 17% the Immigration Office and only 6% the military intelligence service.

12 In this regard, see: 'Chapter VI. Verification of common databases'.

II.1.2. LEGAL FRAMEWORK[13]

II.1.2.1. State Security

Pursuant to Articles 7, 1° and 8, 1° b) and c) of the Intelligence Services Act, which relate to extremist and terrorist threats, State Security is authorised to gather intelligence on anyone who intended to depart to the jihadist conflict zone in Syria and Iraq, spent time there, and returned. Participants in this conflict formed a possible or real danger for the internal and external security of the country.

State Security could use all its powers in relation to both extremism and terrorism in this regard (ordinary, specific and exceptional methods). Strictly speaking, exceptional methods could not be used in the fight against a solely extremist threat. But this finding had to be refined in such a way that the methods could be used to combat radicalisation processes. Although ordinary intelligence methods could also be used abroad in theory, this did not apply to the specific and exceptional methods whose application was limited to Belgian territory (Art. 18/1, 2° of the Intelligence Services Act).[14]

The question of whether intelligence collected by State Security could or had to be passed on to third parties differed, depending on the service involved and the nature of the intelligence. Article 19 of the Intelligence Services Act allows State Security to pass on all information and intelligence to the police services and judicial authorities, if this data is relevant to their assignments. Information that points to a possible crime should be sent to the judicial authorities on the basis of Article 29 of the Belgian Code of Civil Procedure (BCCP) or Article 19/1 of the Intelligence Services Act – and, in this latter case, via the SIM Commission. In relation to forwarding information to foreign services, the Standing Committee I reiterated that the statutory framework was inadequate, particularly as regards the transmission of personal data.[15]

Lastly, Articles 9, 11 §3 and 20 of the Intelligence Services Act instruct intelligence services to cooperate as effectively as possible, not only with each other but also with other administrative authorities, police services, judicial authorities (in the form of technical assistance, for example) and foreign intelligence services. In relation to 'technical assistance' to the judiciary, the Committee has already expressly stated on several occasions that a strict

---

13 After the end of the investigation, various aspects were changed by the entry into force of the Act of 30 March 2017 to amend the Act of 30 November 1998 governing the intelligence and security services and Article 259*bis* of the Criminal Code, *BOJ* 28 April 2017. As a result of this, a number of the findings below ceased to apply.

14 Both restrictions were eliminated by the Act of 30 March 2017 (*supra*).

15 This was partially remedied by a Directive of the Ministers of Justice and Defence 'on the relationships between Belgian intelligence services and foreign intelligence services' (free translation) dated 26 September 2016.

interpretation of this provision does not allow State Security (and GISS) to use intelligence powers for judicial purposes.[16] The Committee was able to conclude that State Security is providing increasingly frequent technical assistance as an expert on various levels to the judiciary in relation to the Syria problem. The Committee was unable to conclude that statutory rules were not being observed in that regard.

II.1.2.2. General Intelligence and Security Service

The Act of 30 November 1998 provided three grounds for GISS to gather and process data on foreign terrorist fighters.[17] First was the '*execution of the assignments of the armed forces*', namely '*any expression of the intent to neutralise, hinder, sabotage, endanger or prevent the preparation, mobilisation and use of the Belgian armed forces, of allied armed forces or of inter-allied defence organisations for missions, actions or operations in a national context or in the context of an alliance or an international or supranational cooperation agreement.*' (Article 11 §2, 3° of the Intelligence Services Act – free translation). Safeguarding the '*execution of the assignments of the armed forces*' allows for the monitoring of any '*activity*' (Article 11 §1, 1° of the Intelligence Services Act) or better still '*any expression of the intent*' (Article 11 §2, 3° of the Intelligence Services Act) that can jeopardise this interest. Contrary to State Security, there accordingly does not need to be any threat (such as extremism or terrorism).[18] The extremist and terrorist activities both of those abroad (foreign fighters) and within Belgium (e.g. extremists in the army) formed the basis for GISS to carry out its intelligence work. Even so, it ought to be emphasised that GISS – unlike State Security – was not authorised to monitor phenomena such as 'extremism' and 'terrorism' *per se*. The Standing Committee I previously held in that regard that '*monitoring of radical Islamism is part of the powers and responsibilities of GISS, to the extent that military security in the broad sense in Belgium and abroad is under threat.*'[19] A second ground was the safety of Belgian nationals abroad. In this regard, GISS had to pay attention to '*any expression of intent to endanger the life or physical integrity of Belgians abroad and their family members collectively by destruction, massacre or pillage*' (free translation). However, the investigation has shown that GISS prepared analyses that extended beyond '*military security*' or the '*protection*

16 If certain investigative acts need to be performed as part of a judicial inquiry, special intelligence methods may not be used for this purpose. Instead, the appropriate judicial investigative methods (such as special detection methods) ought to be applied.

17 The description of GISS's powers was also substantially amended by the Act of 30 March 2017 (*supra*).

18 For the first interest of the military intelligence service to be protected, there must be a specific threat before the service is authorised to act: a '*military means*' must be used (Art. 11 §2 1° of the Intelligence Services Act).

19 STANDING COMMITTEE I, *Activity Report 2007*, 100.

of Belgians abroad'. A third ground was the '*protection and the continued existence of the population*', which, given the number of attacks and attempted attacks, was clearly put at risk by '*military means*'.

GISS could also use the option of intercepting communications that were sent from abroad (Article 259*bis* of the Criminal Code).[20] Such interceptions were possible in the context of the military operation against IS (for example because of the presence of F16s), for the protection of Belgians abroad (especially in the region concerned) and of the Belgian population as a whole. SIGINT activities could not be performed for other reasons within the context of the Syria problem.

Using ordinary intelligence methods was permitted, including abroad, but obviously only to the extent in which the collection could be linked to a threat that GISS could monitor. In the context of the Syria problem, GISS could naturally use specific or exceptional intelligence methods if there was a threat against one of the interests listed in the Act. The use of such methods just had to be limited to Belgian territory (Art. 18/1, 2° of the Intelligence Services Act).[21]

Like State Security, GISS had to work as efficiently as possible with other authorities, without being allowed to use methods outside their own area of responsibility, solely to support the mission of another service.

II.1.3. ASSESSMENT OF THE INFORMATION POSITION OF THE INTELLIGENCE SERVICES

An 'information position' refers to the entire body of intelligence that an intelligence service has at its disposal in relation to a specific topic, person, event, etc. State Security reported at the start of the review investigation in October 2014 that it had a relatively good information position in relation to the Syria problem. Even so, it was stressed that the service had no insight into the activities in Syria and Iraq of around half of the 'Belgian' individuals (people living in Belgium, regardless of nationality). GISS, in turn, stated at the time that its information position was inadequate for it to achieve its ambitions. GISS made its contribution within the Syria file, but this contribution clearly had to be reinforced by more professional support of the analysis capacity and by using new collection techniques. The service also pointed to a number of limitations.

There was little (objectifiable) material available for the manner in which the qualitative assessment of the end products and assessment of the information position of an intelligence service had to be performed. The Committee therefore

---

20 Amended by the entry into force of the Act of 30 March 2017 to amend the Act of 30 November 1998 governing the intelligence and security services and Article 259*bis* of the Criminal Code, *BOJ* 28 April 2017.

21 Amended by the Act of 30 March 2017 (*supra*).

did not evaluate the information position as such, but rather the intelligence processes that had led to that position. These were checked in relation to a number of formal elements (referred to below as 'benchmarks') that by themselves provided a procedural guarantee that a quality information position would be established.[22] This approach was also a form of risk analysis: if certain procedures/work processes were not followed, this could indicate that the information position was on a shaky footing.

II.1.3.1. Data collection and sources

The first benchmark involved the collection of data and the sources. The Committee held the view that, in relation to State Security or GISS, there were no specific risks in this regard. Both services used various disciplines, methods and sources for their collection activities pertaining to FTFs. At State Security, it was particularly HUMINT and the SIMs that attracted special attention in this regard. The data that was finally processed into intelligence – to the extent possible and given the circumstances – was fairly complete and precise; it tried to formulate an answer to the who, what, why, when and where questions. The information was also presented as it was phrased by or shown in the source itself; in other words, it was 'objective'.[23] The data on foreign terrorist fighters was therefore collected in a relatively good way. At least as far as procedures were concerned, it could be stated that both services adopted measures to expand the information position as effectively as possible.

II.1.3.2. Data and knowledge management

A second benchmark involved the manner in which the data was stored, classified and managed (data and knowledge management).

Although the data management system at State Security offered a solid basis for intelligence work, it could have been improved. Both a lack of standardisation and redundancy were found.

Data management at GISS constituted a major risk. The manner in which the information was stored and managed was fairly problematic. Searching for information was not only time-consuming, there was also no guarantee that the correct and all available information would be found. If a search involved connecting the dots, GISS ran the risk that certain data would not emerge, or would not emerge quickly enough, either because the search engine did not find

---

22 The Committee was guided by the DE VALK methodology and chose to carry out an extensive random check. See: G.G. DE VALK, *Dutch Intelligence. Towards a Qualitative Framework for Analysis. With Cases Studies on the Shipping Research Bureau and the National Security Service (BND)*, University of Groningen, 2005.

23 However, the Committee found that the sources were not always systematically evaluated at GISS and that there was not always enough information about the source.

it – for example, because of the problem of separate file folders for different divisions – or because it simply had not been uploaded (incomplete input in the database). For the purpose of assessing how GISS's information position was built up, this was a problem that the service had been dealing with for many years and which had put a severe strain on the quality of its information position.

II.1.3.3. Analysis processes

The manner in which incoming information is analysed to distil 'intelligence' (analysis processes) formed the third benchmark. The Committee investigated how the analysis documents regarding the Syria problem were drawn up and what was the methodological basis. After all, the use of properly substantiated methods is crucial to guarantee the quality of the end product.

It was established in relation to State Security that although the analysis services had a specific toolbox, these methods were not used systematically. According to the service, this was compensated for by the fact that an analyst never faces a problem alone but that colleagues and superiors are also focused on creating a good product.

At GISS, the C(ounter) I(ntelligence)/Homeland service was more advanced in the use of instruments and analysis methods than Division I(ntelligence). The latter put forward the same arguments as State Security, namely that the quality provided does not depend solely on the use of formal methods (which are sometimes time-consuming and/or overly theoretical), but is also guaranteed by the interaction between various analysts and their hierarchy.

Arguments for and against the rigorous use of methods could be put forward for both State Security and GISS. It is important for this to be dealt with consciously (risk assessment).

II.1.3.4. User's needs and feedback

A fourth benchmark was whether the product catered for the user's needs (fit for use) and took advantage of the feedback. The Committee found a number of gaps in this regard that had an adverse effect on the intelligence processes, and thus possibly on the resultant products. It should be pointed out that these gaps were not necessarily fully attributable to the services themselves.

A first problem related to how clients expressed their wishes and needs (or sometimes did not do so) and gave feedback. The Committee found that when clients gave few or no indications regarding their needs or when feedback was lacking, the services sometimes found it more difficult to match their products to those needs.

The Committee noted in relation to the formal aspects of providing information that the services indeed paid attention to properly presenting their products and put forward clear conclusions.

An attempt was generally made to draw up memoranda such that clients could make beneficial use of them. At GISS, at least in Division I, there was even a formal directive that determined how a document had to be drawn up. This offered a certain quality guarantee, at least in relation to form. Other elements, such as Service Level Agreements (SLAs), the distribution list and the existence of the production support position were examples to be followed as well.

II.1.3.5. The predictive nature of intelligence work

The fifth benchmark involved the predictive nature of intelligence work. The Standing Committee I determined that both intelligence services provided more descriptive and explanatory intelligence than predictive intelligence. The Intelligence Outlook Bulletins (IOB) of Division I of GISS was an exception in this regard. Insofar as the competent (judicial, police, political) authorities of the intelligence services wished to be provided with possible scenarios and substantiated hypotheses in order to initiate certain actions in that way, the intelligence provided by the services was usually less suitable for that purpose.

II.1.3.6. Design or planning of the intelligence effort

The design or planning of the global intelligence effort in the Syria problem was the sixth benchmark. The aim was to describe both the collection/analysis efforts and methods and try to establish links between them.

This was an important challenge at both intelligence services. Some building blocks existed at State Security and GISS, but these needed to be better integrated and elaborated than they were at the time of the investigation. Although the individual intelligence processes were not fundamentally disrupted by this shortcoming, the global results of the intelligence effort (in terms of efficiency and coordination) would be improved if more attention was paid to this aspect. It goes without saying for the actual collection approach, and its extent, that certain data could have escaped the services. The Standing Committee I was of the opinion that the collection approach of both services was sufficiently diversified and broad, and offered the necessary guarantees so that the information position could be duly established. This ties in again with the first benchmark.

II.1.3.7. Conclusion

The intelligence services succeeded in limiting various risks associated with the benchmarks while developing their information position regarding the Syria problem. Nonetheless, a number of risks still manifested themselves that the Committee felt needed to be addressed. The data management issue, particularly for GISS, was a priority in this regard.

II.1.4. INTELLIGENCE SERVICES AND LOCAL TASK FORCES (LTF)

Significant differences were discovered in relation to the structure, organisation and execution of the various local task forces. This was not necessarily a problem in itself, since local situations could differ. Even so, the larger the LTF, the more this seemed to affect efficiency.

It was clear that the different participants in the LTF (police, intelligence services, public prosecutor's office, etc.) each came to the meetings with their own expectations and tasks ('intelligence work' versus 'police work'). A number of restrictions also applied to the intelligence services (for example in relation to classification, need to know, and the third-party agency rule) that affected how they cooperated in LTFs.

From the perspective of the intelligence service, the question of security clearances was a major stumbling block: it put a brake on the exchange of information and was not always fully taken into account or appreciated by the other players. This problem was partly solved by the FTF Circular as it was decided that all participants in LTFs had to hold a security clearance at SECRET classification level. The Standing Committee I felt that this was a step forward. However, this implied that all participants would now be in possession of certain classified information that they could not simply share with persons or authorities that did not hold security clearance.

In this regard, the Committee felt reflection was needed on the question of the precise information that needed classifying. The Director-General asked for more openness from State Security in that regard.

Doubts and questions were also raised about what was expected from both State Security and GISS employees in the local task forces. The 'original' FF Circular was too superficial in this respect: although the assignments were described, no tasks were 'allocated'. The participants were left with a number of questions: were the LTFs established for the exchange of information – and, if so, which type of information – or were they rather bodies for networking and raising awareness? And – depending on the purpose – what was then the most appropriate composition? It was suggested, for example, that an analyst should also sometimes be sent to the LTF. In addition to merely providing 'operational' information, State Security could also play a broader contextualising role in this way. The review investigation found that members of State Security considered it appropriate for central management to give direction in this regard. Field expectations were not completely fulfilled.

The new Circular (*supra*) was also helpful here: the specific approach of the foreign fighters was divided into a number of different aspects (determining the presence or absence of the FTF, verifying and enriching the information, the

individual threat analysis and the standardised and personalised monitoring) with a clearly defined remit for everyone.

II.1.5. COOPERATION WITH THE JUDICIAL AUTHORITIES

None of the interviewed services questioned the legal framework of the cooperation, which seemed adequate and adapted to the requirements of the fight against foreign (terrorist) fighters and returnees. All of the interviewed services emphasised the good cooperation between the intelligence services, the police and the Federal Prosecutor's Office[24] in relation to the Syria problem. That cooperation had improved since the arrival of the new State Security management.

However, the Committee found that State Security and GISS pursued a different information policy with regard to the judicial authorities and that little use was made of Article 19/1 of the Intelligence Services Act. In specific case files, protecting the sources of the intelligence services could have been problematic, even though the intervention of the Federal Prosecutor's Office meant difficulties could be avoided.

The various players also considered the direct cooperation between the intelligence services and the police services to be positive. Nonetheless, a specific description of the role that each service could fulfil at an operational level, taking its own expertise into account, was considered desirable.

A delicate problem raised by the police services concerned the culture of classification and security clearances. The police services acknowledged they needed to come up with internal improvements in this regard.

II.2. INFORMATION POSITION OF STATE SECURITY AND THE FAILED ATTACK ON THE HIGH-SPEED THALYS TRAIN

II.2.1. THE FACTS

On 21 August 2015, the high-speed Thalys train between Amsterdam and Paris was the target of a terrorist attack by an individual. However, a number of

[24] For the period from 1 October 2014 to 31 March 2015, State Security received 132 requests for technical assistance (Art. 20 §2 of the Intelligence Services Act), most of which related to international terrorism cases. For the period March-April 2015, GISS received 60 requests for technical assistance, of which 90% related to the problem of foreign fighters. The service complied with these requests.

passengers were able to quickly overpower him. The perpetrator was identified as Ayoub El Khazzani from Morocco. He allegedly boarded the Thalys in Brussels with weapons that he had purchased in Belgium.[25] The Standing Committee I opened an additional investigation as a corollary of its review investigation into foreign terrorist fighters (II.1). This investigation related only to State Security. After all, GISS declared that it held no information relating to Ayoub El Khazzani prior to the attack.

II.2.2. WAS THE PERPETRATOR KNOWN TO STATE SECURITY?

Ayoub El Khazzani had been known to State Security since 2012: his name, together with that of his brother Imram, first surfaced in a report that State Security drafted in June 2012 following a meeting with a foreign partner service. The brothers were associated with a prominent member of a foreign jihadist cell. This member allegedly fled to Belgium and formed the link in a larger network that was involved in sending fighters to Syria. Their identity was included in State Security's database.

Over the subsequent months, intelligence and photographs were exchanged and State Security was asked to verify certain information, which it did. Verifications at the Immigration Office yielded no result. In October 2012, State Security participated in a meeting with the partner service about the jihadist cell and the presence of some of its members on Belgian territory. The intelligence service learnt that a judicial inquiry had been opened into that cell in Belgium. The Standing Committee I found no traces of communication showing that the Federal Police and State Security had exchanged information in this regard.[26]

El Khazzani was placed on an international list in April 2013, presumably by the partner service, after which news regarding the brothers quietened down.

On 11 May 2015, the correspondent sent another document to State Security containing information about Ayoub El Khazzani. The partner service stated it was interested in El Khazzani, his contacts with Belgian extremist circles and his possible role as a liaison within the networks operating via Belgium. No reference is made in this document to any purchase of weapons or a plan to commit a terrorist attack. The partner service also did not provide any photograph of Ayoub El Khazzani or indicate that the matter was urgent. The document was

---

25 The Paris public prosecutor officially charged the perpetrator with attempted murder linked to terrorism and the illegal possession of weapons. At the time of writing, he is awaiting trial.

26 It was noteworthy that State Security had no direct access to the police databases. State Security stated that it received information only when the police took the initiative in that regard or when it expressly requested information. However, pursuant to Article 14 of the Intelligence Services Act, State Security may request any type of information from the police services.

forwarded internally two days later to the Analysis Service and the central service of the External Services. On the same day, the central service sent the document, marked 'for investigation', to the competent provincial post.[27] The provincial post confirmed that it carried out a search in the National Register and went to the Local Police on 30 June 2015. The Committee found that State Security did not take the initiative itself to obtain a photograph of El Khazzani from the police or partner service. No answer was sent to the foreign correspondent. It is not unusual for the service not to have information (known as a silent answer).

On 17 August 2015, State Security received additional information from the partner service, which showed interest in Ayoub El Khazzani again and also asked for three mobile telephone numbers to be identified. The information was shared with the Analysis Service and External Services on 18 August 2015 (i.e. three days before the failed attack). On 19 August 2015, the Assessment Service entered the request in the ICT system for delivery to the competent provincial post. On 22 August 2015, i.e. after the failed attack, State Security proceeded with the identification as requested by the partner service. State Security drafted a document with information about Ayoub El Khazzani, who had meanwhile been arrested, and identified the three mobile telephone numbers.

II.2.3. CONTEXT OF THE CASE FILE

In order to place the events in context, the Committee investigated how State Security managed requests from foreign correspondents at that time.

Documents that are sent to State Security firstly pass through a unique entry point. At the time of the Thalys attack, the procedure was for these documents to then be sent to both the Analysis Service and External Services, within the limits of their respective powers. Changes have been made to this procedure since State Security was restructured in September 2015. Although incoming information still passes through a unique entry point, it is then sent to the competent department of the Analysis Service. This service determines whether and which External Services are to be notified and requests further inquiry, if necessary.

In August 2015[28], State Security received around 1,200 documents from foreign correspondents. A quarter of those were sent to the department that investigates radical Islamism.[29] Just over 40 of those documents contained

---

27 This was also the only time that the ICT tool provided for that purpose in the State Security database was used to send a message. Because the investigation at the time did not yield any results relating to El Khazzani, the provincial post concerned left the task open in the database so that it could, in its own words, continue with it at a later stage.

28 The month in which the partner service sent its request for the identification of telephone numbers, but also the month of the failed attack on the high-speed Thalys train.

29 The Standing Committee I noted that the number of documents received during August 2015 by the department tasked with 'radical Islamism' was not representative of the normal flow of

requests for information that required action by State Security.[30] Only a few of those related to the identification of telephone details. The request relating to Ayoub El Khazzani was the only one that was complied with, albeit after the attack.

As far as requests from foreign correspondents to identify telephone numbers (Art. 18/7 of the Intelligence Services Act) are concerned, the Standing Committee I also studied the figures relating to the period from January to August 2015. These showed that State Security made 130 identifications in this period at the request of a foreign service.[31] Almost ten of these methods – requested for the period from 1 July to 21 August 2015 – related to extremist terrorism. In those case files in which State Security made an identification, the period between the request from the foreign service and compliance with the request fluctuated between 6[32] and 64 days. In the context of the specific request to identify the telephone numbers of Ayoub El Khazzani, this took three days.[33] The Committee therefore concluded that the fact that the identification was not made within three days was not unusual in itself.

Lastly, it ought to be noted that, in hindsight, the requested telephone identification would not have been decisive because the numbers originated from prepaid and thus 'anonymous' cards. However, the subsequent investigation by State Security into the numbers in question did allow for the identification of persons with whom Ayoub El Khazzani had been in contact in Belgium.

II.2.4. FINDINGS AND CONCLUSIONS

State Security performed its work on the basis of intelligence it received from abroad. This information was not very detailed. The Committee had to conclude

---

incoming documents. For example, that department received around 850 documents from foreign correspondents in September 2015 and around 1,050 in October of the same year.

30 There was no uniformity in how questions from foreign correspondents were entered in the ICT system. They were alternately described as 'requests for information' (RFIs), 'questions' or even 'requests to trace'. State Security explained that it can only exercise limited influence on the choice of titles by its correspondents. They depend on the language of the correspondent, the choices made in translation, the standard procedures that apply at correspondents, etc. The questions from the foreign correspondent moreover indicated no level of urgency (routine, urgent, flash). This finding applies only to the documents that the Committee consulted as part of this investigation. As a result, it was not easy to determine the priority of investigation assignments.

31 These 130 methods relate to all matters to be monitored by State Security. That gives an average of 16 identifications a month.

32 It is noteworthy that this rather short period relates to a request for identification by a partner service and in the context of a case file relating to the Verviers cell.

33 Two days should be added to this period if the period it took for the liaison officer of the partner service to send the request is also taken into account.

that monitoring of how the questions from the foreign correspondent were managed had not been optimal:

- The file management was routine. For example, State Security did not make any attempts to obtain further information about the file, with a view to making progress in the investigation;
- There was a lack of management in the central departments;
- Neither State Security nor the foreign correspondent indicated a level of urgency or importance for the processing of information in the El Khazzani case. There was also no mention of a precise threat;
- Although the information of May 2015 was processed via the ICT system provided for that purpose, the investigation assignments, reminders to the Analysis Services and the results (even negative ones) were not included in the system. The Standing Committee I was of the opinion that the failure to use the ICT system weakened the information management;
- The External Services did not forward the results of the investigation assignments carried out in May 2015, even the negative ones, to the Analysis Service and no answer was provided to the foreign correspondent. Likewise, the results of the above investigation assignments did not make it possible to close the case file or open new hypotheses.

The Standing Committee I did not find any exchange of information between State Security and the Federal Police.

The El Khazzani brothers featured on an international list. Although the Standing Committee I did not dispute the value of such a list, it emphasised that both national and international lists exist whose relevance and up-to-dateness is not always guaranteed. State Security cooperated in this list but stated that it did not have the resources to monitor and check every name on it (more than 2,500) without receiving more indications regarding the context and threat represented by the individual. According to State Security, the intelligence services would need to develop a risk management system linked to potential jihadis.[34] Such a system would enable the services to rank those involved according to how dangerous they are.

More generally, the Standing Committee I noted that the resources of the intelligence services that are assigned to investigate those who constitute a threat, are limited. The ease with which those involved could move within and even outside Europe, could use all sorts of different means of communication, and stay anonymously in regions and countries without being discovered, represents a major challenge for intelligence and security services.

[34] The intelligence services have meanwhile held discussions in this regard.

II.3. INFORMATION POSITION OF THE TWO INTELLIGENCE SERVICES BEFORE THE PARIS ATTACKS

II.3.1. EVENTS IN BRIEF

Several deadly attacks took place almost simultaneously in Paris on 13 November 2015. Just after 9 p.m., there were three explosions in the vicinity of the national stadium, *Stade de France*, where a football match was being played between France and Germany. Three suicide bombers wearing explosive belts blew themselves up in the vicinity of the stadium. Besides the attackers, one victim also died. Only 15 minutes later, there were shootings near the patios of cafés and restaurants in the city centre. Dozens of people were killed and wounded. Lastly, in the nearby Bataclan concert hall, 90 people were brutally assassinated. The three attackers here died as well.

In total, there were 130 fatalities that night, with more than 400 people wounded. The terrorist movement Islamic State (IS)[35] claimed responsibility for the attacks in an official statement.

Almost immediately after the bloody attacks, the Standing Committee I opened an '*investigation into the information position of the two intelligence services, prior to the evening of 13 November 2015, regarding the individuals or groups that perpetrated or were involved in the Paris attacks*'[36] (free translation). After all, information quickly emerged pointing to a close connection with Belgium: five terrorists were from or resident in Belgium, the vehicles used for the attacks had been rented in Belgium, Belgian safe houses were involved, the explosive belts had probably been assembled in an apartment in Schaerbeek, etc.

The Standing Committee I firstly assessed what State Security and GISS knew about the perpetrators prior to the attacks and what collection resources they used in that regard. It also examined how those services cooperated with other national and international authorities before and after the Paris attacks. The manner in which the relevant authorities (government, public prosecutor's office, etc.) were informed of imminent threats so they could adopt the necessary

35 The Standing Committee I has opted for the name Islamic State (IS) instead of the acronym DAESH.

36 The investigation was completed in July 2016 (limited circulation – 47 pages). Two interim reports were drawn up prior to that for the Monitoring Committee in the Chamber of Representatives. The first report of 24 February 2016 (limited circulation – 41 pages) was mostly descriptive and quantitative in nature. The second report of 22 April 2016 (limited circulation – 22 pages) was made up of two parts. The first part considered any added value of the collection resources HUMINT, SOCMINT and SIGINT in building up the information position and the manner in which the intelligence was shared. The second part related to a number of structural elements regarding how the Belgian intelligence services organise collection and analysis, as well as the associated risks. The results of both interim reports have been incorporated into this summary.

measures in time was also studied. Lastly, the Committee assessed how the two intelligence services reacted to the events in terms of 'organisation management' and which structural problems and risks arose. However, the Committee did point out in advance that the fight against terrorism and extremism takes place in a fast-evolving legal context.

II.3.2. FAST-EVOLVING LEGAL CONTEXT

Since the attacks in New York (2001), Madrid (2004) and London (2005), many European countries have had a very comprehensive range of preventive – but mostly repressive – measures against terrorism. Even so, this could not stop the attacks in Paris and later also in Brussels. The extent of the problem and the specific threat that it poses requires a targeted and streamlined approach. In that regard, the intelligence services form one of the links in the chain of legal enforcement in general, and the fight against radical Islamism, foreign fighters and returnees in particular.

Particularly after the Paris attacks, plenty of measures were adopted at various policy levels. The Committee asked itself whether this was being done on an adequately coordinated basis and/or whether the need for each measure could be demonstrated. The Committee here referred to the conclusion of an investigation into the effectiveness of the counter-terrorism measures adopted in Europe since 2001, which stated that a thorough evaluation of the measures is more imperative than the introduction of yet more new measures.[37]

II.3.3. INFORMATION POSITION OF THE SERVICES AND THE CONTRIBUTION OF THE VARIOUS COLLECTION RESOURCES

The Committee drew up a timeline for the main people involved, directly or indirectly, in the attacks[38] with the information relating to them that was available to State Security and GISS before 13 November 2015, regardless of the nature (correspondence, analytical memoranda, etc.) and the source (own collection, foreign service, other Belgian authority, etc.) of the information. The information position and how it was established was then briefly described on the basis of the following questions: When did each of them first enter the picture? What was known about this person (who, what, when, why and where)? Were SIM or other methods used? What information was exchanged with foreign services and how did

37 B. HAYES & C. JONES, *Report on how the EU assesses the impact, legitimacy and effectiveness of its counter-terrorism laws*, Statewatch, SECILE project, 2015, 59 p.

