ACTIVITY REPORT 2017

ACTIVITY REPORT 2017

Review Investigations, Control of Special and Certain Ordinary Intelligence Methods and Recommendations

Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee

intersentia

Cambridge – Antwerp – Chicago

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 2017. Review Investigations, Control of Special and Certain Ordinary 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 – Chicago
www.intersentia.com

ISBN 978-1-78068-838-1
D/2019/7849/36
NUR 823

CONTENTS

LIST OF ABBREVIATIONS

BCCP	Belgian Code of Civil Procedure
BELPIU	Belgian Passenger Information Unit
CAC	Conduct after capture
CHOD	Chief of Defence
CI	Counterintelligence
CIP	Central Information Point
C.O.C.	Control Agency for Management of Police Information *(Controleorgaan voor politionele informatie – Organe de contrôle de l'information policière)*
C-Ops	Operation Center
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*)
DGSE	Direction Générale de la Sécurité Extérieure (France)
ECHR	European Court of Human Rights
FTF	Foreign Terrorist Fighter
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*)
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)*
IS	Islamic State
ISTAR	Intelligence, Surveillance, Target Acquisition & Reconnaissance
IT	Information Technology
NATO	North Atlantic Treaty Organisation

NBB	National Bank of Belgium *(Nationale Bank van België – Banque nationale de Belgique)*
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*)
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
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*
TCCC	Tactical Combat Casualty Care
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)*

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 responsible minister or authority. Additionally, the Standing Committee I can act on request of a citizen and of any person holding a civil service position, as well as any member of the armed forces, who has been directly concerned by the intervention of one of the intelligence services.

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

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

1 VAN LAETHEM, W. and VANDERBORGHT, J., *Inzicht in toezicht – Regards sur le contrôle*, Antwerpen, Intersentia, 2012, 265 p.

2 Belgian Standing Committee I (ed.), *All Source Threat Assessments in the Fight Against Terrorism – Fusion Centres throughout Europe*, Antwerpen, Intersentia 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 2017 that are most relevant to the international intelligence community (the review investigations, the control of special and certain ordinary intelligence methods, the recommendations and the table of contents of the complete activity report), have therefore been translated into English. This book is the seventh 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,* the *Activity Report 2014–2015 and* the *Activity Report 2016* (see www.comiteri.be).

Serge Lipszyc, Chairman
Pieter-Alexander De Brock, Counsellor
Laurent Van Doren, Counsellor
Wouter De Ridder, Secretary

1 December 2018

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 2017

TABLE OF CONTENTS

PREFACE

The Standing Committee I's remit has continued to expand over recent years. Existing assignments have been broadened or given substance for the first time. The Committee has also been assigned several new and important tasks. Inevitably, this has all translated into an increased workload, especially since the necessary additional resources have not been provided.

The 'broadening of existing assignments' is the indirect consequence of extending the powers and human resources of the monitored services: State Security and GISS have been given more room to manoeuvre, for example, which means more and other SIM methods must be monitored. The same phenomenon has occurred in the Appeal Body for security clearances, certificates and advice: more sectors are becoming subject to mandatory security screening, resulting in new appeals. And with the new Act of 23 February 2018, the number of screenings, and thus the number of appeals, will only increase.

The fact that intelligence services are being assigned new tasks also has repercussions for the Standing Committee I: for example, GISS has been assigned a central role within the context of cybersecurity. To exercise proper control over how that intelligence activity is performed, the Committee must be able to invest in personnel with specific expertise.

And the Committee has also been confronted with the need to include existing assignments further or even for the first time. For example, over the last three years, the Committee has issued as many opinions at the request of Parliament or a minister as in the previous fifteen years. The Committee was also called in for the first time by two parliamentary inquiry committees. Although it performed important work in those committees, this was obviously at the cost of other assignments.