38 Initially ten people were designated as (co-)perpetrators by various sources at the time of the Committee's investigation. At a later stage of the investigation, this number increased to fourteen people and by the end it had been reduced to eight.

the interaction with the Belgian services and authorities take place? What possible relationships did the intelligence services establish between the persons involved?

II.3.3.1. Information position

State Security had been following most of the protagonists – some for a relatively long, others for a rather short period – and knew them either as criminals or radicalised persons. The only one who was clearly very dangerous was Abdelhamid Abaaoud, who is regarded as one of the leaders of the death squad. There were no prior indications that any of the others would take action. Likewise, it could not be inferred that they had formed an operational cell.

GISS only had information relating to Abaaoud before the attacks. He had entered the picture in 2013 on the fringes of another investigation.[39] When Abaaoud joined IS at the start of 2014, GISS tried to learn more about his activities abroad. As of the dismantling of the Verviers cell in January 2015, he became a priority for GISS. Although the service sent several Requests for Information (RFIs) to its correspondents, those did not produce any useful information. In November 2015, GISS learnt via its own collection resources that IS was determined to commit attacks in Europe. However, the service had no specific information about the date or place. Believing that the information was very important in this case, GISS distributed it almost immediately to the judicial authorities, its foreign correspondents and the National Security Council.

II.3.3.2. Use of the various collection resources

The following findings on the collection resources used by State Security and GISS (HUMINT, SIMs, SIGINT and SOCMINT) can be mentioned in this public report.

In relation to human intelligence (HUMINT):

- State Security had fragmented information from human sources on some of the people under investigation. Although some of those sources were described as being of 'high added value', they did not provide any concrete information in relation to the imminent attacks;
- Some of these sources were managed together with a foreign partner service;
- Well-placed human sources are scarce in the fight against terrorism. That means that a very limited amount of 'high value' human sources formed the basis of the bulk of the information in State Security's possession;
- State Security stated that a lack of personnel limited source processing in the sense that not enough time could be spent on maintaining contacts and searching for new sources;

[39] This is the case regarding Zerkani, who was convicted of terrorism offences in 2016 (also see II.3.4.4).

- GISS has recruited human sources within radicalised Islamic environments in Belgium and abroad.[40] As a result, this service can cooperate more often and exchange more information with certain foreign partners;
- In order to manage these sources – as well as to trace and analyse information via OSINT and SOCMINT (*infra*) – language skills and knowledge of immigrant environments are essential. State Security and GISS should therefore encourage diversity within their services;
- Better coordination between the various units that manage human sources within GISS is needed.

In relation to social media intelligence (SOCMINT):

- A SOCMINT unit was established within State Security in 2015. Its task was to monitor and look up sites, profiles and persons. But it could also cooperate in SIMs and with the HUMINT division;
- The SOCMINT information on the (co-)perpetrators, other than that on Abaaoud, contributed very little towards State Security's information position. However, the data did show that certain people were radicalised or strongly radicalised, although without any indications of concrete plans to commit attacks;
- The Committee was able to conclude that the importance of SOCMINT as a collection instrument is steadily increasing. Even so, SOCMINT is labour-intensive and difficult to manage in terms of the volume of information and its technical aspects;
- The Committee concluded that the capacity both State Security and GISS allocated to SOCMINT was rather limited, particularly in view of the fact that these services had to focus on more than just the phenomenon of terrorism. Far-reaching cooperation is essential to remedy this.

In relation to signals intelligence (SIGINT)[41]:

- Via the SIGINT division, GISS has access to information originating in other countries that have more far-reaching SIGINT capacities. In this way, it can also benefit from sharing international sources;
- Although the SIGINT department of GISS is mostly in possession of data or metadata that is often not linked to an identified person, it did have

40 GISS had no HUMINT regarding the above protagonists, other than Abaaoud, before the attacks of 13 November 2015. The HUMINT information regarding Abaaoud was not recent, voluminous or specific.

41 This refers to the power to intercept communications originating abroad. Only GISS has this power. Such interceptions are legally possible in the context of the military operation against IS (for example because of the presence of F16s), for the protection of Belgians abroad (mainly in the region concerned) and of the Belgian population as a whole.

documents that could be linked to two individuals who transpired on the list of names selected by the Committee;
– The SIGINT department has a unique capacity regarding foreign telephone numbers. Nonetheless, State Security rarely asks for help from this department. The Standing Committee I felt that structural cooperation should be established in this regard.

In relation to special intelligence methods (SIMs):

– The Committee found that State Security had used SIMs appropriately;
– Before 13 November 2015, State Security used special intelligence methods for three of the eight targets selected by the Committee (for the person involved or his environment).[42] Although this did not produce adequate information to prevent the attacks, the information gained from the SIMs was useful for confirming or negating information from other collection resources, supplying other avenues to explore or further developing or excluding investigative hypotheses;
– GISS did not use any SIMs in respect of the selected persons before the attacks;
– Phone tapping was often started because of a request made by a foreign correspondent, often in the context of a more general cooperation;
– People who were monitored regarding terrorism often seemed to realise they were being monitored and developed counterstrategies to evade it.

The Committee was of the opinion that State Security could not be accused of failing to use enough SIMs. The service made considerable efforts to try and gather intelligence.

However, the Committee did make one comment with regard to the possibility of improving the information position based on judicial information. After all, State Security was systematically asked to provide technical assistance in the judicial case files of the Federal Prosecutor's Office. As a result, the service had access to those case files that could also be a source of information. The Committee wondered whether State Security systematically made use of this collection option or opportunity.

II.3.3.3. (Internal and external) information flow

The quantity of incoming data arriving at the intelligence services from other sources, and of the information they collected themselves, was enormous. There was a risk that certain documents would be overlooked and/or would not feature

42 Obviously many SIM methods were used immediately after the attacks. The Committee has investigated those as well.

strongly enough during further handling and reporting. This could have resulted in a loss of substantive quality.[43]

The Standing Committee I investigated this on the basis of a few cases: the intelligence concerning Abdelhamid Abaaoud and Mohammed Abrini collected via HUMINT at State Security and the SIGINT information of GISS.

In relation to State Security, the Standing Committee I found little to no loss in terms of precision and completeness between the HUMINT information collected about Abaaoud on the one hand and the memoranda intended for other authorities on the other hand. What had been reported by the sources found its way outside, albeit it with varying speed.

A different picture emerged with regard to Abrini. HUMINT sources provided a lot of information, but State Security did not draft any external memoranda in this regard. The HUMINT information remained in-house, which of course does not imply that State Security did nothing with it.

The information that was collected by the SIGINT department of the military intelligence service had three addressees: GISS itself, Belgian partner services and foreign SIGINT partners. The SIGINT documents intended for internal use were generally very detailed. The documents for State Security and/or the judicial authorities were generally less detailed and complete.[44] There was thus a loss in terms of precision and completeness of the forwarded intelligence. However, the Standing Committee I could not determine that this involved crucial information *in casu*. Since raw SIGINT information is in principle never sent to external partners, it requires processing and thus takes some time. But if crucial information has to be sent completely and urgently to a partner service, an exception may be made.

II.3.3.4. Analysis of the collected information

Analysis forms an essential component of intelligence work. Although there are various methods for structuring the analysis, the services did not take sufficient advantage of them. The Standing Committee I stressed that this did not stop the services from sending out the necessary warnings when needed.

---

43 The Committee was able to determine that a message State Security received from abroad in mid-2015 regarding IS's potential terrorist plans referred to contacts that the foreign fighters had in 'Molenbeek', while the report to the Public Prosecutor's Office in that regard referred more generally to 'Brussels'. The Committee also established that a report that GISS received in the summer of 2015 was not distributed any further. This report referred to a military unit that had been used to provide assistance to the police, and which believed it had spotted Abaaoud in the Brussels region while everyone thought he was in Syria at that moment. However, the military unit also sent the report to the police.

44 At the end of October 2015, for example, a very detailed document about two supporters of Abaaoud was drawn up for internal use. The memorandum that was sent to State Security in this regard was a lot less explicit. A number of reasons were given for this relating to specific SIGINT operating rules that require, for instance, that raw information be stripped of data that could reveal the source of the information.

One important method is creating possible scenarios and making hypotheses that can be confirmed or negated. For example, State Security had long hypothesised that foreign terrorist fighters (FTFs) planned to settle in the upcoming Caliphate permanently or to die there, and did not intend to return. As a result, the impact of the phenomenon on European soil was generally underestimated at first, although State Security did initially, for a very short time, work from a worst-case scenario. Scenarios like this are important because they provide a starting point in order to subsequently determine via indicators which direction the scenario is heading in. They are important methodological instruments that could be applied more.

However, the Standing Committee I believes that creating such scenarios should preferably be a multidisciplinary effort. As there are several components to a terrorism scenario – both civil and military – State Security and GISS could have cooperated in this regard, which may have led to better results. In other words, it is not because GISS initially considered itself largely unauthorised to act with regard to 'civil' FTFs that it could not have made a useful contribution in this case.

Lastly, the Committee stated that there must be a connection between the collection and the analysis: both must feed and be in balance with each other. This is why the Committee emphasised the importance of a coordinating or 'umbrella' intelligence design for a specific phenomenon, concrete threat or target. In principle, this design should exist not only within each service, but also take into account – and ideally use – the collection and analysis capacities of other services. This is the approach taken in the Memory of Understanding (*infra*) that was drawn up after the attacks.

II.3.4. COOPERATION AT NATIONAL LEVEL

II.3.4.1. Cooperation in the context of the local task forces (LTFs)

The Committee made the following findings regarding the operation of local task forces.

- LTF participants must inform each properly about their needs, requirements, capabilities and limitations. In this way, a mutual understanding of what LTFs can and cannot deliver can be developed;
- In relation specifically to State Security, it was not always clear to the participants what information could be shared. The Committee recommended that the services create internal certainty in this regard and that representatives from the provincial services who participated in the meetings also be actively supported and guided by central management;

- The intelligence services always had to check the appropriate classification level of specific information because not all LTF participants had the required security clearance at the time of the review investigation;
- GISS participated less in LTFs than State Security. The service cited its staff shortage as the reason. GISS suggested that it could be represented in LTFs by State Security. The Committee felt that this working method could be considered, provided that the mutual expectations and procedures for exchanging information were properly recorded;
- As the protagonists of the attacks were located mainly in Brussels, the LTFs in other judicial districts could only contribute limited information.

II.3.4.2. Cooperation in the context of the Radicalism Action Plan (Plan R)

In relation to the functioning of Plan R, the Committee referred in the first instance to the Joint Information Box (JIB). The Standing Committees I and P were already investigating this list of radicalisation vectors managed by CUTA. The investigation mainly showed that the JIB was not very efficient during the investigated period and generally (and mostly only) led to a police description.[45]

Besides the JIB list, reference was also made to various thematic and *ad hoc* working groups that were created for the purpose of Plan R. State Security and GISS formed part of (most of) these working groups. Given the deadline by which the investigation had to be completed, the Committee could not consider the contribution of these groups towards monitoring FTFs.

II.3.4.3. Cooperation between State Security and CUTA

Cooperation between both intelligence services ought to be optimal and effective. The Committee previously found that cooperation could be improved and made several recommendations in that regard.[46] The results of this investigation suggested that the situation before and at the time of the Paris attacks was still not optimal. After all, the Committee made the following findings:

- The bilateral meetings between State Security and GISS with a view to exchanging operational information were few and far between. Contact was obviously possible on other occasions (e.g. within the context of LTF meetings);
- Only a limited number of documents were exchanged between the intelligence services for the purpose of the fight against terrorism;

---

45 The Committee referred in this regard to that investigation and the recommendations it made at the time. STANDING COMMITTEE I, *Activity Report 2015*, 107–111 ('II.1. Joint supervisory investigation into the Joint Information Box of CUTA') and 170–171 (IX.2.1. Recommendations on the Joint Information Box).

46 STANDING COMMITTEE I, *Activity Report 2014*, 92 ('IX.2.2. Closer cooperation between the two intelligence services').

– GISS had difficulty in defining its role in the fight against terrorism, which meant that the different partners did not really know what to expect;
– Lastly, the Committee pointed out that the problems in relation to information management that were found at GISS[47] kept it from cooperating with its partners, including State Security.

II.3.4.4. Cooperation with the judicial authorities and the police[48]

The Committee established the following with regard to cooperation with the police and the judicial authorities:

– Although there was plenty of contact and various forms of information exchange existed between the services (particularly between State Security and the Federal Police), this produced few concrete results in relation to the investigated persons;
– State Security and the police cooperated well in the autumn of 2015 in observing one of the protagonists, with the goal of verifying very specific intelligence;
– As confirmed below (II.3.6.1), State Security issued important warnings at certain times, including to the judicial authorities and the police;
– The Committee noted the role of GISS particularly in the opening and handling of the judicial case file on Zerkani.[49] After all, it was a memorandum from GISS that first alerted the judicial authorities to the presence of a group of radicalised individuals in Molenbeek;
– The Committee found that, as of 2015, GISS had usually complied with requests from the Federal Prosecutor to provide technical assistance. GISS explained it did this to gain access to the case file and thus improve its knowledge about the foreign terrorist fighters.

47 STANDING COMMITTEE I, *Activity Report 2010*, 84–85 ('IX.2.12. An effective information management system for GISS') and *Activity Report 2011*, 104–105 and 174–175.

48 There are a host of rules that govern cooperation and the exchange of information between intelligence services, the police and judicial authorities: Article 29 of the Belgian Code of Civil Procedure (BCCP), Articles 19, 19/1 and 20 §2 of the Intelligence Services Act, circulars COL 9/2005 of the Board of Procurators General concerning the judicial approach to terrorism, COL 9/2012 of the Board of Procurators General governing the intelligence and security services – cooperation between State Security/GISS and the judicial authorities, and COL 10/2015 of the Board of Procurators General relative to the judicial approach to foreign terrorist fighters, and the Circular of the Ministers of the Interior and Justice of 21 August 2015 on the exchange of information relating to and the monitoring of foreign terrorist fighters from Belgium. After the Paris attacks, a Memorandum of Understanding was also drawn up between GISS, State Security, CUTA and the Federal Judicial Police of Brussels. This provided for regular and structural consultation as part of the fight against terrorism, in order to reach a common information position.

49 This individual was convicted together with a number of others by a judgment of the Brussels Court of Appeal on 14 April 2016. However, he was not one of the protagonists who formed part of the investigation.

II.3.4.5. Cooperation with CUTA

Under Article 6 of the Threat Assessment Act, State Security and GISS are obliged, as support services, '*to communicate to CUTA, at their own initiative or at the request of the Director of 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°*' (free translation). It should be noted that State Security has always interpreted this to mean that only processed intelligence and not raw data should be sent.

Both State Security[50] and GISS have two permanent experts seconded to the coordination unit. They also act as liaison officers.

II.3.4.6. Cooperation with the Immigration Office, the Commissioner General for Refugees and Stateless Persons and Fedasil

Cooperation between State Security and these services has already existed for some time and is not limited to terrorism. State Security has a permanent liaison officer at the three services. These positions became especially important because of the massive migration problem that arose during the summer of 2015, when State Security was asked to attend to the screening of all asylum seekers.[51]

GISS has also maintained contact with the three services for some time, and recently designated a contact person to centralise the exchange of information.

II.3.4.7. Cooperation with the Directorate-General of Penal Institutions

The Standing Committee I had previously investigated the cooperation between State Security and the penal institutions,[52] finding that State Security had established a 'GP' ('Gevangenissen/Prisons') unit in mid-2015. This unit processes a lot of information relating to radicalisation and terrorism.[53]

---

50 In order to optimise the flow of information with CUTA, State Security designated a contact person internally, after the Paris attacks, who is close to management and maintains regular contact with the expert seconded to CUTA.

51 Some 17,643 people underwent screening in the period from 7 September 2015 to 11 May 2016. 82 of them were known in State Security's database, 15 of those for radicalisation. Barely six investigations were opened into individuals with potential links to IS, but none of the investigations found any connection to the perpetrators of the Paris attacks. According to State Security, this fairly significant investment only produced a limited result.

52 See 'II.5. State Security and the cooperation protocol with Penal Institutions' of this activity report.

53 At the time of the investigation, the Standing Committee I found that it was not possible to process all the data due to the mass of information.

II.3.4.8. Cooperation with the operational units of Defence

Specifically in relation to GISS, the Committee referred to the links between the intelligence services and the operational units of the army whose task, in support of the police, was to ensure public safety. As these units were widely deployed, they could obviously pick up and report on information from the field (e.g. suspicious events that they witnessed). For example, an operational detachment reported the possible presence of Abaaoud in Belgium in the summer of 2015. This information was reported to the police and, via the military chain, to GISS.

Given its tight deadline, the Standing Committee I could not investigate this information flow and how GISS performed its primary task in relation to the force protection of the army units deployed in the field (see II.4.3.3).

II.3.4.9. Cooperation with the Governmental Coordination and Crisis Centre (GCCCR)

Lastly, although State Security and GISS also had numerous contacts with the Crisis Centre, these did not relate exclusively to terrorism but also, for example, to general public safety (demonstrations). State Security has a permanent liaison officer at the CGCCR.

II.3.5. COOPERATION AT INTERNATIONAL LEVEL

Article 20 of the Intelligence Services Act provides that the intelligence services are responsible for collaboration with their foreign counterparts. The manner in which State Security and GISS implemented this provision will be summarised below.

II.3.5.1. State Security's international cooperation

State Security is part of different multilateral cooperation platforms (Club of Bern, Counter Terrorist Group (CTG), etc.) and cooperates with other services on both an operational level (e.g. exchange of information) and analytical level in the context of those platforms. Policy decisions are also sometimes prepared in the broad area of national and international security. Although operational cooperation is usually at a bilateral level, there was also intense, multilateral cooperation in relation to the fight against terrorism in the field.

There are also forums that are not specifically aimed at intelligence services but that play an important role in the fight against terror (e.g. Europol, NATO, etc.). State Security has a permanent liaison officer in certain forums.

At the time of the investigation, State Security had bilateral contact with services from more than seventy different countries. The intensity and frequency of the cooperation differed significantly. In relation to the fight against FTFs, the most intense relationships were with our neighbouring countries and some non-European countries close to the conflict region.

One of the advanced forms of bilateral cooperation is the exchange of liaison officers. Although State Security had tried to attain this form of cooperation with the French sister service for a considerable time, this only occurred effectively after the Paris attacks.

State Security also formed part of a working group of European and non-European partners that was specifically created to focus on Abaaoud shortly before the attacks. The working group never met prior to the attacks.

The parallel hypotheses on planned attacks in Europe in which Abaaoud would purportedly play a main role mobilised fifteen foreign services, which collectively had significant resources. State Security received a lot of intelligence in this context, although most of the people who were not known to State Security turned out be mainly unknown to the multitude of foreign services as well.

State Security also disseminated information in its possession, or asked partners to complete its own data. The international effects in the summer of 2015 yielded a limited result: from the stories of three terrorists who were detained in three different countries, it was clear that the threat against Europe was very serious.

There has been extensive message traffic since mid-August 2015: State Security receives many memoranda with intelligence or requests for intelligence. State Security gave or requested a lot of information from the partner services itself.

It could be concluded from the above that there was an intense exchange of information and no indication that State Security did not share certain data.

II.3.5.2. GISS's international cooperation

GISS is also a member of various multilateral cooperation platforms. For example, as of August 2015 the service participates in a platform that ensured the monitoring of the social media activities of IS members and sympathisers. GISS also participated in international groups that worked around a counternarrative with a view to neutralising the IS propaganda that was being spread via the internet and social media.[54]

[54] In the days following the Paris and Brussels attacks, GISS developed a close, bilateral cooperation with a number of European and non-European partners. The Committee also found that GISS cooperates with both civilian and military intelligence services.

II.3.6. WHEN AND HOW DID THE INTELLIGENCE SERVICES INFORM THE COMPETENT AUTHORITIES OF THE THREAT?

During the summer of 2015, the services received a number of important signals that made it clear there was a growing terrorist threat specifically aimed at Europe. The Committee investigated whether and how State Security and GISS warned the competent authorities of this, including how the services had acted in previous years. A distinction was made among four periods.

In November 2012, the first known Belgian national left for the Syria region. Islamic State of Iraq and the Levant (ISIL, later IS) was formed during that period.

A new period started as from the autumn of 2013 with the first returnees. Without there being any specific indications, it was clear they could constitute a threat.

The attack in May 2014 on the Jewish Museum in Brussels, the declaration of the Caliphate by IS in June 2014, and the call to carry out attacks marked the start of another new period. It was at this time that Belgium also joined the international coalition deploying military personnel against IS.

A fourth and last period started with the Charlie Hebdo attack and the dismantling of the terror cell in Verviers in January 2015. This cell was partly managed from abroad (with Abaaoud as the central figure). This period was characterised by the fact that candidate terrorists, trained by IS, were infiltrating Europe. A number of them were arrested and revealed plans against France, Belgium and Germany. Just before the Paris attacks (August 2015), there was the failed attack on the high-speed Thalys train.

II.3.6.1. State Security

The Committee was able to determine that State Security detected a growing terrorist threat and issued warnings at key moments.

In the first period, mostly characterised by those leaving for Syria, State Security adopted a wait-and-see attitude. This did not mean, however, that the service did not pay attention to the problem. On the contrary, a memorandum was sent to the political authorities as early as October 2012 to draw their attention to the contingent of foreign fighters in Syria. The warning was already given then that fighters could return to commit attacks. The service thought this would be in the form of lone wolves rather than organised groups.

During the transition from the second to the third period, State Security increasingly sent warnings to the competent ministers. Briefings were also organised in which the problem of returnees was discussed, without there already being any explicit mention of possible attacks in the West.

By the end of the third period – when the threat had become real – very few or no memoranda were sent to the (new) ministers. State Security explained this was because many of the case files had been continued under judicial management since the operation in Verviers.

In the period prior to the attacks, State Security issued two important warnings, referring to possible attacks in France, Belgium and Germany.

The Standing Committee I therefore concluded that State Security had tried to react adequately to the impending threat. State Security realised at a key moment that the threat was real (first those who left, subsequently the threat of returnees) and issued several warnings.

II.3.6.2. General Intelligence and Security Service

The Committee investigated whether GISS had issued the proper warnings at the right time as well. Obviously the fact that GISS was not immediately involved in the problem of the civilian contingent of foreign fighters in Syria must be taken into account. In principle, the service was only authorised to act in case of threats involving military or ex-military personnel, or if military interests were concerned (such as the protection of troops or military installations).

Division SI of GISS had been monitoring Islamic terrorism for a long time. Since 2011, this became a priority and special attention was paid to individuals who were linked to this problem, in Belgium or abroad, and could constitute a threat to Belgian military interests.

During the first period, GISS's reporting was limited to providing intelligence within the military chain for the purpose of force protection, domestically and abroad.

In May 2013, GISS established a Joint Terro service. It was only after Verviers that GISS described its authority in broader terms after a meeting with the National Security Council and also entered 'civilian' terrain. GISS issued a number of significant warnings from that time. The intention was not only to have insight into radicalism within the army in Belgium itself, as well as the terrorist threat against troops in operational theatres (Afghanistan and Lebanon), but also to identify extremist Islamic networks and phenomena in a far wider region and context. This arose from the realisation that terrorism would not necessarily remain in Syria. The Standing Committee I felt that this was a justified reaction.

In February 2015, GISS briefed the National Security Council on the threat posed by IS to Belgium.

A week before the Paris attacks, GISS distributed very important intelligence about an imminent attack.

II.3.7. HOW DID THE SERVICES RESPOND TO THE EVOLVING THREAT?

The Standing Committee I tried to answer the question of how the two intelligence services reacted as an organisation to the growing terrorist threat and whether they adapted their structures or work processes. The Committee considered the problem on the basis of the four aforementioned periods.

II.3.7.1. State Security

By establishing the 'Syria Task Force' in the spring of 2013, State Security focused on the problem of the foreign fighters. The operational work remained exploratory, given that the threat had only just started to materialise and was situated far from Belgium. State Security also participated in a newly established international working group.

Internal procedures were adapted from the second period in the sense that there was closer cooperation between the collection and analysis services in the fight against extremism and terrorism. From the end of 2013, the SIM figures showed that the service's attention had shifted to Syria-related terrorism.

By the end of the third period, plans were made for a comprehensive reorganisation. These structural adaptations formed part of the draft 2015 Action Plan, drawn up in the spring of 2014, in which the fight against terrorism was considered to be the main priority. During the same period, work was also done to improve cooperation with prison administrations and boost SOCMINT capacity,

In the period prior to the attacks in Paris, the 2015 Action Plan, which the National Security Council had approved in June and for which the government had made resources available, was implemented. This reorganisation obviously took time, partly because the reform coincided with the events in Verviers and the failed attack on the high-speed Thalys train. State Security deployed a lot of resources during the last period to search for terrorist elements, but without decisive success.

II.3.7.2. General Intelligence and Security Service

In relation to GISS, the Standing Committee I believed that there was initially no need for major structural changes due to GISS's limited authority.

At the start of the second period – when it became clear that returnees could form a real danger – GISS implemented a structural change. After Verviers, new objectives were documented and the powers were described in broader terms (*supra*). The Standing Committee I felt that this was a justified reaction, even though execution remained difficult due to limited resources.

During the third period, GISS adjusted its priorities and also strengthened international cooperation at SIGINT level. At the end of 2014, it was proposed that more collection resources be used in order to be able to permanently gather intelligence on jihadist terrorism. During the same period, Belgium decided to participate in the international coalition against IS. Through this participation, GISS gained access to information from other partners in the conflict zone.

The fourth period was a key moment for GISS. Its own authority, described as 'military' up to that point, was interpreted in broader terms. GISS would from then on also focus on threats with 'military resources' even if those were carried out by non-military personnel or aimed at non-military targets. GISS also engaged in increased international cooperation, making use of the opportunities offered by the international military developments.

II.3.8. SEVERAL STRUCTURAL PROBLEMS AND RISKS

The Standing Committee I referred to a number of structural problems that arose at the services and their associated risks. At State Security, it was the increase in work pressure; at GISS the problematic situation of data management was pointed out again.

II.3.8.1. Increased work pressure and incomplete reorganisation at State Security

During the course of its investigation, the Committee noted a significant increase in work pressure within State Security, obviously mostly in the fight against terror: more data was being processed, urgency was greater, the threat had increased. On the other hand, the service had 15% fewer employees in 2015 than it had in 2010.[55] There was also the problem of overtime and of holidays not being taken and the fact that although absenteeism due to illness was on the decrease, it was still higher than the federal average. The Committee therefore insisted on a quick transfer of State Security's Close Protection Service to the Federal Police.[56] After all, this would free up some twenty inspectors for intelligence work.[57] Based on the same concern, the Committee referred to the problems that complicated the recruitment of new personnel.

The Standing Committee I was able to conclude that the internal reform of State Security at the level of the collection services was complete. This was not the case for the analysis services at the time of the investigation. This meant that there was no parallelism between the collection – which focused on the subject

55 At the start of 2016, there was a noticeable increase in personnel again due to the Government's decision during the course of 2015 to recruit new inspectors and analysts.

56 STANDING COMMITTEE I, *Activity Report 2014*, 45 *et seq.*

57 This transfer took place.

matter – and the analysis – which still had a geographical focus. That complicated the cooperation. Physically bringing together the collection and analysis services, in order to improve communication between them, was not fully implemented either, which complicated the cooperation as well.

II.3.8.2. Information management at GISS

The Standing Committee I repeatedly pointed out that information management at GISS was a problem.[58] GISS command had also raised this issue on several occasions.

The investigation showed that GISS's own production of intelligence in relation to the protagonists of the Paris attack was limited. This was explained by the fact that GISS focuses in the first instance on military threats, or on threats involving military personnel, and that the perpetrators did not fall within these categories.[59] But there was also another explanation. During its investigation, the Committee namely came across information that was available within the service but could not immediately be found. The Committee therefore had to conclude, once again, that information management within GISS was problematic. After all, the system did not enable all of the available data to be found with certainty.

Although GISS had a simple and modern system that showed relationships between data and had the necessary options to manage the flow of information within an intelligence service, the system was not or hardly used due to a lack of personnel to perform the necessary encoding and due to a lack of training necessary to use it. To summarise, the Committee concluded that information flow management constituted a risk for the overall intelligence process at GISS.

II.3.9. GENERAL CONCLUSIONS

The efforts of the intelligence services did not lead to the timely detection of a cell that had ties with Belgium and was able to carry out large-scale attacks. Moreover, Abaaoud could not be tracked down in time, despite intensive cooperation among almost twenty European and non-European services.

On the other hand, the Standing Committee I could not ascertain any manifest failings in the way in which the two intelligence services tried to fulfil their respective duties prior to the Paris attacks. There was no indication of certain information being withheld from the (foreign) partners.

---

58 STANDING COMMITTEE I, *Activity Report 2011*, 104–105 and 174–175.

59 A change was made only after the events in Verviers: it was clear that the intelligence services were dealing with people who signed up to the 'military strategy' of the IS terror group. From that stage, Abaaoud in particular was clearly a legitimate target, also for the military intelligence service.

However, this does not alter the fact – as in the investigation into the monitoring of FTFs (see II.1) – that the Committee felt there were many aspects that could be improved (see XI.1 and XI.2.1).

II.4. INFORMATION POSITION OF THE TWO INTELLIGENCE SERVICES BEFORE THE ATTACKS IN ZAVENTEM AND MAALBEEK

II.4.1. SUMMARY OF THE FACTS

Since the outbreak of civil war in Syria in 2011, hundreds of Belgians have participated in this conflict. At one stage, Belgium was the European country with the largest number of foreign fighters in Syria per inhabitant. But the battleground has moved since 2015–2016. IS has been carrying out terrorist attacks worldwide.

Belgium has also been targeted. In January 2013, the media reported on residents of Brussels who had left for Syria and threats of an attack on the capital city. On 24 May 2014, Mehdi Nemmouche shot and killed four people in the Jewish Museum in Brussels. He was a returned Syria fighter. This was followed by Charlie Hebdo, Lyon, Paris… all with clear links to Belgium.

After the Paris attacks, an (international) manhunt, involving all police and intelligence services, was organised to find the remaining perpetrators. One of the perpetrators was Salah Abdeslam. He purportedly forced his way into the French national stadium, *Stade de France,* wearing an explosive belt, but had second thoughts. He fled in the direction of Belgium, where he disappeared without a trace. The threat level was at level 3: the threat was serious, possible and likely. Some cinemas closed their doors, while terror experts paid particular attention to nuclear power stations, etc.

On 15 March 2016, the counter-terrorism unit of the Federal Police conducted a search of an apartment in Vorst as part of the investigation into the Paris attacks. The agents expected to find the apartment empty, but were immediately fired at by gunmen. Four of them were wounded. During the raid by special units, a suspect in possession of a Kalashnikov was killed. This later proved to be Mohamed Belkaid, who had previously only been known under his alias Samir Bouzid. Two other suspects took flight. From traces left behind, it could be concluded that the suspects were probably Salah Abdeslam and Amine Choukri, who also had a false Syrian passport under the name of Ahmed Monir Alhay. The investigation continued around the clock.

Three days later, on 18 March, Salah Abdeslam was arrested in a safe house in Molenbeek. Amine Choukri, whose real name turned out to be Soufiane Ayari, was detained with him.

On 22 March 2016, suicide bombers Ibrahim El Bakraoui and Najim Laachraoui (alias Soufiane Kayal) blew themselves up in the departure hall of Brussels Airport. A third terrorist was also present: Mohamed Abrini left behind his trolley with explosives and left the airport on foot.

Three quarters of an hour later, a surveillance camera filmed Khalid El Bakraoui – brother of Ibrahim – and Osama Krayem (alias Naïm El Hamed) at a ticket machine in the Brussels metro station Petillon. The underground Brussels-National-Airport train station had meanwhile been closed. The threat level was raised to level 4: the threat was very serious and imminent. At around 9 a.m., the order was given to evacuate the Brussels metro stations and five train stations. The federal phase of crisis management was announced and the national emergency plan for a terrorist attack was activated. However, this could not prevent suicide bomber Khalid El Bakraoui from blowing himself up at 9.11 a.m. in a metro train that had departed from Maalbeek station towards Kunst-Wet.

Both atrocities were suicide attacks, in which the perpetrators blew themselves up in a crowd using home-made explosives (nail bombs concealed in suitcases). The consequences were enormous: 35 people died and more than 300 were wounded.

Some of the perpetrators were foreign terrorist fighters (FTFs) with links to the terror group Islamic State (IS). IS claimed responsibility for the attacks on the same day and subsequently cited various reasons (capital of the European Union, participation in the Syria attacks, the detention of Malika El Aroud and Salah Abdeslam, the ban on wearing the hijab, etc.).

A link to the Paris attacks was quickly established: Najim Laachraoui was confirmed as having been in the company of Salah Abdeslam; his DNA was found on the explosive belt used in the Bataclan, a Paris concert hall. Immediately after the attacks, State Security stated that it was steadily becoming clearer that the Brussels attacks were an extension of the Paris attacks. After all, both were attacks for which IS claimed responsibility, prepared and executed partly by the same people, and whose preparation (and execution) followed similar patterns.

Mohamed Abrini, who had been sought since the Paris attacks, was detained in Anderlecht on 8 April 2016. Osama Krayem was arrested on the same day in Laken, as was the Rwandan Hervé Bayingana-Muhirwa. The latter was suspected of having helped Abrini and Krayem to hide out after the attacks. Bilal El Makhouki – who was convicted in 2015 during the Sharia4Belgium proceedings – was also arrested.

On 11 April 2016, Ibrahim Farisi was detained together with his brother Smail. Ibrahim Farisi was the tenant of the apartment in Etterbeek from which the perpetrators of the attacks on the Brussels metro had departed. He rented the

apartment in order to receive a benefit from the Public Centre for Social Welfare, but allowed Khalid El Bakraoui to use it.

Ali El Haddad Asufi, who was thought to have played a logistics role in the preparation of the attacks, and Youssef El Ajmi, a childhood friend of Khalid El Bakraoui and Ali El Haddad Asufi, were also arrested. The investigation also led to the apprehension of Jawad and Mustapha Benhattal and Samir Chahjouani on 17 June 2016.

A few months after the attacks, Oussama Atar (alias Abou Ahmad), a cousin of the El Bakraoui brothers, also came on the radar as the possible mastermind behind them. Atar had previously been imprisoned in Abu Ghraib. He remained in Iraqi prisons until 2012, but was released early after Amnesty International and the Belgian government requested Iraq to hand him over to Belgium on humanitarian grounds. Atar then disappeared without a trace. He was thought to be a leader of the contingent of foreign fighters in Syria.[60]

II.4.2. STRUCTURE OF THE REVIEW INVESTIGATION

The investigation followed the same patterns as those after the Paris attacks (II.3).[61] After the offences, the Standing Committee I immediately noted the names of people who were involved in the attacks as (suspected) perpetrators or co-perpetrators.[62] First the information position prior to the attacks in Brussels was outlined with respect to these selected persons. The 'collection disciplines' (HUMINT, SOCMINT, SIGINT and SIM) were then examined further. The cooperation of the services with their partners and correspondents, both nationally and internationally, was also considered. Lastly, the activities that State Security carried out in the period immediately prior to the attacks were also described.

---

60 The name of Yassine, Atar's younger brother, also came up during the investigation. He was arrested and traces of explosives were allegedly found on his fingers.

61 The review investigation '*into the information position of the two intelligence services prior to the morning of 22 March 2016 regarding the individuals or groups that carried out or were involved in the attacks in Brussels and Zaventem, as well as regarding the individuals or groups that allowed Salah Abdeslam to go underground until his arrest on 18 March 2016*' (free translation) was opened on 20 July 2016. The final report is dated 4 November 2016. In view of time restrictions, the Committee could not study all aspects of the problem in this investigation. The Committee considered the following themes in this regard: which leads were possibly missed by the intelligence services, how were the services controlled by their respective managements, how was the cooperation between the relevant police and intelligence services, how did the crisis management at State Security work in relation to the practical approach to the attacks of 22 March.

62 Other possible involved persons only became known later, including Ali El Haddad Asufi, Youssef El Ajmi, Jawad and Mustapha Benhattal, Samir Chahjouani, as well as Oussama and Yassine Atar.

II.4.3. INFORMATION POSITION OF THE INTELLIGENCE SERVICES

II.4.3.1. State Security

The Committee first drew up a list of the documents in possession of State Security containing the name (or alias) of the (selected) perpetrators/co-perpetrators for the period from the Paris attacks to the Brussels attacks. The figures varied from several to many hundreds of documents. The Committee also noted when a perpetrator or co-perpetrator was first noticed by State Security, and when the service last received or processed information about them (prior to 22 March 2016). The Committee then drew up a timeline for each of the perpetrators/co-perpetrators, showing the information flows and describing the information position and how it evolved. Attention was also paid to the 'source' of the information (own collection, for instance via SIM, information from Belgian or foreign services, etc.).

The investigations of the Standing Committee I showed that great efforts had been made to trace Abrini and Abdeslam since the Paris attacks. Significant resources were deployed both nationally and internationally: in relation to Abdeslam, State Security was in contact and exchanged information with 27 foreign services on four continents, while 12 foreign services were involved in the hunt for Abrini. The timeline clearly showed how the intensity of the information flow gradually decreased from February 2016.

However, special intelligence methods were still used in relation to Abrini until just before the attacks. In hindsight, based on Abdeslam's known contacts that were connected to the Brussels attacks, the conclusion could be reached that it was possible to link the names of those involved to each other prior to the attacks. However, this was not obvious. After all, many of the perpetrators/co-perpetrators used aliases and could only be identified late (or only after the attacks). By way of example, in one specific case, there was an assumption that two different individuals were involved, while in fact this was one and the same person. This made it very difficult to build up a thorough information position.

Laachraoui and Belkaid caught the attention of State Security in September 2015 because they were spotted together with Salah Abdeslam. It was then clear within the international intelligence world (and at State Security) that they formed part of the same network. However, their true identities were not known at the time. Najim Laachraoui had false identity documents in the name of Kayal. Belkaid had a false identity card in the name of Bouzid. They could remain in hiding that entire time.

State Security had been aware of the El Bakraoui brothers since December 2015, although initially only with a criminal profile. This changed after the raid

in Vorst, when it became clear that Khalid had rented the safe house under an alias.

Osama Krayem – alias Naïm al Hamed – was the person with the rucksack who had contact with El Bakraoui shortly before he blew himself up in the Maalbeek metro. He was also involved in the preparations for the Zaventem attack and had entered Europe via Greece under a false identity as a Syrian refugee. Krayem was not known to State Security under his true identity until the raid in Vorst, when false documents of his were found.

Prior to the attacks of 22 March 2016, Farisi, Bayingana Muhirwa, Ayari[63] and El Makhouki were not priority targets for State Security. However, it transpired that some of them had provided assistance. For example, Farisi actively participated in helping to remove evidence from a safe house and Bayingana Muhirwa gave shelter to fugitives. The specific role played by the others was not known at the time the review investigation was closed.

II.4.3.2. General Intelligence and Security Service

GISS only had the names of four perpetrators/co-perpetrators in its files, namely Salah Abdeslam, Mohammed Abrini, Najim Laachraoui and Khalid El Bakhraoui.[64] The Committee also established that the military intelligence service had no information on these four people from their own collection methods (*infra*). The available information came from national and international partners and the national and international press. Most of the available information was SIGINT information from foreign partners. This information mostly related to the Paris attacks.

In view of the scarce information – which moreover only involved four perpetrators/co-perpetrators – it must be concluded that GISS had a poor information position.[65] The Standing Committee I was surprised about this because GISS prioritised the monitoring of jihadist terrorism and had/has played a role[66] in relation to force protection regarding the military personnel who carry out surveillance operations in Belgian cities, in addition to the police.

---

63 State Security knew that Soufiane Ayari had been picked up by Salah Abdeslam in another European country prior to the attacks. False identities were used in this case as well.

64 The other perpetrators/co-perpetrators only came to GISS's attention after the Brussels attacks.

65 The Head of GISS expressed himself in the same terms in his report that was drawn up for and addressed to the parliamentary inquiry committee into the 'attacks'. GISS stated that it could largely agree with the conclusions of the Committee's report. The service once again drew attention to a dire shortage of staff.

66 Earlier investigation showed that the Intelligence Services Act provided three grounds for gathering and processing data on foreign terrorist fighters. In this regard, see: 'Chapter II.1.2.2. General Intelligence and Security Service'.

II.4.3.3. A special information flow within defence: Operation Vigilant Guardian

Since January 2015, military personnel has been patrolling a series of strategic buildings. The number increased in line with the threat level from 150 to more than 1,800 units. The purpose of this *Operation Vigilant Guardian* (OVG) is to support the Federal Police.

As in the case of operations where troops are deployed abroad, certain intelligence aspects also arise during these domestic operations. In addition to surveillance and security activities, the deployed military personnel fulfil the role of 'sensor': they observe and report on events and incidents. This 'intelligence activity' normally involves the relevant military personnel being given a detailed or summary briefing of the environment beforehand, with information regarding what to expect and what they need to pay attention to. It is important that they also issue a report during or after the mission within the military chain to specially designated officers ('G2') within their unit. The information is then forwarded to GISS. However, different procedures have been created for the purpose of the OVG. Deployed military detachments – who are under the operational leadership of the Federal Police in the field – report in the first instance to the police.[67] The information is simultaneously reported to the Defence Staff (C-Ops) as well, which coordinates and monitors all operations. However, contrary to what happens in foreign operations, the information is not dealt with substantively within the operational units (by 'G2' officers) or at central level (C-Ops). A copy of the information is sent from C-Ops to GISS, which registers it. In principle, GISS analysts have access to the information from that time.

The Standing Committee I went through all the reports drafted by the military detachments deployed to Brussels and Zaventem between 13 November 2015 and 22 March 2016. This involved 24 documents. The Committee was able to determine that GISS received these reports via C-Ops, but did not substantively process them.[68] The military intelligence service believed that the Federal Police were responsible for processing these reports. The Standing Committee I did not share this view: GISS is not released from the obligation to verify whether documents sent to it contain information that could concern the service. GISS also stated that it was not involved in preparing military personnel for their OVG assignments and did not have any insight into the quality of the reports.

---

67 Defence has assigned a liaison officer to the Federal Police, whose tasks include drawing up a synthesis report for the police from the information reports drawn up in the context of the OVG. The Standing Committee I was unable to investigate whether and how the police put these synthesis reports or the initial field reports to a specific use. This was outside the scope of its powers.

68 GISS stated that it would recommend to the Defence Staff to include the procedure to be followed in the relevant operational plan of the Chief of Defence (CHOD).

The Standing Committee I was able to conclude from three cases that the information flow from the field, as part of the OVG, was questionable in the sense that the information did not reach all sections and potentially involved services.

For example, at the beginning of March 2016, two reports referred to the possible presence of one of the later perpetrators at Zaventem Airport. One of these reports was based on information from the military personnel of a battalion that specialises in intelligence gathering.[69] An earlier report of November 2015 referred to a person who was filming a military security device from a car. The person concerned had his face covered. GISS did not deal with or send any of these three reports to State Security[70] or CUTA.[71]

The Standing Committee I believes that OVG detachments can undoubtedly make a valuable contribution from the perspective of intelligence gathering. The deployed military personnel do not only supply information; they also need intelligence to do their job properly and to be able to adequately protect themselves. GISS has authority to act here as well, in the context of force protection.

II.4.4. COLLECTION RESOURCES

II.4.4.1. State Security

The Committee could clearly conclude from the higher number of reports drafted that State Security had activated its sources (HUMINT) after the Paris attacks.

In response to the attacks, the intelligence services and Federal Police reactivated the social media working group within Plan R. This working group, comprising the SOCMINT units of the police, GISS and State Security, aims to improve cooperation.

In the period between the two attacks, State Security's SOCMINT unit drew up 15 reports on the perpetrators/co-perpetrators. This information did not produce any indication of an imminent attack in Brussels. However, it did show that some of the perpetrators/co-perpetrators knew each other in some way.

---

69 The military personnel were guided by a list of names and photographs of people suspected of involvement in the Paris attacks. When GISS was asked to evaluate this list, it responded that this fell outside the scope of its powers.

70 The Standing Committee I checked whether State Security had perhaps received this information via the Federal Police, but there was no trace of it in State Security's database.

71 The same problem was found in the investigation into the Paris attacks (see 'Chapter II.3. Review investigation into the information position of the two intelligence services before the Paris attacks').

The Committee analysed the special intelligence methods (SIMs) that were used between 13 November 2015 and 22 March 2016 in respect of each perpetrator/co-perpetrator. The conclusions of these analyses were concurrent with those following the review investigation into the Paris attacks (see II.3.2.2). Although the SIMs advanced the investigation into the Paris attacks, they provided no indication of what would subsequently happen in Zaventem and Maalbeek. The Committee was able to determine that terrorists were using increasingly more sophisticated means of communication, which meant that the services were forced to increase the number of SIMs.

The Committee found that, in the context of the judicial inquiries into the perpetrators/co-perpetrators of the Paris attacks, the Federal Prosecutor's Office had divided certain duties, partly in order to avoid the investigative methods of the intelligence services disrupting those used at judicial level.

However, the Committee also found that in the days following the Paris and Brussels attacks, State Security carried out many intelligence methods whose intelligence purpose was not always clear. State Security acknowledged that in the crisis following the attack, targets and selectors were divided between State Security and the Federal Judicial Police. The service was aware that, under specific circumstances, they occasionally worked for the judicial authorities. The reason given was that the judicial police had insufficient manpower. Although the Standing Committee I is aware that managing such crises requires a great deal of flexibility from all involved, it did deem that solutions had to be found for this division of duties to run as smoothly as possible.[72]

II.4.4.2. General Intelligence and Security Service

GISS activated its sources at the request of another Belgian service, and more specifically for two targets. None of the sources provided concrete information.

The Standing Committee I was able to determine that the SOCMINT department of GISS did not actively collect any intelligence on the four targets known to it before 22 March 2016. A list of around twenty people who needed to be monitored was only distributed on 21 April 2016. And yet, this department had been reorganised in October 2015. At that time, GISS's management wanted to equip it with analytical capacity and give the personnel *ad hoc* training. The Standing Committee I has determined that the department only received clear instructions on the targets to be monitored from 25 April 2016. However, according to the personnel of the department, there were not enough people to monitor all the targets.

Only GISS has SIGINT capacity to intercept communications abroad (Article 44*bis* of the Intelligence Services Act). This collection resource was not

[72] Consultation platforms were created after the review investigation in order to divide the targets that needed to be monitored. The Committee has not yet been able to evaluate these consultation platforms.

used for the purpose of this case. However, the SIGINT department of GISS did receive information about three perpetrators/co-perpetrators from foreign SIGINT partners. In one case, relevant intelligence was received by the SIGINT department right before the attacks. The department shared this information both internally and externally (including with State Security, CUTA and the Federal Prosecutor's Office). The Standing Committee I made the same finding in the investigation into the Paris attacks (II.3).

GISS did not start any specific or exceptional intelligence methods regarding the people who turned out to be the perpetrators/co-perpetrators of the Brussels attacks.

The Committee noted that GISS did not work out any investigative leads of its own after the Paris attacks. It was therefore guided by State Security's findings. Even so, GISS helped State Security by providing shadowing assistance and agents who had a command of specific languages.

II.4.5. COOPERATION AT NATIONAL LEVEL

II.4.5.1. State Security

The following elements could be added to the findings that the Committee made as part of the investigation into the Paris attacks (II.1).

The intelligence services and Federal Police decided to create an intelligence fusion unit. In the period between the two attacks, State Security received 200 reports about the perpetrators/co-perpetrators from the Federal Police. CUTA sent 33 reports to State Security, including updates of the consolidated Syria list and intelligence records, a number of reports based on social media and some *ad hoc* data. GISS only supplied seven items of intelligence, mainly of a SIGINT nature. State Security was also the recipient of the 'CI-weekly security situation' reports drawn up by GISS.

Between November 2015 and March 2016, State Security sent 61 memoranda to the Belgian authorities (the Federal Prosecutor's Office, CUTA, Federal Police, Minister of Justice, National Security Council, Immigration Office, Financial Intelligence Processing Unit, Directorate-General of Penal Institutions, GISS) containing the names of one or more of the perpetrators/co-perpetrators. Some of these memoranda were sent to several services and authorities simultaneously.

II.4.5.2. General Intelligence and Security Service

The Standing Committee I examined the 'CI weekly' reports that GISS drew up from mid-November 2015 until just before the Brussels attacks. These were almost weekly, confidential and classified publications (17 in total, during the period under discussion) that were sent to different recipients (CHOD, State Security, CUTA, Federal Police, the Crisis Centre and other national and

international military agencies). The aim of the publication is to provide information on the security situation and threats to military interests, but – where applicable – also covers the safety of Belgians abroad (which also forms part of GISS's duties). The 'CI-weekly' is well-structured and includes an abstract, an assessment and a general threat analysis.

GISS published a 'CI weekly' on the day before the Paris attacks on 13 November 2015. Although this stated that Belgian participation in the coalition against IS did increase the risk of revenge attacks against Belgium, there were no specific indications at the time of possible attacks against military interests in Belgium or elsewhere. Nonetheless, it did state that the threat against Western interests – including Belgian interests – was considered to be serious. Importantly, GISS also warned against the possible infiltration of IS agents via the flow of refugees from the Middle East and Africa. GISS had already been able to conclude before the Paris attacks that there were IS movements of individuals in Europe. The service also shared that information with State Security at the end of October 2015.

GISS also shared operational information with the Belgian authorities. For example, SIGINT data that the service had relating to people who would later play a role in Brussels was sent to State Security. Although GISS was able to contribute immediately after the Paris attacks, the information dried up by mid-January 2016.

It was only able to successively reactivate its network after the raid in Vorst. On 18 March 2016, the service sent a request to its international partners and one day before the attack it received information about one of the perpetrators/co-perpetrators from an international SIGINT partner. However, this information could not be distributed any further before the Brussels attacks.

Lastly, GISS shared other information: on 3 March 2016, a possible threat for March 2016 was reported to State Security, and another between April and June 2016 (albeit mainly against targets in the military sphere). Brussels was mentioned in addition to ten other European cities. GISS had received this information from one of its partners. The service noted that it had no elements to confirm or deny the information, and expressed doubt about the *modus operandi* that was described in the report. The Standing Committee I felt it could state that the report – if there was any truth to it at all – did not provide any concrete information on the Brussels attacks three weeks later.

II.4.6. COOPERATION AT INTERNATIONAL LEVEL

II.4.6.1. State Security

During the period under discussion, State Security received more than 200 reports from around 30 foreign correspondents (*supra*). The Committee noted the following elements in addition to the findings from the previous investigation (II.3):

- State Security emphasised the important role that liaison officers accredited in Belgium play in the exchange of information;
- State Security wished to have its own liaison officers abroad with a view to optimising the exchange of information;
- International cooperation in the intelligence world was evolving massively: the aim was to achieve a more efficient and quicker exchange of information by creating a permanent cooperation structure within the Counter Terrorism Group (CTG).

II.4.6.2. General Intelligence and Security Service

As stated above, most of the information in GISS's possession came from international sources (e.g. the SIGINT information). The Committee made the following remarks concerning the international platforms of which GISS is a member:

- These platforms are at a strategic and political level; operational or tactical information is not shared in them;
- In May 2016, GISS brought together a number of homologous foreign services to exchange operational information on IS;
- Between 2014 and mid-2016, around 200 bilateral meetings were held between GISS and foreign partner services to discuss the terrorist threat;
- From 2015 to mid-2016, the Head of GISS participated in 20 international meetings convened to discuss the terrorist threat.

II.4.7. THE WEEKS BEFORE THE ATTACKS, FROM STATE SECURITY'S PERSPECTIVE

The Standing Committee I examined especially which activities State Security carried out in the period immediately before the Brussels attacks (from 1 March 2016) and how the authorities were informed of those activities.[73]

II.4.7.1. State Security's operational target lists

In its weekly 'operational target lists', State Security indicates which investigative objects or traces have priority and how it will try to gather information about

[73] The Committee had no insight into the judicial inquiries that were running at the time and in which State Security had been designated as an expert (and from which the service could possibly find certain information or intelligence).

them. It also indicates which collection service is involved and which analyst is responsible for the follow-up.[74]

The list of 7 March 2016 contained more than sixty names. As all the later perpetrators/co-perpetrators, except for one, were included, they were priority targets. The list also indicated which further HUMINT sources had to be recruited and a summary was provided of the *ad hoc* information on threats that State Security had received from foreign correspondents. This information did not refer to the atrocities that would occur in Zaventem and Maalbeek.

The target list of 15 March 2016 was mostly identical to the one before it. Although the number of possible threats against or in Belgium had increased, the Standing Committee I determined that these new reports, too, had nothing to do with the attacks that occurred shortly afterwards.

II.4.7.2. Activities in the first weeks of March 2016

State Security's activities and priorities in the last weeks prior to the attacks could best be characterised on the basis of meetings at which one or more of the later perpetrators/co-perpetrators were discussed.

In the period between 4 and 21 March 2016, State Security participated in at least nine meetings in which one or more of the later perpetrators/co-perpetrators of the Brussels attacks were mentioned. Foreign partners were involved in seven of those meetings. The Paris attacks and what preceded them were the central issue of the talks. The services tried to reconstruct the preparations for the Paris attacks. The perpetrators/co-perpetrators were still described as 'dangerous' and capable of planning or committing further attacks. However, there was no indication of a concrete and/or imminent threat against Belgium specifically.

The raid by special units in the Vorst apartment on 15 March was a pivotal moment because the terror suspects were flushed out of their hiding places (although only partially, it later transpired). Following the raid, meetings took place in rapid succession. In conjunction with two partner services, State Security was still trying to obtain more details about the trip that Salah Abdeslam made in the autumn of 2015, returning to Brussels with a number of people (one of whom was killed in the Vorst raid). A meeting was held on the same day with the Federal Prosecutor's Office and Federal Police to discuss the events and look at several leads.

A meeting was held on 17 and 18 March 2016 – including with a Northern European service – regarding the person who was killed in Vorst, which led to his identification (Belkaid).

---

74 The creation of these lists – which were formalised as tools and further refined after the Paris attacks – is in keeping with the Standing Committee I's earlier recommendations to establish a coordinating or umbrella 'collection and analysis design' (applied *in casu* to the area of counterterrorism).

Besides meetings in which data was exchanged, written information was also exchanged with Belgian services. This mostly produced *ad hoc*, operational information, including about Abdeslam's potential whereabouts.

II.4.7.3. The raid in Vorst and the arrest of Abdeslam in Molenbeek

The raid in Vorst on 15 March 2016 was a turning point. Belkaid was killed and two others escaped: Salah Abdeslam and the man who used the name Amine Choukri (later identified as Ayari). State Security compiled a comprehensive memorandum on the Vorst raid for the Minister of Justice, including an update and a report on the leads it had followed.

After the raid in Vorst and the apprehension of Abdeslam in Molenbeek, the National Security Council organised emergency meetings.

On 21 March 2016 – the eve of the attacks – a memorandum was sent to the Minister of Justice. This detailed a number of investigative leads arising from Salah Abdeslam's arrest. The Committee noted that:

- No indications were found during the raid in Vorst of imminent attacks in Zaventem or Maalbeek;
- State Security was not aware of any reconnaissance activities by possible perpetrators in Brussels, or elsewhere, with a view to possible attacks (as happened in Paris and later in Nice);[75]
- Shortly after the raid in Vorst, State Security examined an index card that was attributed to IS (containing details about Belkaid, including naming him as a suicide bomber). The document was part of a series of similar documents that were made public at the start of March 2016. The question of where he wanted to blow himself up – if the rest of the information on the card was correct – remained unanswered;
- Abdeslam remained silent in the days following his arrest.

II.4.7.4. Mainly operational information

The information that was exchanged nationally and internationally was mostly operational in nature. The same went for the memoranda that State Security drafted and sent to the authorities: they contained facts, investigative leads, etc. The Committee did not come across any memoranda with more extensive analyses or formally detailed hypotheses/scenarios on how the events had to be interpreted or what could follow from them and/or memoranda that warned the authorities about imminent threats. When asked about this, State Security explained that such questions and concerns were, however, never forgotten about. The Standing Committee I believed that State Security was swept along

75 As stated above (II.4.3.3), the observations of the OVG were not shared with State Security.

into operational work in the aftermath of Vorst/Molenbeek. The Committee reiterated the importance of forming official hypotheses/scenarios and of 'predictive' intelligence. Obviously the necessary people and resources have to be allocated, a methodology created, and information exchanged for this purpose. The Committee also pointed out that other services have a crucial role to play as well, including CUTA, in particular, whose task is to drawn up threat assessments and strategic analyses.

II.4.8. CONCLUSIONS

As was the case with the Paris attacks, the activities of the intelligence services did not lead to the timely detection of the Zaventem and Brussels attacks. The examination of the information gathered did not reveal that the services had information at their disposal to prevent these attacks either.

The Standing Committee I did not find any evidence of dysfunction in the way State Security carried out its assignments prior to these attacks as the intelligence service explicitly designated by law to act in the fight against terrorism. Some of the perpetrators/co-perpetrators involved had been known since the Paris attacks and were priority targets of the service. Even so, they managed to stay out of sight of State Security – and the other Belgian and foreign intelligence and police services – for more than four months. In the months prior to the attacks, State Security used the available resources (HUMINT, SOCMINT, SIM, etc.) and adapted its operations, but this did not produce much useful information. The international channels and the numerous meetings with partner services prior to 22 March 2016 also contributed little. To summarise, it can therefore be stated that despite considerable efforts, State Security's information position was not strong enough to thwart the threat *in casu*. This does not detract from the accomplishments and concrete contribution that were made towards further identifying and dismantling the terrorist network.