Lastly, there are numerous statutory provisions under which the Committee has recently been given a new assignment: inspecting the common databases for FTFs (now 'foreign fighters') and 'hate preachers' that are managed by CUTA, monitoring certain assignments of the ISTAR battalion, monitoring how GISS makes image recordings and penetrates IT systems abroad, stricter monitoring of certain ordinary methods, monitoring how the intelligence services operate within the Passenger Intelligence Unit (BELPIU) and controlling how they use certain camera images.

The impact of all those recent assignments had not yet been properly assessed when it became clear in mid-2018 that the Standing Committee I was getting

another assignment: it would become the Data Protection Authority for almost all personal data related to 'national security'. In that role, the Committee will not only have to deal with individual requests, but also draw up opinions and enter into protocols with other data protection authorities.

The many new regulatory initiatives have a profound effect on the precarious balance between citizens' rights and freedoms and their restriction for security reasons. But the Standing Committee I is also faced with the quest for this balance. The Committee was established to perform supervisory tasks independently and impartially, in part to assure citizens that the rights granted to them under the Constitution and other laws are and will remain guaranteed. The quality of the work the Standing Committee I 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.

In recent years, the Committee has used every opportunity to explain to the competent authorities that it does not suffice to create statutory review without also investing in the review body. For example, in October 2016, the Committee raised these concerns with the Justice Parliamentary Committee following the discussion of the amendments to the Intelligence Act under which the intelligence services would receive new powers that had to be monitored by the Standing Committee I. A joint letter was also drafted with all the institutions entitled to appropriations and facing the same problem. And the issue of diminishing resources was also discussed in detail during the audit that the Speaker of the Chamber of Representatives had conducted into those institutions. The audit made critical comments about the large number of support staff. The Standing Committee I does not accept that criticism. Certain assignments – such as the functioning of the Appeal Body for security clearances, certificates and advice, whose registry is operated by the Committee – require extensive administrative support that the Committee provides in full.

As the outgoing Chairman of the Standing Committee I, I can only hope this call for additional resources will not fall on deaf ears, so the announced cuts on the one hand, and increased powers and workload on the other hand, will not hurt the quality of operations of a body that plays a fundamental role in our democracy based on the rule of law.

Guy Rapaille,
Chairman of the Standing
Intelligence Agencies Review Committee
5 September 2018

CHAPTER II
REVIEW INVESTIGATIONS

In 2017, the Standing Committee I finalised five review investigations, one of which was in conjunction with the Standing Committee P (II.1 to II.5). The Committee also opened three new investigations that year, one of which was a joint investigation with the Standing Committee P. Two investigations were started officially, and in one investigation the Minister of Defence made a referral to the Standing Committee I (Article 32 of the Review Act).[4] A brief description of those three new investigations follows in II.6.

The Committee received a total of 35 complaints or reports in 2017. Efforts to streamline, deformalise and standardise the 'complaints and reports' work process started in 2016.[5] After verifying some objective information, the Committee rejected 34 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 (e.g. the Standing Committee P, Federal Police and Public Prosecutor). One complaint from 2017 resulted in the opening of a review investigation.

Besides review investigations, the Standing Committee I opens 'information dossiers', which must enable a response to questions about how the intelligence services and CUTA operate.[6] Where such dossiers reveal signs of dysfunction or aspects of intelligence service operations that require further scrutiny, the Committee may initiate a review investigation. However, if it is clear that such an investigation will not provide added value in terms of the Standing Committee I's

---

4 The fact that the Committee receives a referral from a member of the executive authority is rather exceptional. In this regard, see: VAN LAETHEM, W. and VANDERBORGHT, J., 'Torture numbers, and they'll confess to anything. Een analyse van twintig jaar toezichtonderzoeken, studies en adviezen' (An analysis of twenty years of review investigations, studies and opinions) in VAN LAETHEM, W. and VANDERBORGHT, J. (eds.), *Inzicht in toezicht* (Insight into monitoring), Antwerp, Intersentia, 2013, 266.