The Committee was of the opinion that the information position of the services could be strengthened, particularly in relation to informant operations and through better access to the communication channels of the existing and (potential) terrorists.

With regard to GISS, it could be determined that the service tried to activate its HUMINT and SIGINT sources after the Paris attacks, in order to find out more about the perpetrators. Although this produced certain results at the level of insight into IS operations and the interconnection between targets, it yielded no pertinent details about a concrete threat in Belgium. The service did not, however, use any SIM methods or apply SOCMINT either with regard to the four perpetrators/co-perpetrators known to the service or any of the other perpetrators/co-perpetrators. Given the very limited use of its own collection

resources, GISS had scant information and thus a poor information position regarding the threat in Belgium. The Standing Committee I found in its investigation that the information flow from *Operation Vigilant Guardian* could certainly have been better. As part of this operation, the military detachments deployed within the country had brought forward information that was communicated to the police services that the detachments were supporting. The Standing Committee I did not investigate how the police services dealt with this information but did find that the same information was simultaneously sent to GISS, via the military chain of command, which did not deal with it. The Committee believed this should have happened, especially as part of GISS's duty to provide deployed military personnel with all useful information (the concept of force protection). However, the Committee did note that GISS had made part of its operational CI capacity available to State Security, which illustrated good mutual cooperation.

The Committee found that the national and international exchange of data between the competent services increased sharply overall since the Paris attacks, but that it still remained relatively limited in nominal figures. As previous investigations also showed, the exchange of information still needed to be improved. The Committee was able to conclude that cooperation between mainly European intelligence services gained a new dimension during the course of 2016. The exchange needed to still be deepened further at Belgian and international level to strengthen the information position.

The Standing Committee I's report on the investigation into the Paris attacks confirmed that GISS had sent a very important warning about IS's plans against European targets to its domestic and foreign contacts just before the attacks. However, this information was not concrete enough to be able to launch a targeted counteroperation. No new disturbing matters came to light before the Brussels attacks and GISS could only refer to the general presence of a threat against European targets in its weekly bulletins.

Both services were actively involved in consultations in the National Security Council and gave briefings and provided information in that context. In relation to State Security, the intelligence that the service sent to the Belgian authorities was mainly *ad hoc* in nature and the service did not regard itself able to provide more general analyses. Nonetheless, the Committee reiterated that the essential task of an intelligence service is to produce predictive and strategic intelligence for the authorities.

The Standing Committee I has repeatedly found that when the intelligence services are appointed as court experts for the Public Prosecution Offices, judicial logic threatens to outweigh intelligence logic, while what is needed is a proper balance between judicial and administrative action. For this reason, attention must be paid to the optimal management of the intelligence services by the administrative authorities, so the intelligence services do not use their

limited capacities for purely legal assignments, such as collecting evidence. The Committee therefore believes that the risk of developing a 'judicialization' within the intelligence services needs to be addressed as a priority.

Other than that, the Standing Committee I referred to the different focus points and items for improvement included in the final report on the review investigation into the Paris attacks (see II.2.4).

II.5. PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL AND THE SNOWDEN REVELATIONS

II.5.1. INTRODUCTION

On 6 June 2013, *The Guardian*[76] and *The Washington Post*[77] first published information from tens of thousands of documents (classified and otherwise) that had been leaked by Edward Snowden, who held various positions in or for American intelligence services. New revelations have been following in rapid succession since.

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

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

---

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

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

Thereupon the Standing Committee I opened a number of review investigations[78] that were closely connected with each other. Three of those were completed in 2014.[79]

This last review investigation[80] deals with the possible implications of the above foreign programmes on the protection of the scientific and economic potential of the country.[81] Its aim was to check whether the Belgian intelligence services:

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

At the request of this Monitoring Committee, the consequences of the PRISM programme and/or other similar systems for the scientific and economic potential of the country were also examined. The report was completed at the start of 2016.[82]

II.5.2. FINDINGS

II.5.2.1. Massive communication interception and the SEP?

The Standing Committee I was able to determine that the Snowden revelations had – superfluously, and in a documented manner – demonstrated that the

78 A further investigation was initiated following a complaint made by the President of the Dutch-speaking Bar Association at the Brussels Bar ('Investigation following a complaint by the President of a Bar Association into the use of information originating from massive data capturing in Belgian criminal cases' (free translation)). In this regard, see STANDING COMMITTEE I, *Activity Report 2014*, 40–45 (II.3 'Use in criminal cases of information originating from massive data capturing by foreign services').

79 See STANDING COMMITTEE I, *Activity Report 2014*, 11–45 ('II.1. The Snowden revelations and the information position of the Belgian intelligence services', 'II.2. Protection of privacy and massive data capturing' and 'II.3. Use in criminal cases of intelligence originating from massive data capturing by foreign services').

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

81 Edward Snowden explained, for example, that the European Union is a priority target for the NSA and British GCHQ, particularly as regards foreign policy, international trade and economic stability. *'That a major goal of the US Intelligence Community is to produce economic intelligence is the worst-kept secret in Washington.'* In: www.europarl.europa.eu:document/activites/cont/201403/20140307ATT80674/20140307ATT80674EN.pdf.

82 The investigative actions were interrupted various times due to other investigations with a higher level of urgency that were entrusted to the Standing Committee I. The final report, classified as 'CONFIDENTIAL (Act of 11.12.1998)' was sent to the competent Ministers on 11 February 2016.

interception of communications and data by the intelligence services of friendly countries (the United States, United Kingdom, etc.) was a reality. This happened in both a massive and targeted manner. However, the authorities of these countries, insofar as they provided any explanation, stated in their response that the interceptions focused on legitimate targets only – according to their national law – such as the fight against terrorism, organised crime and corruption. They denied these interceptions were used for economic espionage or to benefit their own companies.

After its review investigation, the Standing Committee I had no knowledge of proven espionage against Belgian companies or scientific institutions by means of massive communication interception systems, such as the NSA's PRISM programme.

However, it can be accepted with a probability bordering on certain that foreign companies, both within and outside Europe, were the subject of interception activities by the intelligence services of the above countries. The same conclusion can be drawn in relation to espionage targeting leading politicians (see *Merkelgate*[83]), governments and international institutions such as the European institutions relating to economic and financial policy. These developments were sufficiently coherent and documented to be able to attribute the recorded Belgacom/BICS hacking[84] to the same intelligence services.

The Committee stated that it could assume from this that Belgian companies, scientific institutions and political authorities responsible for financial and economic policy could be the subject of economic espionage. This applies regardless of the espionage techniques used, including targeted and non-targeted interceptions, certainly also by countries other than those mentioned, and all the more so by less-friendly countries.[85]

We can conclude that, despite all the commotion following the Snowden revelations, the foreign interception programmes were not discontinued, but were at most somewhat better substantiated according to the national law of the services involved. There is no indication that communication interceptions or cyber espionage would decrease in future, rather the opposite. It is even reasonably doubtful whether political or international-law arrangements could provide solutions or guarantees, given the inherently secret nature of espionage

83 Edward Snowden revealed that the NSA had tapped telephone calls made by the German chancellor Angela Merkel.

84 In mid-September 2013, the telephone operator BELGACOM stated in a press release that it had found evidence of a digital breach of its internal IT system during a security inspection. A complaint was submitted to the Federal Prosecutor's Office (www.belgacom.com/be-nl/newsdetail/ND). This was an alleged case of cyber espionage aimed at the international telephone communications managed by Belgacom International Carrier Services (BICS).

85 For the sake of completeness, industrial and competitive corporate espionage by private players had to be taken into account as well, even though this fell outside the actual scope of the investigation.

activities. For this reason, particular attention must be paid to the enhanced protection of ICT and communication systems.

Again because of the secret nature of interception operations, as a result of which scant information is available about the extent of the economically-related espionage and even less about the ultimate use or effect of the gathered intelligence, it is illusory to be able to even roughly estimate the harmful consequences of using these espionage systems for the Belgian economic fabric. The damage moreover only manifests itself exceptionally or is indirect, such as the hacking of Belgacom/BICS. This specific case (of targeted hacking and thus *a priori* non-massive interception) shows that the damage can be very significant.

II.5.2.2. Role of the Belgian intelligence services and CUTA

As earlier investigations of the Standing Committee I have shown[86], the Belgian intelligence services hardly played any role in this problem, neither preventively nor through their cooperation in the operations of these foreign services.

In specific reference to the scientific and economic potential, the services showed very few signs of activity to protect this potential against the threat of interceptions (massive or otherwise), even though they were or should have been aware of the risks, especially after the earlier revelations, such as the ECHELON and SWIFT cases.

It had to be concluded that a phenomenon analysis of the massive interceptions and their consequences for Belgium or its scientific and economic potential was not produced at any stage, even after the revelations.

On the other hand, the sectors and authorities involved also did not question the services after the revelations in this regard, except when the authorities asked whether the intelligence services had been complicit in the hacking of Belgacom/BICS.

The applicable statutory framework at the time proved to be inadequate to resist complex threats to the national critical infrastructure.[87] An inventory of the critical infrastructure had still not been drawn up for the purpose of implementing the Critical Infrastructure Protection Act[88], in which a role is set aside for CUTA (and for its support services and the Crisis Centre), for the electronic communications sector.

---

86 See, for example, 'The SWIFT case', in STANDING COMMITTEE I, *Activity Report 2006*, 34–43 or 'ECHELON', in STANDING COMMITTEE I, *Activiteitenverslag 1999 aanvullend* (Additional Activity Report 1999), 2–51.

87 This legislation could offer or reinforce a solution if certain communication or IT infrastructures, such as the servers of the main Belgian telecommunications operators, would be included as part of that infrastructure. This would legally oblige the operator of the infrastructure to raise security to an adequate level.

88 Act of 1 July 2011 on the security and protection of critical infrastructures, *BOJ* 15 July 2011.

In addition, the risk analysis that CUTA has to make in this regard is an all-risk analysis, even though CUTA is restricted to extremism and terrorism in its other assignments (and thus expertise). The Act of 1 July 2011 also defines infrastructure as *'an installation, system or a part thereof, of federal importance, which is crucial for maintaining vital social functions, health, safety, security, economic welfare or social welfare, and whose disruption or destruction would have a significant impact because those functions would be destabilised*' (free translation). Not everyone agreed that (cyber) espionage fell under this definition. However, the Committee believed that the possibility of interceptions or hacking threatened the integrity of critical communication systems, regardless of whether this happened because of espionage or other or more destructive reasons.

Once again, it must also be concluded that the execution of the assignments of the intelligence services, in particular those of State Security, to protect the SEP, does not go smoothly in practice. This was already clear when the statutory authority had to be put into operation and it took considerable time before a definition of SEP could be developed.[89]

According to the Committee, this can probably be explained by the lack of coordination between this intelligence service and the stakeholders, namely the various competent authorities (federal and certainly also regional) for economic and financial policy and the private sector. This seems to lead to a vicious circle of missing analyses, the lack of knowledge of phenomena in the sectors to be protected, and of what these sectors can expect from the Belgian intelligence services. The specific details of this protection moreover seem to suffer from a negative interpretation by the intelligence services (for example in the form of negative opinions on exports or foreign investments). And yet, enhanced protection of the SEP is not only a story of costs and restrictions, but also of economic growth opportunities. For the time being, however, there is no instrument that can form a bridge between the intelligence services and the public and private players of the scientific and economic potential.

The Committee also refers to State Security's action plan, which – at the time of the report – prioritised the protection of the SEP, although the results could not yet be verified. GISS also stated that it wishes to reinforce its efforts in relation to this problem. It further transpires that working groups headed by the National Security Council have been trying to improve the protection of both the SEP and cyber security. Seeing the Centre for Cybersecurity Belgium put into operation was a turning point and a very promising event for the Standing Committee I.

89 STANDING COMMITTEE I, *Activity Report 2006*, 62.

II.6. STATE SECURITY AND THE COOPERATION PROTOCOL WITH PENAL INSTITUTIONS

A review investigation was opened on 1 October 2014 into how State Security implements the '*protocol agreement governing cooperation between State Security and the Directorate-General for the Execution of Penalties and Disciplinary Measures (DGEPM)*'(free translation).[90] This agreement was concluded on 20 November 2006 as part of the Radicalism Action Plan that was approved by the then Ministerial Committee for Intelligence and Security on 28 April 2006. The cooperation agreement came about (mostly) at the request of State Security which had insisted several times at the beginning of the 2000s that there needed to be a better exchange of information with the prisons. In 2001, for example, State Security expressed concern about '*the conversion zeal shown by some Islamist organisations in prisons*' (free translation). The service regretted that '*the Management of Penal Institutions had not (yet) adopted the habit of forwarding information in this regard to State Security at its own initiative*' (free translation).[91]

The aim of the investigation was to assess whether the agreement was being efficiently implemented, whether State Security could extract useful information for its purposes and, albeit on the margin, whether the exchange of information on detainees was in accordance with the protection of the rights of individuals guaranteed by the Constitution and the law.[92] Two prior review investigations were the direct reason for this investigation.[93]

II.6.1. EXCHANGE OF INFORMATION WITH THE PRISON ADMINISTRATION

Article 13 of the Intelligence Services Act stipulates that the intelligence and security services may, as part of their assignments, trace, gather, receive and process intelligence and personal data that could be useful for carrying out these assignments. The prison administration is obviously an important source of information in this regard. The members of this administration are authorised to forward information to State Security by virtue of Article 14 of the Intelligence

90 The DGEPM changed its name and became the Directorate-General of Penal Institutions (DGPI). The Standing Committee I had previously called for a strict application of this Protocol Agreement between State Security and the DGPI, in STANDING COMMITTEE I, *Activity Report 2012*, 77.

91 STANDING COMMITTEE I, *Activiteitenverslag 2001* (Activity Report 2001), 104.

92 The investigation was completed in mid-March 2016.

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

Services Act: officials and agents of public services may share information with the intelligence services, on request or at their own initiative, '*based on any agreements made and the rules laid down by their supervisory authority*' (free translation).

A last paragraph added to Article 14 of the Intelligence Services Act in 2010 stipulates that State Security '*can access the databases of the public sector that are useful for carrying out its assignments*' (free translation). For instance, State Security has direct access to the SIDIS Suite, which is the registry database of the DGPI.

In addition to gathering information, State Security is also obliged, in accordance with Article 20 §1 of the Intelligence Services Act, to cooperate as efficiently as possible with the administrative authorities, among others. State Security may also cooperate with and provide technical assistance to the same authorities by means of protocol agreements (Article 20 §2 of the Intelligence Services Act).

II.6.2. APPLICATION OF THE PROTOCOL OVER THE YEARS

The purpose of the concluded agreement was '*to facilitate and encourage the exchange of information, to determine the practical rules for accomplishing the cooperation, to intensify the exchange of ideas and analyses or, in other words, to focus cooperation for the assignments and activities of the above services more on practice*' (free translation).

The Standing Committee I was able to determine that the implementation of the Protocol Agreement needed a long running-in period. Two periods could be distinguished in its application. On the one hand, the period between 2006 and mid-2014 (in which the mechanisms that were determined for cooperating and exchanging information were only moderately applied). On the other hand, the period from mid-2014 (during which the exchange of information between State Security and the prison system rapidly gained momentum, without this necessarily being based on the mechanisms under the protocol agreement).

The Standing Committee I had to conclude that the manner in which the agreement was implemented in the field until mid-2014 was in stark contrast with the importance that the service attributed to it before but also after its conclusion. For example, only a limited number of documents relating to terrorism or radicalised detainees was exchanged in the period 2006–2014.[94] Although the amount of intelligence exchanged increased over the years, the exchange of information was mostly based on personal/informal contacts. The Protocol Agreement is said to have been a facilitating factor in the sense that

[94] According to State Security, no figures could be given.

staff members of the prison administration (e.g. prison directors) were less reticent in their contact with members of State Security as they knew they were legally and administratively covered.[95] However, the lists of radical detainees and persons related to terrorism as envisaged in the Protocol were never drawn up during that period. This only happened in mid-2014.

The fact that the Protocol was not really used as an instrument for intelligence gathering in the early years possibly had to do with how State Security perceived the threat.[96] The problem seemed to be placed higher on the agenda in later years. 'Extremism – terrorism – Islamism (in) prisons' was placed under 'active prioritised monitoring' in the 2011, 2012 and 2013 Action Plans.

However, the Standing Committee I saw the real causes for the improved exchange of information and cooperation between State Security and DGPI as follows: first, many actual or aspiring Syria fighters and recruiters were imprisoned from 2012–2013 and, second, the new management of State Security emphasised the need for the exchange of information in general, and with the penal institutions in particular.

II.6.3. *AD HOC* EVALUATION OF THE PROTOCOL: FINDINGS

The Committee was able to make the following findings in the course of its investigation:

- Although the protocol focused mainly on Muslim-related radicalisation and terrorism, information was also exchanged in relation to other phenomena, including harmful sectarian organisations, interference, anarchism, and the extreme left and right;[97]
- The Protocol stipulated that lists would be used: State Security would have a list of radical elements and a list of persons related to terrorism; the DGPI would have a list of detainees found guilty of terrorism. The DGPI made the 'PI Terrorism Register' available to State Security.[98] State Security did not draw up any lists from its side. According to the service, it would not be

95 The fact that State Security had appointed someone in 2006 with extensive practical knowledge in this regard to follow up on the subject matter also narrowed the gap between both administrations. This person implemented the obligations under the agreement in quite a practical manner, which also resulted in a greater exchange of information, albeit informally.

96 In its 'Phenomenon analysis on Islamic extremism' from 2009, the service dedicated a chapter to extremism in prisons. The service concluded in this analysis that '*The activities of converts to extremist Islam in Belgian prisons currently seem to be quite limited*' (free translation).

97 As many of the contacts were made informally, no figures could be presented in this regard.

98 The list was discussed for the first time in the Prisons Working Group (Plan R) in February 2014. The list was subsequently shared and regularly updated.

practical or desirable to draw up such lists. In order to keep its side of the bargain, State Security opted to work, from August 2014, with records for each detainee included in the 'PI Terrorism Register'. This record contained relevant information for the prison system: the extent of the flight risk, the likelihood of the detainee radicalising third parties, criminal record in relation to weapon use, etc. The records were delivered to the relevant prison directors, who could in turn adopt the necessary measures;

- The DGPI, which could request additional information from State Security, made increasing use of this option. This was certainly the case since the Syrian crisis, which led to an increase in the number of terrorism-related detainees;
- An important finding was that State Security activated its access to the SIDIS database.[99] State Security previously used specific computers for that purpose and separate access codes, but general access was obtained in 2016. Important changes were made to the SIDIS database in September 2014; the new system (SIDIS Suite) was expanded to include more data (such as visitors, telephone numbers, etc.);
- State Security and the DGPI also jointly attended certain meetings in relation to the Radicalism Action Plan and the ensuing JIB list. Information was exchanged on those occasions as well. Both forms of exchanging information existed alongside each other. The 'PI Terrorism Register' list (for detainees found guilty of terrorism) and the Plan R/JIB list (summary of radicalised elements) were clearly different lists, each with their own objective;
- The Standing Committee I also noted that a practice had developed outside the Protocol by which information was exchanged directly with the prison concerned and not the actual point of contact (POC) at national level. The Committee pointed out the danger of this practice: to the extent that, for example, no formal report or official record was made of this exchange and included in State Security's database (VESTA), there was a risk that the POC would lose the overview;
- According to State Security, the DGPI was increasingly making reports of people who showed signs of radicalisation. This was possibly a result of the radicalisation training – given by State Security – within the prison system. However, State Security itself noted that new developments and

---

99 Article 36*bis* of the Privacy Act of 8 December 1992 makes its compulsory for a service to obtain prior authorisation from the Sectoral Committee for the federal government for '*any electronic communication of personal data by a federal government agency*' (free translation). The Committee found that such authorisation was not requested *in casu*. In the Committee's opinion, this was important as the Privacy Committee stated in its opinion 08/2016 of 24 February 2016 that SIDIS/SIDIS Suite '*did not pass the test of the L.PPD*' (free translation). The Privacy Committee had already ordered the administration concerned in 2013 to '*develop a statutory basis for this database*'(free translation).

increased attention in the media had also led to greater alertness among prison staff;
- The Protocol tried to make a distinction between terrorism and radicalism. This distinction turned out to be artificial; it would require two separate regimes, while in practice there was little difference as regards the practical approach;
- The Standing Committee I pointed out two developments that were important at the time of the investigation. First, State Security and DGPI were increasingly obliged to pay attention to the phenomenon of anarchism. After all, one particular movement proved to be very active in approaching prisoners and opposing the existence of prisons. Information about the 'supporters' of this particular anarchistic movement had been regularly exchanged for several years. The exchange of data yielded pertinent information for both the DGPI and State Security. On the other hand, it was determined that extremist Islamic groups tried to exercise influence over Muslim inmates mostly through correspondence rather than visits.
- State Security indicated that DGPI had reported conspicuous behaviour regarding the radicalisation of detainees in a growing number of cases. However, figures were not available in this regard.
- State Security was very satisfied as regards compliance with the regulations on classified information. The DGPI likewise did not detect any breaches of classified documents from its side;
- As stated above, the Protocol Agreement emphasised the importance of training prison officers.[100] Even so, the Committee found that serious efforts were only made in this regard in 2011 when training was organised for directors, the members of the psychosocial department and some prison officers. The training focused on recognising radicalism. Although trainees would subsequently be able to give training within the penal institutions, this did not function very well, partly due to staff turnover. A general awareness course was given to the management and higher-level security staff in all prisons in 2012 and 2013. The result of this was that only a minority of prison officers was reached;
- Lastly, the six-monthly meetings between the heads of State Security and DGPI agreed in the Protocol almost never took place. This does not mean there was no communication. Employees of both services exchanged experiences and could easily be contacted. However, consultation at a higher level remained absent.

[100] Several options were considered, including introducing COPPRA (Community Policing and Prevention of Radicalisation) training, cooperating in the CUTA deradicalisation project 'ISF', and providing an online tool for prison officers so they could acquire certain skills through self-study. However, these ideas were still in an early stage and not yet very concrete.

II.6.4. STATE SECURITY INITIATIVES OUTSIDE THE PROTOCOL[101]

State Security obviously did not depend solely on the Protocol concluded with DGPI for its information position on radicalised detainees. The service took several other initiatives. For example, there was cooperation in 2013 with a number of European intelligence services, during which experiences were exchanged and which led to the report entitled 'After the Prison'.[102]

In addition, a point of contact (POC) was appointed within State Security, a 'Radicalisation in prisons' unit was established, each provincial post of State Security received a list of contact people of the penal institution within their official area, and a study was made of what was necessary to optimally monitor the problem of radicalisation within prisons.[103, 104]

II.6.5. CONCLUSION

The Standing Committee I concluded that the Protocol had set things in motion. Although significant change was evident, many aspects remained untouched for a fairly long time. Some aspects of the Protocol were never even implemented. Nonetheless, both services were extremely satisfied. Both DGPI and State Security stated that they had not uncovered any serious shortcomings in how the Protocol worked and they experienced it as positive. The Standing Committee I did note that the Protocol Agreement had never been formally evaluated.

II.7. MONITORING A POTENTIAL THREAT AGAINST A FOREIGN VISITOR

In March 2015, an agent of State Security's External Services approached the Standing Committee I to complain about how the Analysis Services had allegedly worked in a case concerning the imminent visit of a Congolese doctor,

---

101 These initiatives did not form the subject of an investigation by the Standing Committee I.

102 A comprehensive internal memorandum by State Security (*'Intensifying State Security efforts in prisons'*) (free translation), highlighted the need to gain insight into radicalisation within penal institutions.

103 This assessment was made in December 2014 and included in the aforementioned memorandum by State Security entitled *'Intensifying State Security efforts in prisons'* (free translation) of 1 December 2014. Among other things, it included a study of staffing needs, the necessity of HUMINT, the possibility of treating a detainee as a human source, determining the frequency of informing authorities, and designating the employees with exclusive access to the SIDIS system.

104 In mid-March 2016, the Committee received an extensive study entitled 'Phenomenon Analysis of Radicalisation and Terrorism in Belgian prisons – March 2016'.

Dr Mukwege, to Belgium. According to the complainant – also an acquaintance of Dr Mukwege and co-organiser of the visit – CUTA had not been correctly informed of all relevant information in order to make an assessment of the potential threat to the doctor.[105]

II.7.1. CONTEXTUALISATION

The Congolese gynaecologist, Dr Mukwege, is known as a champion of human rights. He first attracted State Security's attention in relation to the 2011 elections in the Democratic Republic of the Congo. The service started to monitor his activities within the context of his visits to Belgium. After all, those visits could have had consequences within the African diaspora or for relations between Belgium and the Congo, which could have posed a threat for Belgian security, at home and abroad, or foreign relations.

Dr Mukwege visited Belgium on several occasions. These visits never gave rise to security measures by the Belgian authorities.

In December 2014, State Security was advised of the doctor's intention to visit Belgium again in March 2015. Since the assessment of the situation in the Congo – just like the threats against the doctor – was a permanent assignment, the Analysis Service did not issue any specific judicial order in this regard. The initiative to gather information was autonomously left up to the External Services.

At the end of February 2015, the Analysis Service prepared a memorandum for CUTA and the Crisis Centre based on information obtained from human sources and social media. During the course of March 2015, the service received a number of reports from other sources but those did not yield any further information about a potential threat against the doctor, or constitute any reason to prepare a new memorandum.

On the insistence of an External Services agent (namely the agent who would later file the complaint with the Standing Committee I) and the hierarchical superior, the Analysis Service prepared a supplementary memorandum on the eve of the doctor's visit. This new memorandum did not give CUTA cause to change its threat evaluation, which it maintained at 'level 2'.[106]

II.7.2. FINDINGS

The Standing Committee I found that the gathered information had been evaluated, analysed and communicated to CUTA and the Crisis Centre within a reasonable period, such that the appropriate measures could be taken.

---

105 The review investigation was completed in May 2016.

106 CUTA informed the agent concerned that the level had remained unchanged.

The Committee wondered about the double role and capacity of the complainant: acting on the one hand as a State Security agent and, on the other hand, as a private person.[107] The Standing Committee I pointed out that this 'role confusion' could have adversely affected the ultimate assessment work.

The Committee could not detect any shortcomings in how the Analysis Service had handled Dr Mukwege's visit to Belgium. Although the fact that most of the information gathered came from one collection agent (namely the complainant himself) could have undermined the objectivity of the ensuing analysis, this did not happen *in casu*.

The collection agent's 'freedom to act' in this case can partly be explained by the absence of directives, both from the Analysis Service in relation to the External Services and from the relevant departments of the External Services. There was no collection plan in the strict sense. The hierarchical superior of the agent had given a signal by rejecting two of the agent's reports, but his attitude was otherwise not fundamentally corrected. State Security management could play a role through proactive intervention in such cases.

II.8. A COMPLAINT AGAINST AN INDISCREET COLLEAGUE

In July 2015, a senior officer of GISS filed a complaint with the Standing Committee I alleging that a GISS employee had divulged data relating to his personal and professional life in a public area in the municipality where both he and the employee lived. He even feared that this could have consequences for his safety and that of his family.

The complainant had previously approached the management of GISS on two occasions but did not think they acted firmly enough. He finally filed his complaint with the Standing Committee I. The complaint covered both the alleged indiscretions and the manner in which GISS had responded to them. The final report was approved in May 2016.

II.8.1. FINDINGS

The employee acknowledged that he had discussed the complainant during a 'get-together'. However, he denied disclosing any classified information about the complainant; he would never even have had access to such information. The Head of GISS stated that he had spoken to both parties and that he found the indiscretions of his employee to be professionally inappropriate. His departments

[107] He moreover did not deny his close involvement with the doctor.

were asked to call the administrative assistant to order – which happened – but due to a communication error, he did not receive any feedback in this regard.

GISS initially regarded the complaint as a minor problem. However, the manner in which it was handled left the complainant dissatisfied. Although the Head of GISS considered the behaviour of the administrative assistant to be unacceptable, he found that no confidential information had been misused and a disciplinary sanction was therefore unnecessary. The employee was transferred to another department within GISS. The complaint was ultimately handled within the security clearances department of GISS, and the administrative assistant was given a reprimand.

II.8.2. CONCLUSIONS

The Standing Committee I did not find any indications that the administrative employee had breached his duty of confidentiality. Likewise, no unauthorised access to the complainant's security investigation or to classified information was noted.

However, in relation to the obligation to exercise discretion, it could be determined that the administrative assistant had not shown the necessary professional restraint and caution because he raised professional or private matters concerning the complainant during a 'get-together'. In that respect, the complaint was well founded.