5 First the admissibility of a complaint is studied, after which it is processed by the Investigation Service. 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).

6 The reasons for opening information dossiers differ considerably: the management of an intelligence service reports an incident and the Committee wishes to check how it is handled; the media reports an incident and the Committee wishes to know whether this reporting corresponds with reality or whether there is a more general underlying problem, and so on.

objectives, the information dossier is not followed up. In 2017, an information dossier was opened on the deployment of the GISS intelligence capacity in a conflict zone, which led to a review investigation being initiated in 2018.

Lastly, very regular briefings are organised in which intelligence service members inform the Committee about current and important topics within the intelligence community (such as the functioning of the Belgian Passenger Information Unit BELPIU, the implementation of the directive on cooperation with foreign partner services, how certain countries try to exert their influence on Belgian interests, the functioning of the SIGINT Department, technical innovations in special intelligence methods, risk assessment, the fight against terrorism, and so on). Those briefings must promote informed discussions about the operations, powers and oversight of the intelligence and security services and CUTA. They can also lead to the opening of an investigation.

II.1. A COMPLAINT ABOUT THREE GISS OPERATIONS

II.1.1. CONTEXT

In May 2017, a GISS officer filed a complaint about operations that the I/H Department[7] had allegedly carried out, in which he believed irregularities or even illegalities had occurred. The Standing Committee I decided to open a review investigation into this.[8, 9] This investigation ran parallel to a judicial investigation, as the officer concerned had also approached the Public Prosecutor's Office.[10]

The complaint was threefold:

- the I/H Department allegedly intended to create an 'action unit' in Belgian territory;
- a mission of I/H Department members to a conflict zone was problematic;
- GISS maintained contact in Belgium with a person who has connections with a group that is at least closely involved in a terrorist organisation.

---

7 The I/H Department, which forms part of the GISS's I Division, is tasked with establishing networks of sources and informants that enable GISS to gather intelligence on foreign phenomena. The complainant had worked in this department for around two years.

8 The Minister of Defence and the Parliament were informed that a review investigation had been opened on 10 May 2017. The investigation was closed on 14 July 2017.

9 In 2018, it was decided to carry out a wider review investigation of the I/H Department. This inquiry limited itself to the complaint.

10 Investigators from the Investigation Service I were called upon in the context of this criminal investigation. They had not been involved in the review investigation.

II.1.2. A NEW 'ACTION UNIT' WITHIN THE MILITARY INTELLIGENCE SERVICE?

II.1.2.1. Information put forward by the complainant

The complainant asserted there was an embryonic type of 'action service' within the I/H Department. This unit would gather intelligence, but also – following the example of the French Directorate-General for External Security (DGSE) action units – 'set up operations'. While such an action service would only operate abroad in principle, the idea of it carrying out domestic operations was purportedly raised as well.

The complainant saw preparations for the unit's establishment supported by various factors: an employee of the I/H Department allegedly rented a private shooting range to give a non-military person training there with weapons of war; the complainant referred to text messages exchanged between the Commander of the I/H Department and his Divisional Superior, which allegedly involved deploying an 'action service' within Belgium; survival training was to be organised for external parties abroad; and the department members attended a Conduct After Capture (CAC) course.[11]

II.1.2.2. Findings by the Standing Committee I

The I/H Department did rent a private, but officially licensed shooting range on three different occasions. This was done with the formal approval of the hierarchy of the I Division. Renting a private shooting range has been an established practice for some time (also for the members of the I/Ops Department and the CI Division). After all, the use of a military shooting range is subject to many restrictions.[12] The person who received initiation was a source who had previously been in a very dangerous situation abroad and someone the I/H Department considered appropriate to receive a single basic firearms handling training course. The training unit within the I/H Department was apparently not informed of the shooting range rental. But since this was technical training, the training officer stated that his involvement was not required.

The Committee was further able to establish from text messages exchanged between the Commander of the I/H Department and the Head of the I Division

---

11 This training is organised primarily for pilots of the Belgian Air Force to prepare them should they be brought down behind enemy lines.

12 A strict timetable must be set a long time in advance, which is not always possible when employees have to go abroad. The owner of the shooting range could also provide different weapons to the Belgian army's standard issue, which members of the I/H Department might have to deal with during foreign missions.

that the domestic deployment of the I/H Department had been discussed and reference had been made to an 'action service'. However, the Committee believes this reference should be seen in its time context. It happened the day after the terrorist attacks in Paris, when threat level 4 had been declared in Belgium. Although it was not the intention to develop an 'action service' within Belgium, the Commander of the I/H Department offered his employees to assist the CI Division in Belgium, if necessary, but only to gather intelligence. In practice, however, the members of the I/H Department were not called upon to act in Belgium.

At the beginning of January 2015, the I/H Department sent a Belgian national who did not belong to GISS on a multi-day survival training course abroad. The Committee could establish that this was a new source for the I/H Department, who needed self-confidence and resistance for his own safety during assignments. The training course was organised in conjunction with the internal training department of the I/H Department, which, after a psychological profile of the person concerned, concluded this training was indeed suitable to equip him with additional skills.

As regards the CAC training in which I/H Department members allegedly participated, the Committee could establish that two members – including the training unit manager – of the I/H Department attended a 'light version' of the training course. The aim was to evaluate whether this training could be of interest to department members. The conclusion was negative.

The Standing Committee I therefore decided there were no reasons to assume plans to develop the I/H Department as an 'action service' or to make it domestically active. In addition, all training sessions were in accordance with the prevailing rules within the Belgian Armed Forces.

II.1.3. THE MISSION TO A CONFLICT ZONE AND SUPPORT TO A LOCAL ORGANISATION

II.1.3.1. Information put forward by the complainant

The issue involved a mission to a conflict zone by some I Division members in July 2015. During the mission, the intelligence service of a local organisation was contacted, medical equipment was provided, and according to the complainant, local troops were also given shooting instruction.

II.1.3.2. Findings by the Standing Committee I

In February 2015, military personnel from the I Division went to a conflict zone. The aim of the operation was to develop contacts with military players and

install a secure local IT connection through which intelligence could be sent to Belgium. Belgian foreign terrorist fighters (FTFs) who had joined IS or who were in transit were thought to be in the area. An attempt was made to obtain intelligence on the FTFs from these local players. A further idea was to develop friendly contacts with the militias in the area in case a Belgian F-16 was brought down there and the pilot would subsequently need to be extracted.[13]

The operation was initiated at the request of the Head of GISS at the time. The normal chain of command was followed[14] and there were regular consultations on the steps to be taken and missions to be carried out. Upon their return, the relevant I/H Department members always prepared detailed reports.

The February 2015 mission had already started in September 2014 through a contact with the relevant embassy in Belgium. The first contacts abroad were made in October and December 2014. The next mission left in July 2015; the Belgian delegation (I/H Department members) visited a training camp for local troops and – in exchange for intelligence that the GISS received from the local intelligence services – donated backpacks with medical equipment, intended to deliver first aid in combat conditions.[15] A trained GISS member demonstrated the use of the equipment on site.

II.1.3.3. The general framework for the deployment of military personnel abroad

The Chief of Defence believed such a mission can fit within a dual framework. On the one hand, the mission is 'covered' by the General Defence Operation Plan, drawn up at CHOD level and approved by the government. This plan provides capacity to use a number of military personnel in foreign missions for intelligence operations, without further specification. On the other hand, there is the Intelligence Steering Plan approved by the Minister of Defence. Intelligence gathering for the region concerned is put forward as a priority (given this is an operations area of the Belgian Armed Forces).

---

13 In this sense, the intelligence operation was in line with the government decision of late 2014, which decided to deploy the Belgian F-16 and participate in the Building Partner Capacity Program.