The Standing Committee I did not find any information in its investigation that pointed to a security issue involving the complainant or his family. The Standing Committee I was generally of the opinion that the complaint could have been handled better internally.

II.9. A COMPLAINT CONCERNING WHETHER OR NOT A PAYMENT IS DUE

A former State Security inspector filed a complaint with the Standing Committee I in April 2015. He stated that he was forced to repay a (small) amount that he purportedly wrongly received from the special funds. After failing to defend his position with State Security, he approached the Standing Committee I. He also stated that the problems he had experienced with his direct hierarchy had prompted him to leave State Security.[108]

[108] The complainant worked as a member of State Security's External Services for over three years.

The Committee opened a '*review investigation following a complaint by a former State Security agent regarding the management of the departmental fund of a provincial post*' (free translation).[109]

During the period in which the complainant was asked to repay an amount (2012–2013), the accounting system was not in accordance with the instructions of central management and it was inadequate.[110] The Standing Committee I could moreover not find any evidence for or against the complainant's assertion. As the accounting system at the time did not allow for any subsequent audit, it could not be established through the accounts whether or not the disputed amount was payable. When the complaint was handled at State Security level, nobody was appointed as the person(s) responsible with a mandate to resolve the dispute. This meant that a large number of people were involved with the case without anyone coming up with an acceptable solution for all involved. This procedure led to unnecessary tension and dissatisfaction.

II.10. A COMPLAINT CONCERNING AN INTERVENTION BY TWO PROTECTION ASSISTANTS

An incident with two members of what was State Security's Close Protection Service[111] occurred during an assignment on a public road in June 2015. The protection assistants, who were responsible for the security of a foreign diplomat, noticed the car of a private individual following right behind them, who ignored their orders to maintain a distance several times. When the vehicle of the driver in question stopped at a traffic light, the protection assistants intervened and allegedly acted brutally. One of them even drew his weapon. The driver of the car reported these facts to the Committee.[112]

The Standing Committee I heard testimony from all the protagonists. All internal reports that State Security had drafted in this regard were examined. The Committee also took note of the statutory and regulatory provisions and of the internal directives and rules that applied to close protection assignments.

---

109 The investigation was completed in May 2016.

110 From an earlier review investigation into the use of the so-called 'secret funds' of State Security, it transpired that during the cited period little control was exercised over how money was dealt with at local level, or accounts were kept locally. In this regard, see: STANDING COMMITTEE I, *Activity Report 2013*, 137–138 and *Activity Report 2014*, 64.

111 This authority was transferred from State Security to the Federal Police (Article 7, 3° of the Intelligence Services Act was replaced by Article 20 of the Act of 21 April 2016, *BOJ* 29 April 2016).

112 The Standing Committee I decided to open a review investigation on 24 June 2015. It had to be suspended several times, however, because of other investigations that the Committee was entrusted with and that were considered more urgent. The final report was approved on 11 May 2016.

The person who was escorted on the day of the incident had permanent protection and was the subject of a threat that was evaluated at level 3.[113] The Committee regarded the fact that the complainant had approached the escort vehicle again and again as a reasonable ground for the State Security agents to believe that the life or physical integrity of the person they had to protect was in serious danger. This concern therefore justified the actions taken against the vehicle and its driver. The incident was undoubtedly the result of carelessness and a lack of insight of the complainant, who did not maintain a proper distance from the State Security vehicle.

However, the Committee was convinced that the incident could have been avoided if the protection team had not experienced communication problems. The team could not communicate adequately with the person involved (no communication panel) and did not have appropriate means of communication.[114] As a result of this, they could not verify their appraisal of the situation. The Committee also found that State Security had no training available for realistic stress situations.

The Standing Committee I deemed that the violence was 'reasonable' under the given circumstances, even if the complainant did not agree and despite the fact that, in hindsight, the situation did not pose a threat.

II.11. A COMPLAINT CONCERNING AN INTERVENTION BY CUTA

In May 2015, the Standing Committee I, together with the Standing Committee P, opened an investigation into how CUTA had played a role in revoking an airline pilot's licence.[115] Although the Committees had questions about the intervention and authority of CUTA, they felt that they were not legally authorised to assess the merits of the reasons for suspending the licence. The investigation limited itself to evaluating the role of CUTA. The investigation was completed in December 2016.

---

113 Level 3 is allocated when the threat is considered possible and probable; it therefore requires special attention by the protection agents.

114 During the assignments, the protection teams and the police services communicated via the ASTRID network. The review investigation in 2014 had already revealed problems in the communication network in certain parts of the country. See STANDING COMMITTEE I, *Activity Report 2014*, p. 44–51 ('II.4. State Security and its statutory close protection assignments').

115 On the basis of Article 63 of the Review Act, a member of the Standing Committee I refrained from participating in the review investigation.

II.11.1. ASSESSMENT MEMORANDA OF CUTA

At the start of 2010, the Directorate-General of the Civil Aviation Authority of the Federal Public Service Mobility and Transport notified CUTA that a Belgian national had threatened to carry out an attack in the country where he had worked as a pilot until 1999. His threats were aimed at forcing the competent authorities to reinstate his pilot's licence, which had been revoked on psychological grounds.

The Directorate-General of the Civil Aviation Authority requested a threat assessment from CUTA, which responded quickly: '*CUTA cannot assess whether (the individual involved) actually made the stated threats. However, the nature of the threats is such that the greatest caution must be taken, even if the individual involved denies making the threat. There is – currently – no other information available that would call the police's version into doubt.*' Furthermore, *'an examination of the individual's psychological condition seems more than appropriate. If this examination shows he is psychologically unstable, CUTA cannot reach any conclusion other than that the threat must be regarded as serious and that there is a likelihood of him committing an attack. In view of the above, CUTA sets the level of the terrorist or extremist threat posed by the individual in this hypothesis as SERIOUS (level 3)*' (free translation).

The Directorate-General of the Civil Aviation Authority then revoked the pilot's licence in Belgium. Since there were doubts about the complainant's fitness to retain his licence, he was ordered to undergo a medical examination. This happened in April 2010 and it was decided that the complainant could retain his licence, on condition that he undergo a psychiatric evaluation every year.

CUTA made a new assessment in May 2010. In view of the medical report, the threat level was reduced to level 2. The assessment memorandum stated: '*CUTA continues to regard the gravity of the threat posed by Mr X, in view of the specific threats made in the past, as serious. However, the likelihood of him carrying out the threat, in view of the above psychiatric report, is today deemed to be unlikely*' (free translation). And the memorandum also states: '*However, in this context, it is not legally up to CUTA to give advice on the appropriateness of issuing a new licence to Mr X*' (free translation).

II.11.2. ONE OF CUTA'S POWERS?

The functional (*rationae materiae)* powers of CUTA are described in Article 3 of the Act of 10 July 2006 on the assessment of the threat (Threat Assessment Act) and explained in the Royal Decree of 28 November 2006 implementing the Threat Assessment Act (Threat Assessment Decree). Envisaged are the threats

summarised in Article 8, 1°, b) and c) of the Intelligence Services Act, namely terrorism[116] and extremism.[117] These threats must also be directed against the integrity of people in Belgium and of Belgian nationals abroad, the critical national infrastructure under certain conditions, the defined events or groupings, and the institutions and Belgian interests abroad.

In its first assessment memorandum, CUTA believed that the threat was of a terrorist and extremist nature. According to the initial information, the purpose of the threat was to force the competent authorities to reinstate the pilot's licence.

Since it felt obliged to give an urgent decision, CUTA carried out its assessment based only on the information elements that had been brought to its attention. The following criteria were taken into account:

- The gravity of the threat;
- The reliability of the source of information, which was immediately regarded as established since it involved a foreign police service;
- The ability of the complainant to execute that threat, which was deemed to be established given his profession;
- The likelihood that the individual would execute the threat, which was deemed positive considering his psychological condition.

However, these elements were not verified against the position that the complainant had clarified to the Directorate-General of the Civil Aviation Authority.

The Committees felt that the available information showed that the threats were made for personal reasons and not based on any ideological or political motives. There was accordingly no terrorist or extremist threat in this case. The statutory authority of CUTA to perform an assessment was therefore not established. However, both Committees recognised the difficult situation that CUTA found itself in relating to the request from the Directorate-General of the Civil Aviation Authority.

---

116 Article 8, 1°, b) of the Intelligence Services Act defines terrorism as '*the use of force against persons or material interests for ideological or political reasons with the aim of achieving his objectives by means of terror, intimidation or threats*' (free translation).

117 Article 8, 1°, c) of the Intelligence Services Act defines extremism as '*racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or aims, regardless of whether they are of a political, ideological, religious or philosophical nature, which in theory or in practice conflict with the principles of democracy or human rights, with the proper functioning of democratic institutions, or with other foundations of the rule of law*' (free translation).

II.12. INDIVIDUAL THREAT ASSESSMENTS BY CUTA

II.12.1. INVESTIGATIVE STRUCTURE

CUTA's task is to determine the threat level in relation to terrorism and extremism. This threat level can be determined, among other things, for events, places or individuals. In March 2015, the Standing Committees I and P opened a joint investigation into '*how CUTA determines the threat level posed by or to an individual, into the consequences that this threat level has for the division of duties, the measures to be adopted and the exchange of information among the services involved, as well as into the practical implications for the person involved and his monitoring*' (free translation). This occurred at the request of the Monitoring Committee in the Chamber of Representatives, which wished to be informed of the following questions:

- What criteria does CUTA apply to determine the threat level in relation to an individual?
- Which body sets out the tasks of the services involved once the threat level has been determined?
- What operational measures result from a specific threat level and which service is tasked with their coordination?
- How are the flows of information among the various services organised?
- What are the concrete implications for an individual who is the target of a specific threat level?
- How is the 'classification' of this individual monitored by the local police and administrative authorities?

An interim report was sent to the Monitoring Committee in February 2016. As a corollary of the work for the parliamentary inquiry committee on 'terrorist attacks', both committees decided that the investigation no longer had current value and ended it. Only the interim results of the investigation are therefore discussed below.

II.12.2. LEGAL FRAMEWORK

Pursuant to the Threat Assessment Act of 10 July 2006, the coordination unit has three assignments, including '*to perform a joint assessment on an* ad hoc *basis that must enable one to judge whether threats linked to terrorism and extremism exist and what measures are necessary in such a case*' (Article 8, 2 of the Threat

Assessment Act – free translation). CUTA is therefore not authorised to assess threats other than those related to terrorism and extremism.[118]

The Royal Decree implementing the Threat Assessment Act of 10 July 2006 (Threat Assessment Decree) stipulates that the coordination unit's assessments must relate, on the one hand, to persons, groups, items or events that could involve a terrorist or extremist threat and, on the other hand, to people, groups or items that could be the target or victim of such a threat. For the sake of completeness, it must be noted that the service is also authorised to perform threat assessments for critical infrastructures.

The King determined the terms and conditions for the assessments. Article 11 §6 of the Threat Assessment Decree describes two assessment criteria for the threat level: first, the gravity of the danger or threat and, second, the likelihood of that danger or threat. In order to determine the gravity of any threat (this goes for threats to specific people as well), CUTA determines a 'level' that goes from 1 (low) to 4 (very serious) (Art. 11 §6 of the Threat Assessment Decree).

II.12.3. THREAT ASSESSMENTS BY CUTA (2011–2015)

An internal CUTA memorandum from 2011 stated that '*the* ad hoc *assessment […] always includes the following: an account of the event, a description of the context (political situation, historical precedents, etc.), the determination of the threat level and, where applicable, the proposal of specific measures*' (free translation). The memorandum also prescribed that the assessment had to be subject to quality control on the basis of informal peer counselling.

An earlier review investigation revealed that there were no formal methods or analysis criteria in place for making those assessments.[119] Given the specific nature of each case and the application of 'general analysis principles', CUTA did not even believe it was useful to have a formal assessment procedure. The only quality guarantee involved the verification by management that the assessment conformed to the general policy line of CUTA.

The situation barely evolved between 2013 and 2015. The Committees found that CUTA did not consider it necessary to adapt its working methods.

---

118 For example, threats linked to espionage fall under the authority of the intelligence services and threats involving an attack on the public order or that are linked to organised crime fall under the authority of the Federal Police.

119 STANDING COMMITTEE I, *Activity Report 2012*, 40–42 ('II.5. Joint investigation into the threat assessments by the Coordination Unit for Threat Assessment (CUTA) relating to foreign VIP visits to Belgium').

As part of this review investigation, the Standing Committees I and P analysed some 30 assessments relating to seven individual case files[120] and made the following findings:

- Until the end of 2015, no formal methodology or clear criteria were used to determine the gravity, likelihood and thus the level of threat with regard to or posed by people. The methodology as stipulated in Article 11 §6 of the Threat Assessment Decree, setting out two assessment criteria for the threat level (*supra*), was hardly ever explicitly applied;
- CUTA seldom complied with its own assessment rules. The assessments carried out between 2012 and 2015 were often brief and paid little attention to contextualisation. There were no real assessments;
- Problems were detected in the flows of information between the police services, the judicial authorities and CUTA. The classification of certain information by the intelligence services moreover prevented it from being distributed and used by the authorities entrusted with the implementation of the security measures;
- As soon as the Crisis Centre received threat assessments, these were discussed with the representatives of the different services and authorities. Most measures were discussed jointly before the Government's Crisis Centre made the decision. Where CUTA did make proposals for measures, they were too vague.

II.12.4. A NEW METHODOLOGY

In 2015, the National Security Council and the Strategic Committee for Intelligence and Security ordered CUTA and the Crisis Centre to flesh out a methodology for *ad hoc* assessments '*that can determine the threat level as precisely as possible*' (free translation). The working method proposed by both services distinguished among three types of analyses:

- The threat against persons, events or interests;
- The threat posed by individuals and/or groups;
- The general threat in Belgium.

It was proposed that the methodology for evaluating the threat for the first category (persons, events or interests) would be based on the analysis of three factors:

[120] These were selected during the three years following the joint 2012 investigation of both Committees. During that period, CUTA carried out around 1,000 assessments per year, with over 1,500 in 2015.

- The basic information that gives rise to the evaluation (what is the source of the information? Is it reliable and credible?);
- The likelihood of the information (information must be assessed as 'highly unlikely', 'unlikely', 'possible', 'likely' or 'certain');
- The degree of gravity ('very low', 'low', 'average', 'high', 'very high', 'critical') of the impact on security, public order, the infrastructure, and life of citizens.

A score must be given to each of those factors and a threat level (from 1 to 4) will then be obtained based on the combination of those scores in an assessment matrix. Provision was also made for an internal and external control level.

This new methodology, proposed in October 2015, was submitted for evaluation to the two Ministers in charge. Since the methodology was not implemented during the course of this investigation, the Committees were unable to evaluate its application.

II.13. SPECIFIC DYSFUNCTIONS WITHIN CUTA

The Standing Committees I and P received two anonymous letters in the second half of 2015. They referred to 'irregularities' and 'serious structural problems' within CUTA. The Committees later also received a complaint about the internal functioning of CUTA. In October 2015, the Standing Committees I and P grouped all issues into a '*joint investigation into the report of internal dysfunctions within CUTA*' (free translation).[121]

The first complaint related to the preparation of individual records on foreign terrorist fighters.[122] The complainant believed that the performance of this assignment was incompatible with his function as an expert. Article 3 of the Threat Assessment Decree stipulates that CUTA may have (statutory) analysts and (seconded) experts, each with their own profile.[123] The Committees took the position

---

121 The final report was approved in September 2016.

122 The Circular of 21 August 2015 on the exchange of information and monitoring of FTFs instructs CUTA to prepare an individual intelligence record as soon as a person emerges as a potential FTF. The service must also adopt the necessary measures to monitor this person as soon as possible.

123 Annex 3 to the Threat Assessment Decree defines the profiles.
'Subject to the authority of CUTA director or his/her delegated head of department, the analyst is responsible for gathering and searching for information and intelligence on the phenomenon of terrorism as classified into, among others, geographical, ethnic and religious spheres of interest. The analyst must also thoroughly analyse the geopolitical situation linked to these spheres of influence, according to his/her professional specialisation. The analyst is also responsible for adding his/her processed data to the specialised CUTA documentation files. He/she is tasked with analysing the gathered data and processing it in periodic, strategic assessments, in cooperation with the experts seconded from the various support services' (free translation). The analyst also participates in meetings, domestically and abroad, on terrorism and extremism, and in a permanent-service rotation.

that preparing individual records involved an *ad hoc* assessment of the threat posed by every FTF. Assigning this task to the experts was therefore not incompatible with their profile. Naturally the analysts were assigned tasks in this regard as well. That was not incompatible with their profile either. During the course of the investigation, it could be determined that the division of duties between experts and analysts for the purpose of preparing the FTF records was adjusted to achieve a better balance.

A second section of the complaint concerned the irregular secondment of a contractual staff member of a support service to CUTA. Indeed, the secondment of a contractual agent was contrary to Article 83 of the Royal Decree of 23 January 2007 on the personnel of the Coordination Unit for Threat Assessment.[124, 125] Only an amendment to the regulations would regularise the secondment of contractual staff members.[126]

The anonymous complainant further alleged that an expert had received preferential treatment from management and had been favoured in relation to training. The Standing Committees I and P did not find any indication of this.

Another claimant cited the – according to him unjust – decision to end his secondment. The Standing Committees I and P refrained from judging the merits of this decision. However, they did find that several prior incidents had complicated the professional and personal relationship between management and the complainant. They were of the opinion that the manner in which the formal decision was taken disregarded the general principle of proper management. Nonetheless, the Committees did not have the authority to undo or overrule the decision.[127]

The complaint also made reference to unnecessary travel and inappropriate international contacts of CUTA. The Committees had previously investigated those allegations.[128] The complaint did not contribute any new information in this regard.

'*The expert […] is responsible for gathering and searching for information and intelligence on the geopolitical situation and the phenomenon of terrorism […]. He/she is tasked with the permanent analysis of the obtained data and responsible for processing it in useful,* ad hoc *assessments on the potential terrorist threat, in close cooperation with the other experts and analysts at CUTA*' (free translation). The expert also functions as a liaison officer with his/her original service. He/she is responsible for adding to and updating the processed data in the specialised CUTA documentation files.

124 '*The positions of experts and administrative staff at CUTA are filled through the secondment of permanent officials in the support services in accordance with an allocation that is made by the National Security Council on the recommendation of the director and deputy director*' (free translation).

125 CUTA management insisted that the secondment had never been the subject of any appeal and that it was very satisfied with the individual's work. However, this did not undo the irregularity.

126 CUTA management took an initiative in this regard but did not receive any response from the Ministers in charge.

127 The Committees took note of the fact that the complainant did not appeal to the Council of State or the competent courts.

128 STANDING COMMITTEE I, *Activity Report 2015*, 132–135 ('II.7. International contacts of CUTA').

In relation to the comment about 'latent alcohol problems' among some staff members, management was asked to evaluate the objective scope of the problem and report on the preventative or disciplinary measures adopted. The Committees took note of the adopted measures.

Lastly, the complainant stated that pressure was put on him not to raise the aforementioned dysfunctions. Due to an absence of tangible elements, the Committees were unable to consider this allegation.

II.14. A COMPLAINT CONCERNING A SECURITY INVESTIGATION AT GISS

II.14.1. CONTEXTUALISATION

In April 2015, the Standing Committee I received a complaint about a security investigation conducted by GISS. More specifically, the complainant alleged that GISS had processed incorrect information about her as part of its security investigation into her husband. She believed that she was being accused of having unlawfully obtained information from the Immigration Office (IO) database about a member of Defence with whom her husband had been in contact. The complainant strenuously denied this. She explained that GISS had incorrectly entered personal information in its database and that this had raised doubts about her professional integrity.[129]

II.14.2. FINDINGS

GISS based its security investigation for this case solely on data that was gathered in accordance with statutory provisions.[130] This firstly involved personal data that the applicant, and by extension his partner, had provided in the basic questionnaire and, secondly, additional intelligence (administrative, police and judicial data) gathered by the intelligence service.[131] After examining the security file, the Committee determined that the complainant's name did not feature in the decision on the security investigation and that GISS had never besmeared her integrity.

---

129 Her husband did not agree to the reduced level of his new security clearance and successfully appealed this to the Appeal Body for security clearances, certificates and advice. The review investigation had to be suspended because of these appeal proceedings. The investigation was closed in March 2016.

130 The Act of 11 December 1998 on classification and security clearances, certificates and advice and the Directive of 16 February 2000 of the (then) Ministerial Committee for intelligence and security on the scope of security investigations.

131 This data can be accessed only by GISS agents who are specifically designated for that purpose and only insofar as knowledge of and access to that data is essential for the performance of their duties and assignments to process this data for the purpose of a security clearance application.

II.15. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2016 AND INVESTIGATIONS INITIATED IN 2016

II.15.1. INFORMATION POSITION OF CUTA BEFORE THE PARIS ATTACKS

Almost immediately after the Paris attacks in November 2015, the Standing Committee I opened a review investigation into the information position of the two Belgian intelligence services (see II.3 in this regard). The Standing Committee P also initiated a review investigation into police service operations. At the request of the Parliamentary Monitoring Committee, and pursuant to Article 53, 6° of the Review Act, the Standing Committees I and P decided at the end of January 2016 to start a joint investigation into the '*information position of CUTA prior to the evening of 13 November 2015 regarding the individuals or groups that perpetrated or were involved in the Paris attacks*' (free translation). The purpose of the investigation was to determine what information CUTA had in relation to people who were involved in the terror attacks and to examine whether the coordination unit had requested and/or obtained information from various support services and foreign partner services prior to the attacks.

Because both Committees had to carry out other investigations – with higher priority – in mid-2016 for the parliamentary inquiry committee on 'terrorist attacks', the investigation was suspended. Since the director of CUTA subsequently gave evidence several times before the inquiry committee, which *de facto* dealt with the investigative questions, the Committees no longer regarded it relevant to resume the investigation activities.[132]

II.15.2. INTERNATIONAL EXCHANGE OF DATA ON FOREIGN TERRORIST FIGHTERS

During an international meeting with various European review bodies[133], it was decided to start a similar review investigation in all participating countries into the international cooperation between the various intelligence services with

---

132 In their joint meeting of 13 June 2017, both Committees decided to close the review investigation and not draw up a final report. The chairperson of the Monitoring Committee was advised of this decision on 15 June 2017 and did not object.

133 The Belgian Standing Intelligence Agencies Review Committee, the Dutch Intelligence and Security Services Review Committee (CTIVD), the Swiss Strategic Intelligence Service Supervision and delegations from Sweden (Commission on Security and Integrity Protection), Norway (Parliamentary Oversight Committee) and Denmark (Intelligence Oversight Board). In this regard, see STANDING COMMITTEE I, *Activity Report 2015*, 80–81.

regard to the fight against foreign terrorist fighters (FTFs). This initiative subsequently received the express support of the chairperson of the Monitoring Committee. The intention is for every review body to study this theme from its own perspective and authority but based on the same philosophy and with a certain common approach.

The structure of the Belgian section of the investigation[134] consists in trying to obtain the clearest and most complete picture possible of the formal (but also informal) bilateral or international exchange of information between State Security and GISS, on the one hand, and foreign services, working groups or cooperative arrangements on the other hand, in relation to the FTF problem.

The ultimate aim of the investigation is to assess the exchange of information and, if necessary, to make recommendations to optimise this so that the information position of the services involved can be improved, without undermining the fundamental rights of citizens.

In the second half of 2016, various investigations were carried out both nationally and internationally. The results of the Belgian review investigation will – where possible, given restrictions due to classified information – be used as input for the international investigation.

134 The investigation started at the end of August 2016 after the initiative had been submitted to and approved by the Monitoring Committee of the Chamber of Representatives.

CHAPTER III
CONTROL OF SPECIAL INTELLIGENCE METHODS

This chapter summarises the use of special intelligence methods by State Security and GISS in 2016, and the manner in which the Standing Committee I has performed its jurisdictional control in this regard.[135] It is based on the report that the Standing Committee I drew up pursuant to Article 35 §2 of the Review Act of 18 July 1991.[136]

The first part, however, deals with the four Acts that entered into force during the course of 2016 and introduced an amendment for SIM methods. Because of these amendments, it is not yet possible to compare the figures of the 2016 operating year with those of previous years.

For obvious reasons, this chapter does not yet take two other legislative amendments into account. The first is the so-called PNR Act of 25 December 2016.[137] Although this was voted on by Parliament in the year under review, it had not entered into force yet. The second is the far-reaching amendment to the SIM Act which was debated in Parliament in 2016 but only came into force on 8 May 2017.

---

135 The SIM Commission is responsible for the *a priori* review of the use of special intelligence methods. In this regard, see: STANDING COMMITTEE I, *Activity Report 2010*, 59–60 ('III.1.2. Control by the SIM Commission') and P. DE SMET, 'Check and balances. A priori and a posteriori review', in VAN LAETHEM, W., VAN DAELE, D. and VANGEEBERGEN, B. (eds.), *De Wet op de bijzondere inlichtingenmethoden* (The Act on special intelligence methods) Intersentia, Antwerp, 2010, 93–118.

136 Under the Act of 5 February 2016 amending criminal law and criminal procedure and regarding various provisions in the matter of justice (*BOJ* 19 February 2016), modifying Article 35 §2, first paragraph of the Review Act, the Committee, as from 2016, will no longer report on the application of the SIM methods '*every six months*' but '*annually*'.

137 Full description: the Act of 25 December 2016 on passenger data processing, *BOJ* 25 January 2017. PNR stands for Passenger Name Record.

III.1. FOUR LEGISLATIVE AMENDMENTS FROM 2016

III.1.1. A NEW ASSIGNMENT FOR THE INTELLIGENCE SERVICES

Under the Act of 29 January 2016[138] both intelligence services were expressly given the assignment of '*collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory*' (Articles 7, 3°/1; and 11 §1, 5° of the Intelligence Services Act – free translation). Under Article 18/1, first paragraph, 1° and 2° of the Intelligence Services Act, both State Security and GISS may use specific or exceptional methods in this regard. In many cases, this new power is closely connected to the ability to monitor foreign intelligence services engaging in espionage or interference in Belgium. The Committee noted that the intelligence services referred to this latter threat and not the new power in such cases. The Standing Committee I drew the attention of State Security and GISS to this fact, so that an accurate picture of the use of this new power can be created in future.

III.1.2. IDENTIFICATION OF THE USER OF TELECOMMUNICATION OR OF A USED MEANS OF COMMUNICATION AS AN ORDINARY METHOD

Under the Act of 5 February 2016 amending criminal law and criminal procedure and regarding various provisions in the matter of justice (*BOJ* 19 February 2016) – following the recommendations of the Standing Committee I[139] – the identification of the user of telecommunication or of a used means of communication is regarded as an ordinary method to the extent that this happens through a request to or direct access to the customer files of an operator. This was previously a specific method. The amendment was made through the addition of the new Article 16/2 to the Intelligence Act of 30 November 1998.

If the identification (and localisation) is made with the help of a technical resource – and thus not through a request to an operator – the collection remains a specific method. Articles 18/2 §1 and 18/7 §1 of the Intelligence Services Act were amended for this purpose. A new specific method was also included in these provisions: obtaining payment method data, the identification of the payment instrument and the date of payment for the subscription or for the use of the electronic communications service through a request to an operator of an electronic communications network or a provider of an electronic communications service, or by direct access to the relevant files.

---

138 *BOJ* 24 February 2016.

139 STANDING COMMITTEE I, *Activiteitenverslag 2012* (Activity Report 2012), 69.

The new arrangement imposes an obligation on State Security and GISS to keep a register of all requested identifications and of all identifications made through direct access. The Standing Committee I receives a monthly list of the identifications requested and of each access.

This legislative amendment entered into force on 29 February 2016. This meant it was not straightforward for the Committee to produce figures that allow for a full comparison with previous years (see further under III.2).

III.1.3. A NEW DATA RETENTION LAW WITH IMPLICATIONS FOR THE INTELLIGENCE SERVICES

Since the Act of 29 May 2016,[140] the obligation for operators to retain metadata for twelve months has been changed. This legislative amendment was the result of a ruling of the European Court in Luxembourg and a judgment of the Constitutional Court.

The legislative amendment also had consequences for the use of some specific methods by the intelligence services. For example, requesting certain data through operators became limited in time. Article 18/8 of the Intelligence Services Act makes it possible for both intelligence services '*when necessary, by requesting cooperation from the operator of an electronic communications network or from the provider of an electronic communications service, to proceed with or make arrangements for: 1. tracing the call-associated data of electronic communication devices from which or to which calls are being or have been made; 2. tracing the origin or destination of electronic communications.*' (free translation). If State Security or GISS wish to obtain this data through an operator, the Act sets the following restrictions: for a potential threat that relates to an activity that may relate to criminal organisations or harmful sectarian organisations, the head of the service, in his decision, can only request the data for a period of six months prior to the decision. If the threat relates to espionage, interference or proliferation, this period may be nine months. The period for activities that relate to terrorism or extremism is twelve months prior to the decision.