14 The existence of the operation was also reported to the CHOD at the time during a briefing on 29 March 2015.

15 This was Tactical Combat Casualty Care (TCCC) training. The use of the equipment is demonstrated in 'realistic' circumstances, i.e. partly on a real training ground and with participants in combat gear and sometimes even while under actual fire. Although this could wrongly be considered 'shooting instruction', it is part of how wounded people can be evacuated under fire. Such assignments are normally part of interventions or training missions by operational units of the Belgian Armed Forces (Special Forces or OPS/Trn). But this assignment was of an intelligence nature. The short initiation to the supplied equipment was just a practical consequence.

At the time of launching the operation, there were no official (political) directives from the National Security Council, setting criteria to determine the external intelligence services with which cooperation is possible.[16]

II.1.3.4. Information provided to the military and political echelons

The normal chain of command was followed within the I/H Department and GISS: I/H received formal approval to conduct the mission and kept the hierarchy informed of the operations. The CHOD received a briefing after the February 2015 mission and the Head of the Air Component was also informed (without operational details).

Outside the military chain, the Standing Committee I and State Security were also briefed, again without any operational details (April 2016).

In previous review investigations[17], the Committee stated that political assessment and cover is required in certain cases when making commitments within the context of international alliances. The Committee recommended at the time that competent ministers should be adequately informed so they could assume their political responsibility towards Parliament. The Minister of Defence and his office were informed in this case. A number of factors have contributed towards that: the fact that the operation and mission were conducted by a special agency of the I/H Department; the fact that it was an operation in a conflict zone and moreover in an air operations area of the Belgian Armed Forces (at the heart of Belgian military and political interest, so operations on the ground could have consequences at political level); and there were specific operational risks for the GISS members concerned. Those factors can be seen as risks that must be considered when deciding on an operation: the higher the risk, the quicker the minister should be informed.

In view of the above factors, the Standing Committee I therefore considered a briefing of the Minister of Defence to be an obvious step. It is up to the head of the service to choose the right moment for this. GISS acted correctly in this regard.

However, the Standing Committee I did find there was no structured framework and that the risk analysis – both strategic-policy and operational – had not been formalised.[18] Nonetheless, there were several evaluation moments.

The Committee noted that a private delivery service was used to transport the relevant medical equipment to the area. This posed a particular risk for the person concerned and was apparently not assessed in advance.

---

16 These directives only came into force later (Directive on the relationships between Belgian intelligence services and foreign intelligence services dated 26 September 2016).

17 See *inter alia* STANDING COMMITTEE I, *Activity Report 2014*, 33–34 and 89.

18 For the missions to these conflict zones in March and April 2017, the I/H Department used for the first time a specific document to determine the operational risks.

II.1.4. CONTACTS WITH A GROUP PURPORTEDLY LINKED TO A NON-ISLAMIST TERRORIST ORGANISATION

II.1.4.1. Information put forward by the complainant

A third issue raised by the complainant concerned contacts of GISS and I/H Department with a person belonging to a group – active in a conflict zone – which was purportedly part of or at least had close links to a non-Islamist terrorist organisation. However, GISS was not only alleged to have maintained contact with (the person from) this non-governmental group, but also to have played a facilitating role in contacts between the person concerned and a Belgian company. After all, the group tried to obtain certain materials through their representative, albeit of a non-lethal nature.

II.1.4.2. Findings by the Standing Committee I

The Standing Committee I found that GISS did have contacts with a group, active in a conflict zone, both in Belgium and in the conflict zone itself. The aim of the operation was to strengthen the GISS intelligence network. The group was an important player in this area and a possible source of intelligence about Belgian foreign terrorist fighters. Potential access to sources in other conflict zones was also envisaged through this channel.

The question of what GISS could give to this group in exchange for the intelligence was raised (*do-ut-des*). The non-lethal material was discussed during a preparatory meeting.

Regarding the classification of the group as 'terrorist' or 'linked to a terrorist organisation', the Committee found that the I Division analysis services had described this group as a 'franchise' of a non-Islamic terrorist organisation in 2015. A number of I/H Department reports also referred to this non-Islamic terrorist organisation when the representative of the group linked to it in Belgium was mentioned. Lastly, a regional superpower describes the group as the wing of a terrorist organisation and thus – by definition – a terrorist group itself.

On the other hand, this group does not figure in an international list of terrorist organisations, even though it has carried out certain acts in the war zone that could be questionable. GISS was also not the only service that maintained contact with this group; the army of a friendly power supported the group as early as September 2014 and has been supplying arms to it since May 2017.

The Committee therefore decided the group is not formally regarded as a terrorist organisation until further notice, but that the contacts were clearly of a 'sensitive nature'.

The Standing Committee I noted that this was an intelligence operation under the Information Steering Plan, but that special factors called for caution to be exercised.

II.1.4.3. Information provided to the military and political echelons

The hierarchy of the I/H Department was systematically kept informed of the contacts, both within the I Division and at command level. The CI Department of the SI Division was also informed.[19] Other military authorities were not informed, including the CHOD.[20] The CHOD was only told at the end of April 2017.

At the start of the operation, the I/H Department contacted the judicial authorities (first the Federal Judicial Police, then the Federal Magistrate) to inform them the person concerned was involved in an intelligence operation. A representative of State Security also attended the meeting. As soon as the operation got underway, the various services remained in contact with each other.

The Minister of Defence was not briefed in advance about this operation; he was only informed at the end of April 2017. However, the same factors applied as in the previous operation (see above): it was carried out by the I/H Department, was therefore very delicate by definition, and concerned a mission to a conflict zone with increased operational risks in an influential region of a NATO partner known not to be favourably disposed towards this group. These factors had to be taken into account when considering whether and when the intelligence service should brief the responsible minister. In addition, there was a link between the organisation concerned and a terrorist group (even though the organisation itself was not on an international terrorist list), there was a link with an ongoing judicial investigation, and it was known that the contacts could affect State Security's relationship with a partner service and possibly compromise the operation by this partner service. In view of the importance of the operation for GISS and its sensitive, even risky nature, including for Belgium's international relations, the Head of GISS should have informed the Director-General of State Security of the operation, so a common position could be adopted at the highest level.

Since this was a high-risk operation, the Standing Committee I considered it necessary for the Minister of Defence to have been briefed. The Committee

---

19 At the start of the operation, CI informed the I/H Department that the person concerned had been named in a judicial investigation by the Federal Prosecutor's Office responsible for terrorism.

20 According to the CHOD, it would be useful to inform C-OPS of such operations (perhaps even earlier than the CHOD himself), so C-OPS would be aware that Belgian military personnel have a covert presence in the area.

believed it was up to the head of the service to choose the right moment for this. When questioned, he stated he had felt the operation was still at an 'embryonic' stage and that the Minister of Defence (and the CHOD) would have been informed if more concrete progress had been made. The Standing Committee I believes the latter point – namely whether to inform the Minister in due time – is a choice of opportunity that only the Minister himself can ultimately assess. Since the Minister of Defence's office stated that the Minister – who only knew the facts after the operation was leaked – had completely covered this, it can be assumed the Minister believed that GISS had acted correctly.

Lastly, elements of a risk analysis were also included in various documents for this operation, for example, it was decided not to meet the group in Belgium because of the risk of compromise by the partner country. However, there was no overall risk assessment. The fact that GISS could have also opened up such an assessment to State Security was specifically relevant to the operation. After all, GISS knew that State Security maintained a relationship with a NATO partner service and that this service would not have been in favour of the Belgian contacts with the group.