This new arrangement means that GISS is also statutorily obliged to indicate which of these specific threats its collection falls under. This is new in the sense that GISS is normally not bound by these seven threats in its operations. However, little will change in practice because GISS has always referred to one of the seven threats in its SIM decisions.

Lastly, it must be noted that the detailing of this system did not take the new power of State Security and GISS to monitor the activities of foreign services in Belgian territory into account. A maximum period for the inspection of metadata should be specified regarding the latter as well.

140 *BOJ* 18 July 2016.

III.1.4. IDENTIFICATION OF A PREPAID-CARD HOLDER

The Act of 1 September 2016 (*BOJ* 7 December 2016) introduced a new ordinary method in Article 16/2 of the Intelligence Services Act: '*§2. For the purpose of performing their assignments, the intelligence and security services may request a bank or financial institution to cooperate in identifying the end user of the prepaid card referred to in Article 127 of the Act of 13 June 2005 on electronic communications, based on the reference of an electronic bank transaction that relates to the prepaid card and that is communicated in advance by an operator or provider pursuant to section 1*' (free translation). State Security and GISS must – as when the user of telecommunications or of a used means of communication is identified (see III.1.2) – keep a register of all requested identifications.

This system only entered into force in mid-December 2016. It has not given rise to specific applications.

III.2. STATISTICS RELATING TO SPECIFIC AND EXCEPTIONAL METHODS

Between 1 January and 31 December 2016, a combined total of 1,868 authorisations was granted by the two intelligence services for the use of special intelligence methods: 1,747 by State Security (of which 1,558 specific and 189 exceptional) and 121 by GISS (of which 88 specific and 33 exceptional).

The following table draws a comparison with the figures of previous years.

	GISS		State Security		TOTAL
	Specific methods	Exceptional methods	Specific methods	Exceptional methods	
2013	131	23	1,102	122	1,378
2014	114	36	976	156	1,282
2015	87	34	1,143	128	1,392
2016	88	33	1,558	189	1,868

On the one hand, these figures show that the *status quo* has been maintained for GISS and, on the other hand, that there was a significant increase (of no less than 34%) for State Security. However, in order to make a proper comparison with the figures of last year, the fact that 'ordinary identifications through the operator' have not been regarded as a specific method since 29 February 2016 must also be taken into account (see III.1.2).

From March 2016, State Security made no fewer than 2,203 requests to operators, while GISS made 216 requests. A comparison with the figures of 2015 shows that this would correspond to more than 1,700 methods of 'identifications

through operators' for State Security and around 60 for GISS.[141] State Security only used a fraction of these methods in 2015. Only 663 'identifications' were authorised.[142] It certainly must not be concluded from this enormous increase in 2016 that the streamlined procedure led to ill-considered use of this method. After all, the monthly figures for the requests to operators for the period 2015 and 2016 show that the large increase in the number of identifications relates to the attacks in Paris, Zaventem and Maalbeek.

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

III.2.1. METHODS WITH REGARD TO GISS

III.2.1.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Entry into and surveillance of or in places accessible to the public, using a technical device	14	7	4	2
Entry into and searching of places accessible to the public, using a technical device	0	0	0	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator	0	0	0	0
Inspection of identification data for electronic communications, requesting the cooperation of an operator, or direct access to data files	66 methods	67 methods	55 methods	–[143]
Inspection of identification data of electronic communications through a technical resource; or requesting the cooperation of an operator in connection with the payment instrument or method of a user	–	–	–	12 methods

141 After all, the use of one identification method usually implies multiple requests to different Belgian operators.

142 GISS used this method 55 times in 2015.

143 From 29 February 2016, this method has, on the one hand, been narrowed to '*the identification or localisation, with the help of a technical resource, of the electronic communication services and devices to which a specific person has subscribed or that are usually used by a specific person*' and, on the other hand, been broadened to '*the request made to the operator of an electronic communications network or the provider of an electronic communication service to obtain payment method data, the identification of the payment instrument and the date of payment for the subscription or for the use of the electronic communications service*' (free translation) (see III.1.2 in this regard).

NATURE OF SPECIFIC METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Inspection of call-associated data for electronic communications and requesting the cooperation of an operator	15	12	12	42
Inspection of localisation data for electronic communications and requesting the cooperation of an operator	36	28	16	32
TOTAL	**131**[144]	**114**	**87**	**88**

The number of 'inspections of identification data' was higher in previous years purely because identifications through operators are being regarded as an ordinary method since February 2016 (III.1.2). An approximate comparison with last year shows a slight increase. However, the number of 'inspections of call-associated data' and of 'localisations' has increased far more: tripling and doubling respectively. The average duration of the localisation also increased significantly (from 164 to 201 days).

These figures show that the trend observed in 2014 and 2015, when less use was made of identifications and localisations, did not continue.

III.2.1.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Entry into and surveillance in places not accessible to the public, with or without a technical device	1	1	3	1
Entry into and searching of places not accessible to the public, with or without a technical device	0	1	0	0
Setting up and using a fictitious legal person	0	0	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	0	0	0	1
Collecting data on bank accounts and banking transactions	5	5	3	11
Penetrating IT systems	0	3	3	4
Monitoring, intercepting and recording communications	17	26	25	16
TOTAL	**23**[145]	**36**	**34**	**33**

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

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

In relation to exceptional methods, the number of tapping measures decreased significantly, while far more banking details were requested.

III.2.1.3. Interests and threats justifying the use of special methods[146]

Since the entry into force of the Act of 29 January 2016 on monitoring the activities of foreign intelligence services in Belgium (see III.1.1), GISS may use specific and exceptional methods in relation to four instead of three assignments:

- The intelligence assignment focused on threats against, among other things, the inviolability of the national territory, the military defence plans, and the scientific and economic potential in the area of defence (Article 11, 1° of the Intelligence Services Act);
- The military security assignment focused, for example, on safeguarding the military security of defence personnel, military installations, and military IT and network systems (Article 11, 2° of the Intelligence Services Act);
- The protection of military secrets (Article 11, 3° of the Intelligence Services Act);
- Collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory (Article 11, 5° of the Intelligence Services Act). This relates to the new assignment for which special intelligence methods can be used.

NATURE OF INTEREST	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Intelligence assignment	111	109	112	64
Military security	15	5	6	1
Protection of secrets	28	36	4	1
Monitoring the activities of foreign services in Belgium	–	–	–	Not known

NATURE OF THREAT	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Espionage	94	123	101	55
Terrorism (and radicalisation process)	6	7	4	5
Extremism	24	15	13	6
Interference	1	0	4	0
Criminal organisation	16	2	0	0
Other	13	0	0	0

146 Each authorisation may involve multiple interests and threats.

Despite the fact that the number of methods remained the same, the figures on the 'nature of the interest' and 'nature of the threat' show a sharp decrease across the board. This is simply because of a different registration method. The nominal figures are significantly lower, but the relationships between them remained almost the same. In relation to the use of special methods, espionage remains the main threat for GISS.

III.2.2. METHODS WITH REGARD TO STATE SECURITY

III.2.2.1. Specific methods

NATURE OF SPECIFIC METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Entry into and surveillance of or in places accessible to the public, using a technical device	109	86	86	125
Entry into and searching of places accessible to the public, using a technical device	0	0	0	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator	0	0	0	0
Inspection of identification data for electronic communications, requesting the cooperation of an operator or direct access to data files	613 methods	554 methods	663 methods	[147]
Inspection of identification data of electronic communications through a technical resource; or requesting the cooperation of an operator in connection with the payment instrument or method of a user	–	–	–	215 methods
Inspection of call-associated data for electronic communications and requesting the cooperation of an operator	136	88	33	622
Inspection of localisation data for electronic communications and requesting the cooperation of an operator	244	248	361	596
TOTAL	**1,102**	**976**	**1,143**	**1,558**

147 From 29 February 2016, this method has, on the one hand, been narrowed to '*the identification or localisation, with the help of a technical resource, of the electronic communication services and devices to which a specific person has subscribed or that are usually used by a specific person*' and, on the other hand, been broadened to '*the request made to the operator of an electronic communications network or the provider of an electronic communication service to obtain payment method data, the identification of the payment instrument and the date of payment for the subscription or for the use of the electronic communications service*' (free translation) (see III.1.2 in this regard).

As indicated above, the total number of authorisations for the use of specific methods by State Security has increased very significantly. The above table shows that this is almost completely due to the 'inspection of call-associated data' that increased from just 33 cases in 2015 to 622 in 2016. But the number of observations and localisations also increased. Lastly, there has also been a significant growth in 'identifications', which have been regarded as an ordinary method if they are made through an operator since February 2016. Based on the available data, the Committee estimates that the number of identifications used exceeds 1,700.

This sharp increase in the number of special methods used obviously coincides with the wave of terrorist attacks.

III.2.2.2. Exceptional methods

NATURE OF EXCEPTIONAL METHOD	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Entry into and surveillance in places not accessible to the public, with or without a technical device	6	9	6	7
Entry into and searching of places not accessible to the public, with or without a technical device	6	21	8	18
Setting up and using a fictitious legal person	0	0	0	0
Opening and inspecting post, whether or not entrusted to a postal operator	6	18	5	8
Collecting data on bank accounts and banking transactions	11	8	6	6
Penetrating IT systems	12	18	16	27
Monitoring, intercepting and recording communications	81	86	87	123
TOTAL	122[148]	156	128	189

The many attacks, both in Belgium and abroad, have turned the decrease noted in the number of applied exceptional methods in 2015 into a sharp increase. Mainly the number of searches (from 9 to 22), intrusions into IT systems (from 16 to 27) and tapping measures (from 91 to 123) were responsible for this increase. There were not only more measures, their average duration was also significantly longer.

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

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

The following table lists the threats (and potential threats) for which State Security issued authorisations for specific and exceptional methods. Of course, a single method may be directed against multiple threats. State Security may use specific methods in respect of all threats falling within its competence (Article 8 of the Intelligence Services Act). Exceptional methods could not yet be used in the context of extremism and interference in 2016 (but this is possible from 2017). However, they are allowed in the context of the radicalisation process that precedes terrorism (Article 3, 15° of the Intelligence Services Act). The Act uses the following definitions (free translation):

1. Espionage: seeking or providing intelligence which is not accessible to the public and the maintenance of secret relationships which could prepare for or facilitate these activities;
2. Terrorism: the use of force against persons or material interests for ideological or political reasons with the aim of achieving its objectives by means of terror, intimidation or threats;
3. Radicalisation process: a process whereby an individual or a group of individuals is influenced in such a manner that this individual or group of individuals is mentally shaped or is prepared to commit terrorist acts;
4. Extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or aims, regardless whether they are of a political, ideological, religious or philosophical nature, which in theory or in practice conflict with the principles of democracy or human rights, with the proper functioning of democratic institutions or with other foundations of the rule of law;
5. Proliferation: trafficking in or transactions with respect to materials, products, goods or know-how which can contribute to the production or the development of non-conventional or very advanced weapon systems. In this context, this refers, among other things, to the development of nuclear, chemical and biological weapons programmes and the transmission systems associated with them, as well as the persons, structures and countries involved;
6. Harmful sectarian organisations: any group with a philosophical or religious purpose or which appears to be such and which, in terms of its organisation or practices, carries out harmful illegal activities, causes harm to individuals or society, or violates human dignity;
7. Interference: an attempt to use illegal, fraudulent or clandestine means to influence decision-making processes;
8. Criminal organisations: any structured association of more than two people that endures over time, aiming to carry out criminal acts and offences by mutual agreement, in order to directly or indirectly acquire material benefits,

where use is made of intimidation, threats, violence, trickery or corruption, or where commercial or other structures are used to conceal or facilitate the commission of crimes. This means the forms and structures of criminal organisations which have a substantial relationship to the activities referred to in the above threats, or which could have a destabilising impact at a political or socio-economic level.

Since the entry into force of the Act of 29 January 2016 on monitoring the activities of foreign intelligence services in Belgium (see III.1.1), State Security may use specific and exceptional methods for '*collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory*' (Article 7, 3/1° of the Intelligence Services Act – free translation).

Bearing in mind that various threats may be at play for each authorisation, the figures are the following:

NATURE OF THREAT	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Espionage	359	319	253	209
Terrorism (and radicalisation process)	580	499	812	684
Extremism	246	267	171	67
Proliferation	15	33	30	6
Harmful sectarian organisations	9	0	0	0
Interference	8	10	10	15
Criminal organisations	9	8	0	0
Monitoring the activities of foreign services in Belgium[149]	–	–	–	Not known

The above figures show that 'terrorism' has remained the absolute priority at State Security for the use of SIM methods.

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

– The internal security of the State and maintenance of democratic and constitutional order, namely
  a) the security of the institutions of the State and the protection of the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to

149 This power was only introduced by the Act of 29 January 2016 (see III.1.1).

every constitutional state, as well as human rights and fundamental freedoms;
b) the safety and physical and moral protection of persons and the safety and protection of goods;

– The external security of the State and international relations: the protection of the inviolability of the national territory, the sovereignty and independence of the State, the interests of the countries with which Belgium is striving towards a common goal, and the international and other relationships which Belgium maintains with other States and international or supranational institutions;
– Safeguarding the key elements of the scientific or economic potential.

Bearing in mind that different interests may be at play for each authorisation, the figures for 2016 are the following:

NATURE OF INTEREST	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
Internal security of the State and maintenance of democratic and constitutional order	1,177	1,100	1,258	968
External security of the State and international relations	1,160	1,075	1,150	927
Safeguarding the key elements of the scientific or economic potential	11	10	4	13

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

III.3.1. STATISTICS

This section deals with the activities of the Standing Committee I in relation to specific and exceptional intelligence methods. Attention will only be paid to the jurisdictional decisions made in this regard. However, it must first be stressed that the Committee subjects *all* authorisations to use special methods to a *prima facie* investigation, with a view to whether or not they should be referred.

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

– At its own initiative;
– At the request of the Data Protection Commission;
– As a result of a complaint from a citizen;

– By operation of law, whenever the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and has prohibited the use of the data;
– By operation of law, if the competent Minister has issued an authorisation based on Article 18/10, §3 of the Intelligence Services Act.

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

METHOD OF REFERRAL	NUMBER 2013	NUMBER 2014	NUMBER 2015	NUMBER 2016
1. At its own initiative	16	13[150]	16	3
2. Data Protection Commission	0	0	0	0
3. Complaint	0	0	0	1
4. Suspension by SIM Commission	5	5	11[151]	19
5. Authorisation by Minister	2	1	0	0
6. Pre-judicial consulting body	0	0	0	0
TOTAL	**23**	**19**	**27**	**23**

This table shows one noteworthy evolution: the Standing Committee I made significantly fewer referrals at its own initiative, certainly taking into account the increasing number of special intelligence methods. In 2015, 1.1% of case files were referrals at the Committee's own initiative, while in 2016 this was limited to 0.15%. There are two reasons for this. First, it is clear from the *prima facie* check of each SIM file within the Committee that the two intelligence services take due account of the statutory restrictions, the decisions of the SIM Commission and the case law of the Committee. The other reason is that the SIM Commission suspends potentially problematic methods more often (19 cases). As the following table shows, the Committee did fully or partially revoke the suspension by the Commission in 11 of those 19 cases.

It is also interesting to note that for the first time since the introduction of this possibility in 2010, a complaint by a citizen led to a ruling by the Committee. Due to its importance, further attention will be paid to this case (see below).

150 In two cases, the Committee's decision was given only in January 2015.
151 In one case, the referral was made in 2015 but the Committee's decision was given in 2016.

Once a referral has been made, the Committee can make a number of interim or final decisions (the interim decisions are listed under points 3–10; the final decisions under 11–16). In three cases (1, 2 and – sometimes – 6) a decision is taken before the actual referral.

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

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

The Standing Committee I must deliver a final decision within one month of the day on which a referral has been made to it in a particular matter (Article 43, 4° of the Intelligence Services Act). Except for in the complaint file – in which the case had to be postponed – this period was observed in all files.

NATURE OF DECISION	2013	2014	2015	2016
Decisions prior to the referral				
1. Invalid complaint	0	0	0	0
2. Manifestly unfounded complaint	0	0	0	0
Interim decisions				
3. Suspension of method	0	3	2	1
4. Additional information from SIM Commission	0	0	0	0
5. Additional information from intelligence service	0	1	1	4
6. Investigation assignment of Investigation Service	50	54	48	60
7. Hearing of SIM Commission members	0	0	2	0
8. Hearing of intelligence service members	0	0	2	0
9. Decision regarding investigative secrecy	0	0	0	0
10. Sensitive information during hearing	0	0	0	0
Final decisions				
11. Discontinuation of method	9	3	3	6
12. Partial discontinuation of method	5	10	13	4
13. Lifting or partial lifting of ban imposed by SIM Commission	2	0	4	11
14. No legal competence	0	0	0	0
15. Lawful authorisation / No discontinuation of method / Unfounded	7	4	6	2
Pre-judicial opinion				
16. Pre-judicial opinion	0	0	0	0

III.3.2. DECISIONS

The final decisions delivered by the Standing Committee I in 2016 are briefly discussed below. The summaries have been stripped of all operational information. Only those elements relevant to the legal issue have been included. The Committee had to take the necessary care in this regard as many of the decisions were classified (sixteen as CONFIDENTIAL and four as SECRET).

The decisions have been divided into five categories:

- Justification for the authorisation;
- Proportionality and subsidiarity requirements;
- Legality of the method in terms of the applied techniques, data collected, duration of the measure, and nature of the threat;
- Consequences of an unlawful method or an unlawfully implemented method;
- The jurisdictional decision relating to the complaint.

Where relevant, some decisions are included under several categories.

III.3.2.1. Justification for the authorisation

The Committee had to assess in four different cases whether the authorisation to carry out a method was adequately motivated, both in fact and in law.

In the first file, an intelligence service wished to inspect '*data on past connections (particularly IP addresses) with regard to the social network accounts used by a target, for which the period was limited to 90 days before the notice to the SIM Commission*' (free translation) (dossier 2016/4542). The intelligence service had considered this as an inspection of call-associated data. The Committee noted that '*the methods seem more like the localisation of the origin or of the destruction of electronic communications rather than an identification and inspection (…); however, localisation is also a specific method whose conditions are identical to those that apply to identification and inspection and any change to the 'classification' therefore has no effect on legality*' (free translation). The method was therefore not unlawful.

In the second file, the 'factual motivation' was assessed. A foreign intelligence service asked its Belgian partner service to inspect and localise Belgian telephone numbers that had allegedly been used to issue two death threats against foreign dignitaries. The SIM Commission suspended the method because the wording and spirit of the SIM Act require the decision to give more precise indications of the link with 'terrorism' as one of the threats to be monitored (dossier 2016/4707). The Committee asked for additional information from the Belgian service. This did not reveal any direct link to terrorism. But the Committee stated that '*in the current circumstances, death threats made twice against persons related to the*

government […] of a European country can be regarded as 'terrorism' within the meaning of Article 8, 1°, second paragraph, b, even if these threats are currently not very explicit' (free translation).

There was uncertainty about the exact purpose of the intelligence service in another case. In reference to Article 18/16 of the Intelligence Services Act, an intelligence service wished to place software in a certain communication device in order to identify the nature of the communications and listen to conversations (dossier 2016/5365). Because monitoring conversations falls under Article 18/17 of the Intelligence Services Act, a further explanation was requested from the intelligence service concerned. It transpired from this that the intention was *not* to actually monitor the conversations. The Committee therefore decided that the method '*is lawful, insofar as there is no intention to use the method to monitor, inspect or register communications*' (free translation).

The last case related to whether the intelligence service could monitor a group of foreigners who lived in Belgium (dossiers 2016/4875 and 2016/4877). These people who held, or had previously held, important positions in their country of origin were assumed to be members of a certain movement. The intelligence service based its decision on 'interference' as a threat and explained the motives that showed it had an interest in the monitoring. However, the SIM Commission and the Committee found this to be inadequate: '*Considering that it must be concluded that the presentation of both the identified threat and the motives were far from optimal because, for example, the organisation on which the group depends is described as a sectarian organisation simply by referring to a foreign study and that the (actual or potential) interference was inadequately demonstrated because the unauthorised, deceptive or clandestine means were not identified*' (free translation). The Committee therefore requested additional information. '*Considering that after additional investigation, the Committee is unable, in principle, to replace the inadequate motivation of the requested method as put forward by the service with a better motivation; that, in this case, however, and particularly because the organisation is a movement that is trying to gain a foothold in Western Europe, including Belgium, and is relatively new and thus not as well known as other (similar) movements, the Standing Committee I decided to request additional information. This leads the Committee to consider allowing the specific method*' (free translation). After all, there was enough information available to show that this did not only relate to 'interference' but also to 'extremism'. '*Considering that the method is legal for the motives as they were requalified*' (free translation).

III.3.2.2. Proportionality and subsidiarity requirements

A method not only has to comply with a number of statutory requirements, it must also be proportional to the underlying threat and may not be more intrusive than is necessary.

The test of these proportionality and subsidiarity requirements came up in the aforementioned case (dossier 2016/4707). A foreign intelligence service had asked its Belgian sister service to inspect and localise Belgian telephone numbers that had allegedly been used to issue two death threats against members of foreign governments. The Committee held that '*the proposed method needed to allow for the objective assessment of the threats given that ordinary methods are inadequate and the method concerned only involves limited intrusion into the privacy of persons; Considering that any decision to rely on other methods relating to those mobile telephone numbers or their users must specify in more detail why the threat is of a terrorist nature; Considering that the specific method concerned is therefore lawful, proportional and subsidiary*' (free translation).

The issue of proportionality was also raised in dossier 2016/4785. An intelligence service wanted to trace the call-associated data of the means of communication of its target, as well as of some of his family members. In view of the stated motivation and the information provided, the method seemed to be justified in respect of the target. '*However, tracing the call-associated data of the family members is motivated by the possibility that the target could use the telephone of one of his family members*' (free translation). When asked, the service concerned did not have specific indications that the target would use his family members' telephones. The Committee therefore did not regard the use of the intended method in relation to these family members to be proportional.

III.3.2.3. Legality of the method in terms of the techniques applied, data collected, duration of the measure, and nature of the threat

The intelligence services obviously cannot use just any method to gather information about someone. The law sets clear boundaries on various levels: for what kind of threat and in order to protect which interest may a method be used? Which acts may and may not be performed in this regard? By whom, in respect of whom, and in respect of which data? How long may a technique be used? May the measures be used outside Belgium? And so on… The Standing Committee I has explained some of these boundaries in a number of decisions.

III.3.2.3.1. An intelligence purpose, not a judicial purpose

The SIM Commission had suspended a method because it was noted in the intelligence service's decision that the results of the method '*ought to finalise the intelligence file (…) so it can be added to another current judicial inquiry (…) in which State Security is a technical assistant*' (free translation) (dossier 2016/4414). The SIM Commission correctly stated that an intelligence service's duties do not include gathering intelligence to supplement a judicial file. However, the Committee asked for further clarification from the service concerned. It stated that the motivation was too brief. The information provided showed that the

intention was to gain insight into a certain network. As the service therefore did have an intelligence purpose in mind, the method was considered to be lawful.

III.3.2.3.2. Boundaries of the assignments of the intelligence services

The intelligence service wished to determine the means of communication that a group of people were using in order to subsequently localise (file 2016/4633) and observe (dossier 2016/4634) them. This involved people who had been part of a political opposition movement in their country of origin and had requested the status of refugee in Belgium. The service believed that this political movement '*threatens or could threaten the internal security of the State and the maintenance of the democratic and constitutional order, the external security of the State and international relations*' (free translation). The Committee noted that although the service referred to an interest to be protected, the decision did not adequately demonstrate a threatening activity (espionage, interference, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations), other than merely mentioning that the group involved engaged in 'sectarian practices'. The decision did state that the organisation was suspected of '*having tried to infiltrate the state apparatus [of their country of origin]*' (free translation), and that the organisation also tried to exert influence both on the diaspora and on Belgian political decision-makers. The Committee held '*that this motivation does not comply with the definition of interference at all, given that interference legally involves the following: '<u>the attempt to use illegal, deceptive or clandestine means to influence decision-making processes</u>*' (free translation). The service was therefore not authorised to gather intelligence in this regard.

III.3.2.3.3. Boundaries of the method to request banking details

The relevant intelligence service wanted to determine who was the holder of a certain bank account (dossier 2016/4688). When the service learnt that this person had made a deposit into the account of a firm, it wanted to check all deposits into the firm's bank account for a certain period. It based this on Article 18/15 §1 of the Intelligence Services Act: '*For the successful execution of their assignments, the intelligence and security services may be authorised to requisition the following information: 1. the list of bank accounts (…) of which the person targeted is the holder, nominee or beneficial owner, and, as the case may be, all information concerning those; 2. the banking transactions which were carried out in a given period on one or more of those bank accounts or financial instruments, including the details of each originating or destination account*' (free translation). The Committee noted that this provision does not permit the banking details of a third person to be requested; this is permitted only with regard to '*the person targeted*'. The Committee therefore decided that '*the law*

*therefore does not permit the bank account of a third party (*in casu*, the firm) to be investigated in order to ultimately identify the person targeted*' (free translation).

III.3.2.3.4. Lack of clarity regarding the duration of a method

In the decision to use a specific method, it was firstly stated that it could be used '*for the period from [specified date] up to and including [specified date]*' and secondly that it '*can be carried out for three months from the decision of the head of the service and after notice of this decision to the Commission*' (free translation). There was no clarity in the decision about the start and end dates. The Committee held that the start date coincided with the date on which the notice was given to the Commission. The Committee further stated that in case of '*any discrepancy of dates, the shortest period must be chosen*' (free translation) (dossier 2016/4515).

III.3.2.3.5. The calculation of the new period under Article 18/8 of the Intelligence Services Act

In relation to possible espionage, the intelligence service decided at a certain time to proceed through an operator with the inspection of call-associated data for a period of nine months that predated the request in its entirety (dossier 2016/5266). By this time, the relevant Article 18/8 of the Intelligence Services Act had been amended in the sense that '*in his decision, the head of the service can request the data for a period of nine months prior to the decision*' (free translation) [our underlining]. The Committee stated that '*in order to give effect to the wording of the Act, the term 'préalable' (prior to) must be understood to mean that the date on which the decision is made serves as the starting point that is not included in the aforementioned statutory period*' (free translation). *In casu,* this meant that the method related to a period that was one day too long.

III.3.2.3.6. An incomplete request

The Committee had to intervene in two files because the request to the operators was incomplete.

For example, an intelligence service wished to obtain call-associated data for a 90-day period (dossier 2016/4542). However, the request that was sent to the provider made no reference to that limit. The intelligence service believed that the provider only kept that data for 90 days. In fact, this was not the case and the service received the data for an entire year. Even though the service stated that it would not use this data, the SIM Commission suspended the method and the Committee concluded that the method was partially unlawful.

In another case, an intelligence service was in possession of foreign telephone numbers that belonged to people who were linked to a terrorist group (dossier 2016/4838). It wished to determine, through the inspection and

localisation of call-associated data, whether these people had contacted others in Belgium during a certain month. However, the request to the operator did not state that the method was limited to 'Belgian contacts'. The Commission thus suspended the method. The Committee investigated the case and determined that the operator had forwarded all information in its possession. None of this data related to a Belgian number or to a contact that could be situated in Belgium. The Committee decided as follows: '*Whereas the methods are lawful to the extent that they target contacts in Belgium of foreign numbers used abroad; Whereas, however, the implementation of the methods is not lawful to the extent that the request to the operator is not in accordance with the decision because it is not limited to Belgian contacts*' (free translation).

III.3.2.3.7. The SIM Act and the Vienna Convention on Diplomatic Relations of 18 April 1961

A service wanted to use a number of methods that related to interests falling under the scope of application of the Vienna Convention of 1961 (dossier 2016/4458). The SIM Commission suspended the methods. The Committee confirmed this decision.

The Standing Committee I intervened at its own initiative in two other cases (2016/5147 and 2016/5259) to verify whether the method used was compatible with the principle of legality and, more specifically, with the Vienna Convention. After investigation, it transpired that all or part of the methods related to data that fell within the 'inviolable perimeter' as set out by the Committee in its case law (dossier 2014/3148). The Committee also reiterated that it had pointed out the lack of directives in relation to the Ministerial Committee for Intelligence and Security (now the National Security Council) at the time. In dossier 2016/5259, the Committee also found that such directives were still not available. It added the following preamble: '*Whereas the Standing Committee I reiterates, this time insistently, that no methods with regard to [certain aspects] that fall under the Vienna Convention of 1961 can be permitted under such circumstances*'[152] (free translation).

III.3.2.4. Consequences of an unlawful method or an unlawfully implemented method

Due to the urgency of the situation, a head of service orally authorised a specific method in seven similar files (dossiers 2016/4490 to 2016/4496). The written confirmation only followed over six weeks later. Because Article 18/7 §2 requires that '*the oral decision shall be confirmed at the earliest opportunity by a reasoned*

[152] In order to discuss the problem thoroughly, the Committee ordered a work meeting with the Offices of the Prime Minister, Justice and Defence, at which the different positions and concerns were set out.

written decision from the head of the service' (free translation), the SIM Commission suspended the method. The Committee did not agree with this decision of the SIM Commission because: '*Whereas it must be concluded that the Act has not explicitly provided for sanctions if this obligation is not observed; Whereas the Standing Committee I has previously formulated recommendations for improving the urgent procedure; Whereas there is no doubt that the Act was not observed in this case with regard to the written confirmation of the request that must be made at the earliest opportunity by law, but that the Committee must also decide on the consequences of failing to observe this formal obligation; Whereas the delay by the intelligence service in confirming the oral request in writing is due to the factual circumstances in which the method was implemented; Whereas the established formal irregularity has not affected the reliability of the information and also not infringed the fundamental rights of the persons who were the subject of the method; Whereas the Committee refers in its decision to the Antigoon case that the legislator has included in Article 32 of the Preface to the Code of Criminal Procedure and to the administrative case law in certain cases where formal requirements and procedures have not been observed*' (free translation).

III.3.2.5. The jurisdictional decision relating to the complaint

The complainant was prosecuted for terrorism offences. He found information in his criminal file confirming that he had been monitored by State Security. The file also included photographs of the complainant. He wished to know whether State Security had acted lawfully in using what were – in his opinion – specific intelligence methods.

Various fundamental issues were raised in this case. Due to their value as a precedent, these issues are set out in detail below.

III.3.2.5.1. Request to refer questions for a preliminary ruling

The complainant firstly wanted the Standing Committee I, as a jurisdictional body, to refer a number of questions to the Constitutional Court for a preliminary ruling on the basis of Article 26 §2, second paragraph of the Special Act on the Constitutional Court[153] or – if the Committee did not comply with

153 '*Do the provisions of Chapter IV/2 of the Act of 30 November 1998 governing the intelligence and security services infringe Articles 10 and 11 of the Constitution in the sense that the* a posteriori *review of the intelligence services, such as observation with a technical resource in this case, occurs only at the request of the legal subject and not automatically, and that a separate complaint has to be submitted for this purpose, even though a review by the Indictment Division of the special detection methods, such as observation with a technical resource, always happens, in accordance with Article 235ter of the Belgian Code of Criminal Procedure, when the examining magistrate sends their file to the Public Prosecutor pursuant to Article 127 §1, paragraph 1 of the Belgian Code of Criminal Procedure?*' and '*Does Article 43/8 of the Act of 30 November 1998 governing the intelligence and security services infringe*

this request – to the European Court of Justice in Luxembourg.[154] The Committee, which acts in this matter as a jurisdictional body and is therefore authorised, in principle, to refer questions to the Constitutional Court for a preliminary ruling, held that it did not have to comply with this request.

In relation to the first question, the Committee referred to the following elements:

- Contrary to what the complainant asserted, *every* special intelligence method is reviewed automatically, and without exception, first by the SIM Commission and then by the Standing Committee I.
- In 2010, the Constitutional Court already rejected an application to fully or partially nullify the provisions that the complainant also cited. In its judgment no. 145/2011 of 22 September 2011, the Constitutional Court held that there were no inconsistencies between the Intelligence Act of 30 November 1998 and the Constitution.
- The special detection methods of the police follow a different method and course than the special intelligence methods. The legislature has provided an appropriate procedure for each of these methods in order to protect every legal subject. The double monitoring of the SIMs (namely an *a priori* review by the Commission, followed by an *a posteriori* review by the Committee) offers more than adequate guarantees against any unlawful use of special intelligence methods.

In relation to the second question to be referred for a preliminary ruling, the Court pointed to the following aspects, among others:

- Article 43/8 of the Intelligence Services Act stipulates that the SIM decisions of the Committee cannot be appealed. As stated above, an application for the full or partial nullification of the SIM Act was already heard at the Constitutional Court in 2010. In its judgment, the Constitutional Court had

---

Articles 10 and 11 of the Constitution in the sense that it is not possible for the complainant who submits a complaint in accordance with Article 43/4 of the Act of 30 November 1998 governing the intelligence and security services to file an appeal against the decision of the Standing Intelligence Agencies Review Committee regarding the review of the intelligence methods, even though it is possible for an accused or suspect to further appeal against a decision of the Indictment Division regarding the review of the special intelligence methods?' (free translation).

154 '*Does Article 26 of the Special Act on the Constitutional Court infringe the Treaties and, more specifically, Articles 47 and 48 of the Charter of Fundamental Rights of the European Union, in conjunction with Article 20 of the Charter of Fundamental Rights of the European Union, in the sense that it is not possible for a legal subject to refer a question to the Constitutional Court for a preliminary ruling concerning the infringement of his fundamental rights because the Standing Intelligence Agencies Review Committee is not a jurisdictional body in the meaning of Article 26 of the Special Act on the Constitutional Court, even though the Standing Intelligence Agencies Review Committee rules in the only and last instance on the regularity of the intelligence methods used?*' (free translation).

already ruled that it saw no inconsistencies between the Act of 30 November 1998 and the Constitution.
– The Committee further reiterated that it is a *sui generis* jurisdictional body that does not form part of the judiciary and that was created in order to make it impossible to infringe the fundamental rights of legal subjects by imposing a lawfulness check in order to prevent unlawful actions by intelligence services. The Committee is an independent body and gives far-reaching guarantees of impartiality, which were moreover clearly recognised by the Constitutional Court.

The following arguments were developed with regard to the issue of whether the Committee was obliged to refer the questions formulated by the complainant to the European Court of Justice for a preliminary ruling:

– Where the complainant cited in his proposed initial question that the Standing Committee I is not a jurisdictional body, this should be contradicted. The application to refer a question to the European Court of Justice for a preliminary ruling is thus based on an incorrect premise.
– In any case, it also fell outside the competence of the Committee to rule on the application of the Special Act of 6 January 1989 to the Constitutional Court in general, and specifically to test this against the EU treaty provisions.
– Since there was no connection between referring a question for a preliminary ruling in this case and the jurisdiction of the Standing Committee I and this also could not contribute towards resolving the dispute, it was devoid of all purpose.
– The aforementioned Articles 46 and 47 of the Charter moreover belong to the penal sphere and are applicable in criminal courts. This subject matter too falls outside the competence of the Standing Committee I and is not in any way connected with the jurisdiction of the Committee.

III.3.2.5.2. Suspensive effect procedure

The complainant asked the Committee to assign a suspensive effect to its control with regard to the use of the intelligence contested in the criminal proceedings. The Committee rejected this request as 'devoid of purpose'. The Intelligence Act of 30 November 1998 refers only to the 'suspension' of a method. This means suspending the implementation of the method. Since the method in question had already been implemented and completed in 2013, it could no longer be suspended.

III.3.2.5.3. Access to file documents

The complainant asked to be given access into all information regarding the observations, the authorisations of the head of service, and the decision of the

SIM Commission in this case. This was to allow him to verify the lawfulness of the intelligence method.

The Committee pointed out that under the Classification Act of 11 December 1998, such documents are never communicated to people who do not hold the required security clearance, since each of those documents are classified. It is moreover not up to the complainant to request that certain documents be produced since the Act makes provision for a very specific procedure to access all relevant information. This procedure, which is set out in Article 43/5 §3 of the Intelligence Services Act, stipulates that the file '*contains all information and intelligence relevant to this case, except for that which would breach the protection of sources, the protection of the privacy of third parties or 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*' (free translation).

However, the complainant was of the view that he did not adequately possess the necessary information to assess proportionality and subsidiarity. He alleged he needed access to the information that State Security possessed prior to the observations in order to check whether an ordinary intelligence method could have been used. The Committee pointed out that it is up to the SIM Commission and the Standing Committee I to assess proportionality and subsidiarity as these are the two bodies that have been authorised to check compliance with these principles.

III.3.2.5.4. Assessment on the merits

The Standing Committee I found that the methods in question complied with the principles of proportionality and subsidiarity. *In casu,* the purpose was to objectively determine with certainty that the complainant had been in contact with persons known for their extremist Islamic views and/or that there was a link to the Syria problem. Ordinary methods were '*inadequate and installing a camera that recorded images was the appropriate option to gather the intelligence and record the contacts between the complainant and others, all without compromising the second principle that must be taken into consideration, namely proportionality*' (free translation). *In casu,* the potential threats (namely terrorism and extremism) were serious enough to justify a special intelligence method. All formal and procedural conditions were moreover fulfilled.

III.3.2.5.5. The *ultra petita* principle

The complainant initially referred in his complaint to two observations, but subsequently expanded on this with the motivation that he had found out that he had been observed several times.

The Standing Committee I referred to the *ultra petita* principle which entails that a jurisdictional body cannot award more than has been claimed. The Committee therefore saw no need '*other than the review of the intelligence methods of 3 June 2013 and 13 December 2013, to submit any other special intelligence methods to a review. For the assessment of this complaint, the lawfulness of all intelligence methods that applied to the complainant was therefore verified*' (free translation).

III.3.2.5.6. Destruction of data and prohibition on use

Lastly, the complainant requested that there be no further use of the unlawfully gathered data and that it be destroyed immediately.

Discontinuing the use of the information and its destruction are options afforded by the legislature to the Standing Committee I for each special intelligence method presented to it for its *a posteriori* review.

The Standing Committee I decided in each case, for each special method, that there was no need to discontinue the use of data or to destroy it. The Standing Committee I had already made a final decision in this regard during its systematic review.

III.4. CONCLUSIONS AND RECOMMENDATIONS

The Standing Committee I has formulated the following general conclusions and recommendations with regard to the review of the special intelligence methods:

- The number of special methods used by State Security has grown exponentially. This was because of the increased intelligence activities after the attacks in Paris and Zaventem/Maalbeek. The increase was almost completely due to the 'inspection of call-associated data' that increased from just 33 cases in to 622. But exceptional methods have also increased significantly. There were not only more exceptional measures, their average duration was also significantly longer;
- Despite the attacks, the number of specific and exceptional methods used by GISS has remained fairly stable;
- The number of requests to operators for the identification of the user of a means of telecommunication (new Article 16/2 of the Intelligence Services Act) was very high. But this was also the direct consequence of the terrorist attacks;
- Where GISS traditionally focused on 'espionage' for the use of SIM methods, this focus remained on 'terrorism' for State Security;

- While the Committee still made referrals at its own initiative in 1.1% of case files in 2015, this remained limited to 0.15% of cases in 2016. One reason for this is that it was clear from the *prima facie* check of each SIM file within the Committee that the two intelligence services took due account of the statutory restrictions, the decisions of the SIM Commission and the case law of the Committee;
- The Committee pointed out that State Security and GISS, in their SIM decisions, can explicitly refer, where relevant, to the new power to monitor the activities of foreign intelligence services on Belgian territory (see III.1.1);
- The details for the system of requesting information from operators (see III.1.3) did not take the new power of State Security and GISS to monitor the activities of foreign services in our territory into account. The Standing Committee I recommended that the legislature set a maximum period for the inspection of metadata here too.

CHAPTER XI
RECOMMENDATIONS

Based on the review investigations concluded in 2016, the Standing Committee I has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred on individuals by the Constitution and the law (XI.1), the coordination and efficiency of the intelligence services, CUTA and the supporting services (XI.2) and, finally, the optimisation of the review capabilities of the Standing Committee I (XI.3).

XI.1. RECOMMENDATIONS WITH REGARD TO THE PROTECTION OF THE RIGHTS CONFERRED ON INDIVIDUALS BY THE CONSTITUTION AND THE LAW

XI.1.1. CLOSING THE LEGAL LOOPHOLE IN RELATION TO DATA RETENTION[155]

The details for the system of requesting information from operators (see III.1.3) did not take the new power of State Security and GISS to monitor the activities of foreign services in our territory into account. The Standing Committee I recommends the legislature to set a maximum period for the inspection of metadata.

XI.1.2. USE OF UNLAWFULLY OBTAINED INTELLIGENCE[156]

State Security and GISS can obviously receive information or intelligence from foreign partners. They can process that information themselves and/or forward it to the competent Belgian services (e.g. CUTA). The Committee has previously

[155] This recommendation stems from the report on the application of the specific and exceptional methods by the intelligence and security services, and the review thereof by the Standing Committee I (2016).

[156] See 'Chapter II.1. The issue of foreign terrorist fighters'.

already stated in this regard[157] that the '*receiving service should make the minimum effort to determine how the intelligence in question has been obtained*.' (free translation), in order to allow for the refusal of any data from third states that has been collected unlawfully.[158]

XI.1.3. EXCHANGE OF INFORMATION AND COOPERATION WITH FOREIGN SERVICES[159]

As far as the cooperation with foreign services is concerned, the Committee had already insisted several times on a directive that ought to be issued by the National Security Council.[160] On 26 September 2016, the Ministers of Justice and National Defence presented the 'Directive on the relationships between Belgian intelligence services and foreign intelligence services' classified as 'Confidential Act 11.12.1998' in a memorandum to the National Security Council. However, the forwarding of information/personal data to foreign services was only dealt with very briefly in this directive. The Committee therefore persists with its earlier recommendations in this regard and considers an initiative to be a priority. Particular consideration must be given to the principle that the intelligence services must deal carefully with the exchange of information.

XI.1.4. TECHNICAL ASSISTANCE TO THE JUDICIARY[161]

In relation to 'technical assistance' to the judiciary (Art. 20 §2 of the Intelligence Services Act), the Committee has already expressly stated on several occasions that this provision does not allow State Security and GISS to use intelligence powers for judicial purposes.[162] The intelligence services must permanently pay attention to this aspect.

---

157 STANDING COMMITTEE I, *Activity Report 2014*, 11–38.

158 Cf. Directive of 26 September 2016 on international cooperation with foreign intelligence services, paying attention to aspects including 'respect for human rights'.

159 See 'Chapter II.1. The issue of foreign terrorist fighters' and 'Chapter II.5. Protection of scientific and economic potential and the Snowden revelations'.

160 STANDING COMMITTEE I, *Activity Report 2014*, 88–89.

161 See 'Chapter II.1. The issue of foreign terrorist fighters'.

162 STANDING COMMITTEE I, *Activiteitenverslag 2014* (Activity Report 2004), 138 and *Activity Report 2006*, 50–52. The SIM legislature therefore agreed with the Committee's vision in this regard: although an initial proposal included the possibility for State Security and GISS to use ordinary and specific methods in a criminal investigation, this was not incorporated into the final arrangement.

XI.1.5. COMPLIANCE WITH ARTICLE 36*BIS* OF THE PRIVACY ACT[163]

The Committee recommends State Security to take the necessary steps to comply with the obligation included in Article 36*bis* of the Act of 8 December 1992 on privacy protection in relation to the processing of personal data for the purpose of exchanging information with the prison administration. This provision makes its compulsory for a service to obtain prior authorisation from the Sectoral Committee for the federal government for '*any electronic communication of personal data by a federal government agency*' (free translation).

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

XI.2.1. RECOMMENDATIONS SPECIFICALLY AIMED AT FIGHTING TERRORISM AND RADICALISM

XI.2.1.1. Cooperation within the local task forces (LTFs)[164]

The Standing Committee I recommends the different participants in LTFs to inform each other properly of their needs and requirements, of each other's capabilities, and each other's limitations. In this way, a mutual understanding of what LTFs can and cannot deliver can be developed. In relation specifically to State Security, it appears as though it was not always clear to the participants what they could say in meetings (classified information). The Committee recommends that the services create internal certainty in this regard and that representatives from the provincial services who participate in the meetings are also actively supported and guided by central management.

The Standing Committee I also recommends that the intelligence services investigate the correct/appropriate classification level for any information or intelligence that can be tabled at an LTF.[165]

---

163 Protocol agreement governing cooperation between State Security and the Directorate-General for the Execution of Penalties and Disciplinary Measures (DGEPM).

164 See 'Chapter II.1. The issue of foreign terrorist fighters'.

165 A solution, or at least the start of a solution, was found in the new FTF circular. This states that the position of 'information officer (InfOffr)' will be introduced at Local Police level. As the replacement for the chief of police, the information officer represents the police zone in the LTF. He or she transversally manages, within his organisation, the tracking and monitoring efforts in relation to foreign fighters and ensures the quality of the information flow in the zone. The information officer is the point of contact for the intelligence services,

XI.2.1.2. Cooperation and synergy between both intelligence services[166]

The cooperation between the two Belgian intelligence services in relation to the Syria problem was limited and on an *ad hoc* basis. The Standing Committee I recommends that both services investigate which synergies are possible and/or whether there is room for stronger cooperation, including in relation to OSINT, SOCMINT, (CYBER)HUMINT and SIGINT. Another possibility to consider would be for State Security to represent GISS within certain working groups (e.g. within LTFs or in contacts with the prison system).

XI.2.1.3. HUMINT in radicalised and terrorist environments[167]

Information that is provided via HUMINT is often decisive in the sense that it makes a useful contribution in a disruptive strategy or towards preventing an attack. However, it is not easy to recruit sources in radicalised or terrorist environments. This needs to become a priority.

XI.2.1.4. Personnel with language and field knowledge[168]

It is advisable both for running an informant in radical environments (HUMINT) and for monitoring open sources (OSINT and SOCMINT) that the services have access to collection agents and analysts who master several languages and have a good understanding of these people's daily existence (diversity).

XI.2.1.5. Strategic analyses in the fight against terrorism[169]

An urgent reaction is often needed in the fight against terrorism. Partly because of this, analysts are not often able to draw up strategic analyses and information gathering focuses on immediate needs, rather than long-term analysis. State Security should reflect on its individual nature as an intelligence service and its role in the fight against terrorism.

CUTA and the Federal Police for exchanging classified information. He or she holds a security clearance, just like the chief of police.

166 See 'Chapter II.1. The issue of foreign terrorist fighters' and 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

167 See 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

168 See 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'. The Committee made a previous recommendation in the same sense: STANDING COMMITTEE I, *Activity Report 2007*, 112 ('VIII.2.4 Recruitment of personnel with knowledge of specific languages').

169 See 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

XI.2.2. RECOMMENDATIONS WITH GENERAL SCOPE

XI.2.2.1. Better exchange of information via interconnected databases[170]

The exchange of information is very important. There is undoubtedly far more information available at basic collection level within the various Belgian intelligence and police services than State Security and GISS can access. An effort must be made to achieve a greater and better horizontal exchange and flow of information. This will require an extensive effort in terms of expanding, interconnecting and unifying (common) databases, and take up more time and resources than are currently available within the services. This problem must be resolved and the correct (individual) position of the intelligence services needs to be guaranteed.

XI.2.2.2. Predictive intelligence[171]

The Standing Committee I believes that producing what is known as predictive intelligence is an essential task of an intelligence service. The Committee recommends that State Security and GISS investigate, together with their 'clients', the extent to which predictive intelligence is necessary or useful, what the concept entails precisely, what can be expected of it, and how the services could achieve their ambition in this regard.

XI.2.2.3. Use of standardised analysis techniques[172]

Analysis forms an essential component of intelligence work. Many standardised techniques are available regarding analysis. Such techniques are used not to comply with some axiom, but to prevent analytical shortcomings (cognitive or factual errors). The aim is to avoid risks that could arise within the intelligence processes and affect the information position. The Committee has found that the services do not use formal analysis methods coherently.[173] It therefore recommends the services to develop a plan that clearly and transparently sets out their attitude regarding this problem, which policy they are pursuing in this regard, and how they keep (analytical) risks under control.

---

170 See 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

171 See 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

172 See 'Chapter II.1. The issue of foreign terrorist fighters' and 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

173 State Security is aware of the importance of such analysis techniques: its aim is to structurally incorporate these techniques in the analysis activities.

One important method is creating possible scenarios (such as worst-case scenarios) and making hypotheses that can subsequently be confirmed or negated. This important methodological instrument could be applied more often. The Committee believes such scenarios should preferably be created in a multidisciplinary manner: since a terrorism scenario has several components (both civil and military), State Security and GISS must cooperate in this regard.

XI.2.2.4. A planned approach to phenomena[174]

Intelligence processes benefit from a planned approach or design, in which the investigative questions with regard to the phenomena to be monitored are determined in advance, together with how the information will be gathered (collection methods) and analysed (analysis methods). Such a design is derived from the higher strategic level, but differs from, for example, a traditional collection plan because it covers both the collection and analysis methods. In this way, collection and analysis can be streamlined better and the intelligence processes can run more efficiently. There is an urgent need for this in both services. The Standing Committee I recommends the services to incorporate such an approach into their work and to intentionally create a coordinating or umbrella collection and analysis design when taking on a new or unfolding phenomenon – for example, the Syria crisis. However, in principle, this design should exist not only within each service, but also take into account – and ideally use – the collection and analysis capacities of other services.

XI.2.2.5. Questioning clients[175]

The Standing Committee I repeats its recommendation[176] that both services should explicitly ask their 'clients' precisely what intelligence they wish to acquire and how they evaluate the intelligence (feedback). This establishes shared responsibility. On the one hand, the services must make clear under which conditions, how and to whom they wish to or may distribute intelligence and what 'ambition' may be expected of the service in that regard (descriptive, explanatory or predictive intelligence). On the other hand, clients must obviously cooperate in this process themselves, i.e. indicate what they expect and state their (intelligence) requirements.

---

174 See 'Chapter II.1. The issue of foreign terrorist fighters' and 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.

175 See 'Chapter II.1. The issue of foreign terrorist fighters'.

176 For example, see: STANDING COMMITTEE I, *Activity Report 2011*, 172–173 ('IX.2.1.1. Recommendations regarding organisational conditions required for a proper deployment of resources').

XI.2.2.6. Form and content of analysis products[177]

The Committee previously recommended giving an indication of the source(s) of information in analysis products intended for other authorities. After all, this can help the recipient assess the reliability of the product. The Committee reiterates this recommendation.

Instructions must also be issued regarding when and the form in which analysis products must be sent to other authorities, and the exact recipients must be indicated.

XI.2.2.7. Data management at GISS[178]

The Standing Committee I recommends – and not for the first time[179] – that the databases of GISS must be urgently expanded (data input, unambiguous and clear classification of data, access rights from the different divisions), that paper collections should be quickly computerised, that effective search systems should be developed, and that a number of related problems (e.g. RFIMS, classification of incoming information during CCIRM) should be dealt with as a priority.

XI.2.2.8. Qualified translators for SIGINT[180]

The Committee once again stresses the need for qualified translators at the SIGINT department of GISS.

XI.2.2.9. Standardisation of procedures[181]

For the purpose of international exchanges and, more specifically, the management of requests for information from foreign correspondents, the Standing Committee I recommends the development of structured and internationally standardised procedures. Requests for information should include compulsory elements, such as the level of urgency and response period, and must also be supplemented with all elements that are necessary or useful for carrying out the request. The same applies to instruments that are necessary for the fight against terrorism, i.e. the national and international lists. Lists of terrorists or radicalised persons should be standardised. The work that State Security has initiated with its partners in this regard must continue.

---

177 See 'Chapter II.3. Information position of the two intelligence services before the Paris attacks'.
178 See 'Chapter II.1. The issue of foreign terrorist fighters'.
179 In this regard, see: STANDING COMMITTEE I, *Activiteitenverslag 2015* (Activity Report 2015), 6 ('I.2.3 Information management at GISS').
180 In 'Chapter IV. Monitoring the interception of communications broadcast abroad'.
181 See 'Chapter II.2. Information position of State Security and the failed attack on the high-speed Thalys train'.

XI.2.2.10. Investigation into information flows and ICT resources[182]

The Standing Committee I recommends that State Security investigates its working processes, the information flows and the ICT resources that support the whole organisation.

XI.2.3. RECOMMENDATIONS ON SPECIAL INTELLIGENCE METHODS

XI.2.3.1. Correct reference in SIM decisions[183]

The Committee recommends that State Security and GISS, in their SIM decisions, explicitly refer, where relevant, to the new power to monitor the activities of foreign intelligence services on Belgian territory (see III.1.1).

XI.2.3.2. Use of SIM methods abroad[184]

In order to intercept communications originating abroad, for example for the security and protection of our troops and those of our allied partners during missions abroad, GISS has a specific statutory mandate (Art. 259*bis* §5 of the Criminal Code, as read together with Art. 11 §2, 3° of the Intelligence Services Act). Contrary to SIGINT, which can be used abroad, SIM methods are restricted to Belgium itself. The Committee repeated[185] its recommendation for the legislature to hold a debate about the need to make certain SIM methods possible abroad. The legislative amendment of 30 March 2017 responded to this recommendation.

XI.2.3.3. Restrictions in the use of intelligence methods[186]

The Committee recommends that the authorities investigate the efficiency of the resources that the intelligence and security services have at their disposal in the field and their current restrictions (e.g. anonymous prepaid phone cards).[187]

---

182 See 'Chapter II.2. Information position of State Security and the failed attack on the high-speed Thalys train'.

183 This recommendation stems from the report on the application of the specific and exceptional methods by the intelligence and security services, and the review thereof by the Standing Committee I (2016).

184 See 'Chapter II.1. The issue of foreign terrorist fighters'.

185 STANDING COMMITTEE I, *Activity Report 2013*, 170 and *Activity Report 2014*, 93–94.

186 See 'Chapter II.2. Information position of State Security and the failed attack on the high-speed Thalys train'.

187 This recommendation has been met with regard to prepaid cards (see III.1.4. The identification of a prepaid-card holder).

XI.2.4. RECOMMENDATIONS ON THE PROTECTION OF THE SCIENTIFIC AND ECONOMIC POTENTIAL[188]

XI.2.4.1. Joint threat analysis in respect of the SEP

The two intelligence services, CUTA and the Belgian Centre for Cybersecurity Belgium should carry out a joint analysis of the phenomenon of the threat posed by foreign interception systems for the Belgian SEP, and also identify the critical infrastructures.

XI.2.4.2. An information platform for the strategic protection of the SEP

The Standing Committee I recommends the creation, headed by the National Security Council, for example, of an information platform for the strategic protection of the scientific and economic potential. This should definitely include contributions from the competent regional and federal authorities for the economy, representatives from the private sector and research world, the two intelligence services, the Centre for Cyber Security, the Federal Computer Crime Unit (FCCU), CUTA, the Crisis Centre and the National Security Council. The Committee has already been able to establish that organisations with specific expertise, such as the Financial Intelligence Processing Unit and the National Bank, have a lot of information that is not always fully used.

This platform can serve as an information-exchange channel and pave the way for an integrated policy in which the role of the two intelligence services and CUTA are specified. This should ultimately lead to a clear tasking of all participants and their cooperation.

On the other hand, efforts for improved cyber security must be simultaneously continued. The Centre for Cyber Security can – and, according to the presentation of this centre, will – also play a major role in this regard. This also requires an evaluation of the suitability of the Act of 1 July 2011 on the security and protection of critical infrastructures.

XI.2.4.3. Approval of ICT systems and encryption

The task to approve the ICT systems, including own encryption, must immediately be entrusted to a public service, such as the National Security Authority or the Centre for Cyber Security.

---

188 This recommendation stems from 'Chapter II.5. Protection of scientific and economic potential and the Snowden revelations'.

XI.2.4.4. Approval of SEP list of GISS

The National Security Council's approval of a list of players – both natural persons and legal entities – that operate in the economic and industrial sectors and are related to Defence, as specified in Article 11 of the Act on the intelligence and security services, is required.

XI.2.5. RECOMMENDATIONS ON COOPERATION WITH THE PENAL INSTITUTIONS[189]

XI.2.5.1. Towards a new protocol

The Standing Committee I is of the opinion that the cooperation protocol between State Security and DGPI is outdated in its current form. The protocol needs to be amended or rewritten so it can anticipate future challenges, such as new phenomena and evolutions in both uses and methods. Practices that have arisen throughout the years alongside the current protocol must also be integrated or regularised. The initiatives that State Security has taken outside the protocol could also be continued within it.

XI.2.5.2. Recommendations for a better exchange and processing of information

The Standing Committee I believes that it is preferable when exchanging information to work with a designated point of contact (POC) rather than via the provincial posts of State Security, since all exchanged information must be concentrated at the headquarters in Brussels.

The Standing Committee I also points out that the various lists (DGPI list, JIB list, etc.) must be used carefully and that the purpose of the various lists must be determined and observed. A solution must also be found for exchanging 'defederalised' information and certain ambiguities (such as unnecessarily splitting up various procedures for exchanging information) must be eliminated.

[189] Recommendations from 'Chapter II.6. State Security and the cooperation protocol with Penal Institutions'.

XI.2.6. RECOMMENDATIONS ON THE OPERATION OF CUTA[190]

The Standing Committees I and P recommend to CUTA:

- to reject every request for a threat assessment that does not fall within its legal scope of competence;
- not to allow any secondment of non-statutory government officials from support services, unless there is a legislative amendment;
- to regularise the administrative situation of the seconded people;
- to create a personnel file for each staff member, without distinguishing between statutory staff members, seconded staff members or even members of management;
- to send proposals to the competent Ministers for the amendment of the Royal Decree that determines the status of statutory and seconded staff;
- to ensure that every decision to end a secondment on disciplinary grounds is taken in the broad sense without disregarding the principle of good governance which entails that the person involved, who is the subject of a decision, must be heard.

XI.3. RECOMMENDATION RELATED TO THE EFFECTIVENESS OF THE REVIEW

XI.3.1. INTERCEPTION PLAN[191]

The communication of the interception list is often delayed.[192] As a result, the Committee cannot fully perform its monitoring assignment. It therefore insists on the timely communication of the list. The Committee also once again emphasised that the interception plans should more narrowly describe the targeted persons and organisations.

190 Recommendation from 'Chapter II.13. Specific dysfunctions within CUTA'.

191 In 'Chapter IV. Monitoring the interception of communications broadcast abroad'.

192 STANDING COMMITTEE I, *Activity Report 2010*, 85 ('IX.3.2. Timely communication of relevant security interceptions') and *Activiteitenverslag 2015* (Activity Report 2015), 71. The Committee was only given the 2017 Interception Plan upon the completion of this report.

APPENDIX

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT
(extract)

CHAPTER I – GENERAL PROVISIONS

Article 1
Both a Standing Police Services Review Committee and a Standing Intelligence Agencies Review Committee shall be established. In particular, review shall relate to:
1° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the police services on the one hand and the intelligence and security services on the other;
2° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the Coordination Unit for Threat Assessment;
3° The way in which the other support services satisfy the obligation laid down in Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.
An Investigation Service shall be established for each of these committees.

Art. 2
The review governed by this Act does not relate to judicial authorities nor to the actions taken by them in the exercise of the prosecution function. The review does not relate to the administrative police authorities either.
The review referred to in this Act is governed without prejudice to the review or inspection governed by or by virtue of other legislation. In the event of review or inspection governed by or by virtue of other legislation, the review referred to in this Act relating to the activities, methods, documents and directives of the police

services and of the intelligence and security services, shall only be undertaken to ensure fulfilment of the assignments provided for in this Act.

Art. 3
For the purposes of this Act, the following definitions shall apply:
1° "Police services": in addition to the local police and the federal police, the services that come under the authority of the public authorities and public interest institutions, whose members have been invested with the capacity of judicial police officer or judicial police agent;
2° "Intelligence and security services": State Security and the General Intelligence and Security Service of the Armed Forces;
3° "Coordination Unit for Threat Assessment": the service referred to in the Act of 10 July 2006 on threat assessment;
4° "Other support services": the services other than the police services and the intelligence and security services referred to in this Act, that are required, in accordance with the Act of 10 July 2006 on threat assessment, to pass on information to the Coordination Unit for Threat Assessment;
5° "Threat Assessment Act": the Act of 10 July 2006 on threat assessment;
6° "Ministerial Committee": the Ministerial Committee referred to in Article 3, 1° of the Act of 30 November 1998 governing the intelligence and security services.

Shall be equated to police services for the purposes of this Act, the people who are individually authorised to detect and establish criminal offences.

CHAPTER II – REVIEW OF THE POLICE SERVICES

This chapter that concerns review of the police services by the Standing Committee P is not reproduced.

CHAPTER III – REVIEW OF THE INTELLIGENCE SERVICES

SECTION 1 – THE STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE

Subsection 1 – Composition

Art. 28
The Standing Intelligence Agencies Review Committee, hereinafter referred to as the "Standing Committee I", shall consist of three full members, including a

Chairman. Two substitutes shall be appointed for each of them. They shall all be appointed by the Chamber of Representatives, who may dismiss them if they perform one of the functions or activities or hold one of the positions or mandates referred to in paragraph 4, or for serious reasons.

The Standing Committee I shall be assisted by a registrar. In his absence, the Standing Committee I shall provide for his replacement in accordance with the terms defined in the rules of procedure referred to Article 60.

At the time of their appointment, the members and their substitutes shall satisfy the following conditions:
1° Be Belgian;
2° Enjoy civil and political rights;
3° Have attained the age of 35 years;
4° Reside in Belgium;
5° Hold a Master's degree in Law and demonstrate at least seven years' relevant experience in the field of criminal law or criminology, public law, or management techniques, acquired in positions related to the operation, activities and organisation of the police services or of the intelligence and security services, as well as having held positions requiring a high level of responsibility;
6° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

The members and their substitutes may not hold a public elected office. They may not perform a public or private function or activity that could jeopardise the independence or dignity of the office. They may not be members of the Standing Police Services Review Committee, nor of a police service, an intelligence service, the Coordination Unit for Threat Assessment, or another support service.

The Chairman shall be a magistrate.

The decisions assigned to the Standing Committee I by this Act or other acts shall be taken in plenary session.

Art. 29
The registrar shall be appointed by the Chamber of Representatives, who may dismiss him or terminate his appointment in the cases referred to in Article 28, paragraph 4. At the time of his appointment, the registrar shall satisfy the following conditions:
1° Be Belgian.
2° Enjoy civil and political rights;
3° Have knowledge of the French and Dutch languages;
4° Have attained the age of 30 years;
5° Reside in Belgium;
6° Hold a Master's degree in Law;
7° Have at least two years' relevant experience;
8° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Before taking up his duties, the registrar shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Chamber of Representatives.

Art. 30
The members of the Standing Committee I and their substitutes shall be appointed for a renewable term of six years starting from the time they take their oath. At the end of this term, the members shall remain in office till their successors have taken their oath.

The substitutes shall be appointed for a renewable term of six years starting from the time the member whom they are replacing took his oath.

A member whose mandate ends before the expiry of the term of six years shall be replaced for the remaining period of the mandate by his first substitute or if the latter relinquishes this position, by his second substitute. If a position of substitute member should become vacant, the Chamber of Representatives shall appoint a new substitute member forthwith.

For the appointment of a substitute member, the conditions laid down in Article 28, paragraph 4, shall be verified by the Chamber of Representatives upon taking up his duties.

Before taking up their duties, the members of the Standing Committee I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Chamber of Representatives.

Subsection 2 – Definitions

Art. 31
§1. For the purposes of this chapter, "the competent ministers" shall mean:
1° The minister responsible for National Defence, with regard to the General Intelligence and Security Service;
2° The minister responsible for Justice, with regard to State Security;
3° The minister responsible for a service referred to in Article 3, 2°, in fine;
4° The minister responsible for the Interior, with regard to the assignments of State Security relating to the maintenance of law and order and the protection of people, as well as the organisation and administration of State Security when that organisation and administration have a direct influence on the execution of assignments relating to the maintenance of law and order and the protection of people;
5° The National Security Council, with regard to the Coordination Unit for Threat Assessment or the other support services.

In this chapter, "the competent authority" shall mean the director of the Coordination Unit for Threat Assessment.

Subsection 3 – Assignments

Art. 32
If the investigation concerns an intelligence service, the Standing Committee I shall act either on its own initiative, or at the request of the Chamber of Representatives, the competent minister or the competent authority.

When the Standing Committee I acts on its own initiative, it shall forthwith inform the Chamber of Representatives thereof.

Art. 33
Within the framework of the objectives laid down in Article 1, the Standing Committee I shall investigate the activities and methods of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services, their internal rules and directives, as well as all documents regulating the conduct of the members of these services.

The intelligence services, the Coordination Unit for Threat Assessment, and the other support services shall, on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services. The Standing Committee I and the Investigation Service for the intelligence services shall have the right to be provided with all texts that they consider necessary for the performance of their assignment. The Standing Committee I may, based on a reasoned request of its Chairman, request the administrative authorities to provide it with the regulations, guidelines and documents issued by these authorities which the Committee considers essential for the performance of its assignment. The concerned administrative authority has the right to assess whether it is relevant to communicate the requested regulations, guidelines and documents to the Standing Committee I.

The Standing Committee I shall provide the competent minister or the competent authority, as well as the Chamber of Representatives with a report on each investigation assignment. This report shall be confidential until its communication to the Chamber of Representatives in accordance with Article 35.

This report shall include the conclusions relating to the texts, activities or methods that could jeopardise the objectives laid down in Article 1.

The competent minister or the competent authority may, with regard to the investigation reports, hold an exchange of views with the Standing Committee I. The Standing Committee I may itself propose that such an exchange of views be held.

The competent minister or the competent authority shall inform the Standing Committee I within a reasonable period of time of his/its response to its conclusions.

The Standing Committee I may only advise on a Bill, Royal Decree, Circular Letter, or any documents expressing the political orientations of the competent

ministers, at the request of the Chamber of Representatives, or the competent minister.

When the Standing Committee I acts at the request of the competent minister, the report shall only be submitted to the Chamber of Representatives at the end of the term laid down in accordance with Article 35, §1, 3°. The Chairman of the Monitoring Committee concerned referred to in Article 66bis shall be informed of the request of the minister to the Standing Committee I and of the content of the report before the end of the term laid down in Article 35, §1, 3°.

Art. 34

Within the framework of the objectives laid down in Article 1, the Standing Committee I deals with the complaints and denunciations it receives with regard to the operation, the intervention, the action or the failure to act of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services and their personnel.

Without prejudice to the provisions of Article 46, the Standing Committee I may decide not to follow up a complaint or a denunciation that is clearly unfounded. It may delegate this responsibility to the Head of the Investigation Service for the intelligence services.

The decision of the Standing Committee I not to follow up a complaint or denunciation and to close the investigation shall be justified and communicated to the party who made the complaint or denunciation.

When the investigation is closed, the results shall be communicated in general terms.

The Standing Committee I shall inform the managing officer of the intelligence service, the director of the Coordination Unit for Threat Assessment, or the managing officer of the other support service, depending on the case, of the conclusions of the investigation.

Art. 35

§1. The Standing Committee I shall report to the Chamber of Representatives and the Senate in the following cases:

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the Chamber of Representatives and the Senate, and to the competent ministers by 1 June at the latest. In this report, the Standing Committee I shall pay special attention to the specific and exceptional methods for gathering information, as referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, as also to the application of Chapter IV/2 of the same Act and to the implementation of the Act of 10 July 2006 on threat assessment.

2° When the Chamber of Representatives has entrusted it with an investigation.
3° When at the end of a period that it believes to be reasonable, it notes that no action has been taken concerning its conclusions, or that the measures taken are inappropriate or inadequate. This period may not be less than sixty days.

§2. The Standing Committee I shall present a report annually to the Chamber of Representatives regarding the application of Article 16/2 and Article 18/2 of the Act of

30 November 1998 governing the intelligence and security services. A copy of this annual report shall also be provided to the Ministers of Justice and Defence, and to State Security and the General Intelligence and Security Service, who may draw the attention of the Standing Committee I to their remarks.

The report shall contain the number of clearances granted, the duration for which the exceptional methods for gathering information are applicable, the number of persons involved and, if necessary, the results obtained. The report shall also mention the activities of the Standing Committee I.

The elements appearing in the report should not affect the proper functioning of the intelligence and security services or jeopardise the cooperation between Belgian and foreign intelligence and security services.

Art. 36
In order to prepare its conclusions of a general nature, the Chamber of Representatives may request the Standing Committee I to provide each and every investigation dossier, according to the terms and conditions that they determine and which in particular aim to safeguard the confidential nature of these dossiers and to protect the privacy of individuals. If the investigation was initiated at the request of a competent minister, his consent shall be required before handover of the investigation dossier, unless the term laid down in Article 35, §1, 3° has expired.

Art. 37
After acquiring the advisory opinion of the competent ministers or the competent authority, the Standing Committee I shall decide, within a period of one month from the request for advice, to make public all or part of its reports and conclusions, according to the terms and conditions it stipulates.

The reports and conclusions made public shall include the advisory opinion of the competent ministers and the competent authorities.

Art. 38
The Prosecutor-General and the Auditor-General shall ex-officio send to the Chairman of the Standing Committee I a copy of the judgments and judicial decisions relating to the crimes or offences committed by the members of the intelligence services and the Coordination Unit for Threat Assessment.

The public prosecutor, the labour prosecutor, the federal prosecutor or the prosecutor-general of the Court of Appeal, depending on the case, shall inform the Chairman of the Standing Committee I whenever a criminal or judicial investigation into a crime or offence is initiated against a member of an intelligence service or the Coordination Unit for Threat Assessment.

At the request of the Chairman of the Standing Committee I, the prosecutor-general or the auditor-general may provide a copy of the deeds, documents or information relating to criminal proceedings against members of the intelligence services and the Coordination Unit for Threat Assessment for crimes or offences committed in the execution of their duties.

However, if the deed, document or information concerns an ongoing judicial investigation, it may only be communicated with the consent of the examining magistrate.

The copies shall be delivered without charge.

Art. 39.
The Standing Committee I shall exercise its authority over the Investigation Service for the intelligence services, assign investigations to it, and receive reports on all investigations that are carried out.

However, when they perform a judicial police assignment, the Head and the members of the Investigation Service for the intelligence services shall be subject to review by the prosecutor-general of the Court of Appeal or the federal prosecutor.

SECTION 2 – THE INVESTIGATION SERVICE FOR THE INTELLIGENCE SERVICES

Art. 40
By order of the Standing Committee I or, except with regard to the Coordination Unit for Threat Assessment and the other support services, on its own initiative, in which case it shall immediately inform the Chairman of the Standing Committee I, the Investigation Service for the intelligence services, hereinafter referred to as the "Investigation Service I", shall supervise the operations of the intelligence services, the Coordination Unit for Threat Assessment and the other support services, through investigations, within the limits of Article 1.

It shall examine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another support service. Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

On its own initiative or at the request of the competent public prosecutor, military public prosecutor or examining magistrate, it shall, together with the other officers and agents of the judicial police, and even with a right of priority over them, investigate the crimes and offences which the members of the intelligence services and the Coordination Unit for Threat Assessment are charged with. With regard to the members of the other support services, this provision only applies with respect to the obligation laid down by Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

If the person filing a denunciation so wishes, his anonymity shall be guaranteed. In this event, his identity may only be disclosed within the Service and to the Standing Committee I.

Art. 41

A person may not be appointed Head of the Investigation Service I if he has not been a magistrate or a member of an intelligence or police service for a period of five years, or if he cannot demonstrate at least five years' relevant experience as a public servant in positions relating to the activities of the intelligence or police services. At the time of his appointment he must have attained the age of 35 years.

The Head of the Investigation Service I shall be appointed by the Standing Committee I for a renewable term of five years.

Before taking up his duties, the Head of the Investigation Service I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the Chairman of the Standing Committee I.

He must have knowledge of the French and Dutch languages.

He shall retain his right to advancement and salary increase.

He may be dismissed by the Standing Committee I.

Art. 42

Without prejudice to Article 39, second paragraph, the Head of the Investigation Service I shall manage it and set out the tasks, under the collegial authority, direction and supervision of the Standing Committee I.

He shall be responsible for relations with the Standing Committee I, from which he shall receive the assignments and to which he shall send the reports.

He shall be responsible for relations with the judicial authorities, from which he shall receive the requests and to which he shall send the reports referred to in Article 46.

Art. 43

Except for the cases laid down by Articles 40, paragraph 3, and 46, the Head of the Investigation Service I shall inform the competent minister or the competent authority that an investigation is initiated.

He shall send a report to the Standing Committee I at the end of each investigation assignment.

However, in the cases referred to in Articles 40, paragraph 3, and 46, the report shall be limited to the information necessary for the Standing Committee I to perform its assignments.

Art. 44

The members of the Investigation Service I shall be appointed and dismissed by the Standing Committee I on the recommendation of the Head of the Investigation Service I.

At least half of the members, and this for a renewable term of five years, shall be seconded from an intelligence or police service or an administration in which they have acquired at least five years' experience in positions relating to the activities of the intelligence or police services.

The members of the Investigation Service I shall take the same oath as the Head of the Service.

In the service or administration that they have been seconded from, they shall retain their right to advancement and salary increase.

Art. 45

The Head and the members of the Investigation Service I shall have the capacity of judicial police officer, assistant public prosecutor and assistant military public prosecutor.

In order to be appointed, they must hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Art. 46

When a member of the Investigation Service I has knowledge of a crime or offence, he shall produce a formal report that is forthwith sent by the Head of the Investigation Service I to the public prosecutor, to the military public prosecutor, or the examining magistrate, depending on the case.

The person who lodged the complaint or filed the denunciation, or the authority who called upon the Standing Committee I, shall be informed thereof by the Head of the Investigation Service I.

Art. 47

When a member of the Investigation Service I observes facts during an investigation that could constitute a disciplinary offence, the Head of the Investigation Service I shall forthwith inform the competent disciplinary authority thereof.

SECTION 3 – INVESTIGATION PROCEDURES

Art. 48

§1. Without prejudice to the legal provisions relating to the immunity and privilege, the Standing Committee I and the Investigation Service I may summon for hearing any person they believe useful to hear.

The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services which are being heard may testify about facts covered by professional secrecy.

§2. The Chairman of the Standing Committee I may have members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services summoned through the medium of a bailiff. The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services are bound to testify after having taken the oath prescribed by Article 934, paragraph 2 of the Judicial Code.

The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services are bound to disclose to the Standing Committee I the secrets that they know of. If these secrets relate to an ongoing criminal or judicial inquiry, the Standing Committee I shall consult the competent magistrate in advance regarding this.

If the member or former members of the intelligence service, the Coordination Unit for Threat Assessment, or the other support services is of the opinion that he must not disclose the secret he has knowledge of because its disclosure would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule, or, if it concerns a member or former member of the Coordination Unit for Threat Assessment or another support service, the Chairmen of the two Standing Committees, who shall rule jointly.

§3. The Standing Committee I and the Investigation Service I may request the collaboration of interpreters and experts. They shall take the oath in the way used in the Assize Court. The remuneration due to them shall be paid in keeping with the rates for fees in civil cases.

§4. Article 9 of the Act of 3 May 1880 on parliamentary investigations shall apply to the members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services who are heard or summoned by the Standing Committee I as witnesses, and to the experts and interpreters who are called upon.

The formal reports establishing the offences committed before the Standing Committee I shall be drawn up by the Chairman and sent to the prosecutor-general of the Court of Appeal in the district where they were committed.

The members or former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services who refuse to testify before the Standing Committee I, and the experts and interpreters who refuse to collaborate, shall be liable to imprisonment of between one month and one year.

Art. 49
The members of the Investigation Service I may request the assistance of the public power in the performance of their assignments.

Art. 50
Any member of a police service who observes a crime or offence committed by a member of an intelligence service shall draw up an information report and send it to the Head of the Investigation Service I within a period of fifteen days.

Art. 51
The members of the Investigation Service I may make all observations in any location.

They may at all times, in the presence of their Head of Department, or his substitute, and of the chief of police, director or senior civil servant concerned, or his replacement, enter the premises where members of an intelligence service, the Coordination Unit for Threat Assessment or other support service perform their duties, in order to make substantive observations. In these locations, they may confiscate any objects and documents useful to their investigation, except for those relating to an ongoing criminal or judicial investigation. If the chief of police or his substitute is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 November 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule. If the director or the senior civil servant or his replacement is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 threat ass 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairmen of the two Standing Committees, who shall rule jointly. The confiscated objects and documents shall be recorded in a special register kept for this purpose.

CHAPTER IV – JOINT MEETINGS OF THE STANDING POLICE SERVICES AND INTELLIGENCE AGENCIES REVIEW COMMITTEES

Art. 52
The Standing Committees shall exchange information on their activities and send each other the reports and conclusions referred to in Articles 9, 11, 33 and 35.

At least twice a year, they shall hold joint meetings, during which additional information may be exchanged.

Art. 53
During their joint meetings, the Standing Committees shall jointly perform their assignments (laid down in Articles 9, 10, 11, 33, 34 and 35):
1° With regard to the public services that perform both police and intelligence assignments;
2° With regard to the division of the assignments and the coordination of the operation between the police services on the one hand, and the intelligence services on the other;
3° With regard to any question put to them, either by a joint request from the ministers responsible for the Interior, Justice and National Defence, or at the request of the Chamber of Representatives;
4° With regard to any question that each Standing Committee believes does not fall within its exclusive competence;
5° With regard to any question considered by a Standing Committee to be sufficiently important to warrant a joint meeting;
6° With regard to the Coordination Unit for Threat Assessment or another support service.

A report shall be produced jointly by the Standing Committees at each joint meeting. This report may include advisory opinions and recommendations. It shall be sent as stipulated in Articles 9, 11, 33 and 35.

Art. 54
These joint meetings shall be chaired alternately by the Chairmen of the Standing Committees.

The functions of the secretariat of the joint meetings shall be performed by the longest serving registrar or, in the event of equal length of service, by the youngest registrar.

Art. 55
During the joint meetings, the Standing Committees may decide to assign investigation assignments to the two Investigation Services or to either one of them. They shall receive the reports on all the investigations that are carried out.

CHAPTER V – COMMON PROVISIONS

Art. 56
Each Standing Committee shall examine the complaints that are lodged with it by its former members or by former members of the Investigation Services who believe they have been subject to prejudicial measures because of the functions they have carried out in the Standing Committees or in the Investigation Services.

Art. 57
The funds required for the operation of the Standing Committees and the Investigation Services established by this Act shall be imputed to the appropriations budget.

The Chairmen, the members and the registrars of the Standing Committees, as well as the Director-General of the Investigation Service P and the Head of the Investigation Service I shall enjoy exemption from postal charges for official business.

Art. 58
Each Standing Committee shall appoint and dismiss the members of its administrative staff, on its own initiative or at the proposal of the registrar.

Under the collegial authority and supervision of the Standing Committee in question, the registrar shall be responsible for leading and managing the members of the administrative staff and shall distribute the tasks among them.

The Director-General of the Investigation Service P and the Head of the Investigation Service I shall have authority over the members of the administrative staff, where the number of members and their job requirements shall be defined by the Standing Committee in question, which assigns these members to them.

The registrar shall have authority over the members of the Investigation Service P or I, depending on the situation, where the number of members and the job requirements shall be defined by the Standing Committee in question, which assigns these members to him.

The staff members referred to in the third and fourth paragraphs shall retain the rights and obligations specific to the statute applicable to them.

Art. 59
The travel and subsistence expenses of the Chairman, the members and the registrar of each Standing Committee, the Director-General of the Investigation Service P, the Head of the Investigation Service I and the members of these services shall be determined according to the provisions applicable to the public services.

Art. 60
Each Standing Committee shall adopt its rules of procedure. The rules of procedure for the joint meetings shall be adopted jointly by the two Standing Committees.

The rules of procedure of both Standing Committees shall be approved by the Chamber of Representatives.

In accordance with paragraph 2, the Chamber of Representatives may amend the rules of procedure after acquiring the advisory opinion of the Standing Committee concerned. The advisory opinion shall be deemed favourable if it has not been given within sixty days of the request.

Art. 61
§1. The members of the Standing Committees shall enjoy the same status as the councillors of the Court of Audit. The rules governing the financial statute of the councillors of the Court of Audit, contained in the Act of 21 March 1964 on the remuneration of the members of the Court of Audit, as amended by the Acts of 14 March 1975 and 5 August 1992, shall apply to the members of the Standing Committees.

The members of the Standing Committees shall enjoy the pension scheme applicable to the civil servants of the General Administration. The following special conditions shall also apply.

The pension may be granted as soon as the person concerned has attained the age of fifty-five years. It shall be calculated on the basis of the average remuneration of the last five years, in proportion to one twentieth per year of service as a member of the Standing Committee.

A member who is no longer able to perform his duties due to illness or infirmity, but who has not attained the age of fifty-five years, may retire irrespective of his age. The pension shall be calculated according to the method laid down in the preceding paragraph.

The services that do not fall under the regulations referred to in paragraphs two to four and that qualify for the calculation of a state pension, shall be taken into account in application of the laws governing the calculation of the pensions for these services.

§2. Unless he has been dismissed, the member of a Standing Committee shall, when his duties are terminated or if his term of office is not renewed, receive a fixed severance grant equivalent to the gross monthly salary of the last eighteen months.

If this severance grant is granted before expiry of the first period of five years, it shall be reduced accordingly.

The following are excluded from this allowance:
1° The members to which Article 65 applies.
2° The members who were members of a police service or an intelligence and security service before their appointment to the Standing Committee and who rejoin this service.

§3. The registrars of the Standing Committees shall enjoy the same statute and pension scheme as the registrars of the Court of Audit.

Article 365, §2, a), of the Judicial Code shall apply to the registrars of the Standing Committees.

Art. 61*bis*

The Chairman of each Standing Committee shall, in accordance with the principle of collective responsibility, preside the meetings of that Committee and assume the day-to-day management of its activities. He shall ensure the application of the rules of procedure, the proper functioning of the Committee, as well as the proper performance of its assignments. He shall also ensure that the performance of the judicial police assignments does not impede the performance of the investigations. To this end, he shall hold the necessary consultations with the competent judicial authorities.

For the implementation of the authorities entrusted to him, the Chairman of each Standing Committee shall be assisted by the registrar and, respectively, by either the Director-General of the Investigation Service P or the Head of the Investigation Service I.

Art. 62

Without prejudice to Article 58, the registrar shall act under the collegial authority and the supervision of the Standing Committee in question, the registrar of each Committee shall among others manage the following:
the administrative staff;
the infrastructure and equipment of the Committee;
the secretariat of the Committee meetings and the minutes of the meetings;
the sending of documents;
the preservation and protection of the secrecy of the documentation and archives.

He shall prepare the budget of the Committee and keep the accounts.

Art. 63

The members of the Standing Committees are prohibited from attending the deliberations on affairs in which they have a direct or personal interest, or in which relatives by blood or marriage to the fourth degree inclusive, have a direct or personal interest.

Art. 64

The members of the Standing Committees, the registrars, the members of the Investigation Services, and the administrative staff shall be obliged to preserve the secrecy of the information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment of between eight days to one year, and a fine between one hundred

francs and four thousand francs, or only one of these penalties, if they divulge these secrets in circumstances other than those stipulated by law or by the rules of procedure.

Art. 65
§1. Articles 1, 6, 1 and 12 of the Act of 18 September 1986 instituting political leave for the members of staff of the public service shall apply, where appropriate and with the necessary adaptations, to members of the Standing Committees.
§2. Members of the judiciary may be appointed as members of the Standing Police Services Review Committee and as members of the Standing Intelligence Agencies Review Committee, and as Director-General of the Investigation Service P or Head of the Investigation Service I.

Article 323bis, paragraph 3, of the Judicial Code shall apply if a magistrate from the public prosecutor's office is a chief of police.

Art. 66
Excluding its Chairman, each Standing Committee shall have as many French-speaking members as Dutch-speaking members.

The Chairman of one of the Standing Committees shall be French-speaking, the Chairman of the other Dutch-speaking.

Art. 66*bis*
§1. The Chamber of Representatives shall create a permanent committee responsible for monitoring the Standing Committee P and the Standing Committee I.

The Chamber of Representatives shall stipulate in its regulation, the rules relating to the composition and functioning of the monitoring committee.

§2. The monitoring committee shall supervise the operation of the Standing Committees, and ensure observance of the provisions of this Act and the rules of procedure.

The monitoring committee shall also perform the assignments assigned to the Chamber of Representatives by Articles 8, 9, 11, 1°bis, 2° and 3°, 12, 32, 33, 35, §1, 2° and 3°, 36 and 60.

§3. The monitoring committee shall meet at least once per quarter with the President or the members of each Standing Committee. The monitoring committee can also meet at the request of the majority of its members, at the request of the Chairman of one Standing Committee, or at the request of the majority of the members of a Standing Committee.

Every denunciation by a member of a Standing Committee relating to the inadequate functioning of that Standing Committee, the non-observance of this Act, or the rules of procedure, may be brought before the monitoring committee.

The monitoring committee may issue recommendations to each Standing Committee, or to each of its members, relating to the functioning of the Standing Committee, the observance of this Act, or the rules of procedure.

§4. The members of the monitoring committee shall take the necessary measures to safeguard the confidential nature of the facts, acts or intelligence that they have knowledge of by virtue of their position, and shall be subject to an obligation of confidentiality. They shall be obliged to preserve the secrecy of any information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Any violation of this obligation of confidentiality shall be penalised in accordance with the rules of the Chamber of Representatives.

APPENDIX

30 NOVEMBER 1998 ACT GOVERNING THE INTELLIGENCE AND SECURITY SERVICES

(extract)

[Amendments brought until May 2017 – unofficial consolidated version]

TITLE I
GENERAL PROVISIONS

(…)

[TITLE IV/2
A POSTERIORI CONTROL OF THE SPECIFIC AND EXCEPTIONAL METHODS FOR THE GATHERING OF INTELLIGENCE BY THE INTELLIGENCE AND SECURITY SERVICES

Article 43/2

Without prejudice to the competences defined in Article 1 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment and in Article 44 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
All decisions, opinions, authorisations and confirmations 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 on the basis of any 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 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.

Except if it is likely to jeopardise the assignments of the intelligence and security services, 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 and security 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 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.]

(…)