II.2. POSSIBLE ILLEGAL RETRIEVAL OF BANKING TRANSACTIONS AND PROFESSIONAL SECRECY

II.2.1. A TWOFOLD COMPLAINT

The Standing Committee I received a complaint from the managing director of an accounting firm in mid-August 2017 through a lawyer. The complaint, which was directed against a State Security inspector, had two parts: on the one hand, it was alleged the inspector had pressurised the managing director in the sense that she was obliged to violate her professional secrecy[21]; on the other hand, it was claimed the information requested should have been the subject of a special intelligence method (Article 18/15 of the Intelligence Services Act).

II.2.2. RECONSTRUCTION OF THE FACTS

The State Security inspector contacted the accounting firm by telephone in mid-July 2017. The managing director was absent, so the inspector left his contact details. He explained he had introduced himself as a staff member of the

[21] Under Article 58, paragraph 4 of the Act of 22 April 1999 on the accounting and tax professions and in Article 458 of the Criminal Code.

Ministry of Justice who wanted to obtain information relating to a money laundering investigation.

On her return, the director contacted him by telephone and they agreed to meet in early August 2017. At the meeting, he immediately identified himself as a member of State Security, showed his official identification (service card) and explained the true circumstances of his visit (an investigation into possible espionage activities). State Security was interested in a client of the accounting firm. The inspector requested information on how contact had been made, access to the purchase and sales ledgers, copies of e-mails, etc. A copy of the target's financial statements were also handed over.

Their statements regarding the 'obligation' to cooperate differed: the managing director stated the inspector told her she was 'obliged' to cooperate. The inspector maintained he did not explicitly refer to an 'obligation', but did refer to the Intelligence Act.

There was no further contact between State Security and the accounting firm.

II.2.3. ASSESSMENT

The Standing Committee I did not find the inspector's actions unacceptable. He contacted someone by telephone to make an appointment and identified himself as a staff member of the Justice department, which is correct. Although he referred to 'money laundering' (which was not the truth), he could not give any classified information over the telephone. Using a cover story during initial contact, certainly by telephone, is acceptable, but one should not give the impression that you have specific powers.

The investigation could not determine whether the inspector actually referred to an 'obligation', and if so, what he would have meant by that.[22] The Standing Committee I was unable to reconstruct the exact wording of the discussion, but could not find the inspector had been unfair, intimidating or rude.

The managing director also stated that she was bound by specific professional secrecy, and this also applied to State Security. She claims she was wrongly induced to violate this secrecy. Article 16 of the Intelligence Services Act as amended by the Act of 30 March 2017 (and thus applicable in August 2017 when the interview between State Security and the managing director took place), stipulates that private persons and organisations may share information and personal data with the intelligence services if they are useful for those services' assignments and, conversely, that the intelligence services may request such information. This provision does not impose any restrictions on the professional

22 'Moral' obligation, legal obligation that can be sanctioned, 'duty' as a good citizen, etc.

secrecy of private persons or institutions, except as regards the professional secrecy of lawyers and doctors and the source secrecy of journalists. On the contrary, it can therefore be concluded that other forms of professional secrecy do not apply in relation to State Security. However, the Committee felt it would be appropriate for the legislator to determine more explicitly whether and in which cases other forms of professional secrecy could be waived, partly because such acts may directly affect the privacy of individuals as set out in Article 8 ECHR.

The remaining question: should a SIM method have been applied? Article 18/15 of the Intelligence Services Act stipulates that the intelligence services may request lists of bank accounts, safe-deposit boxes or financial instruments, banking transactions during a certain period or the details of holders of safe-deposit boxes or authorised representatives from a bank or financial institution. The managing director handed over the company's purchase and sales ledgers, which contained financial data, including banking transactions and bank accounts. But this is not what is meant in Article 18/15 of the Intelligence Services Act. The fact that the data provided by the accounting firm included banking details therefore does not mean that State Security should have applied a SIM method for this purpose. The banking details appeared only 'occasionally' in the requested data and State Security did not request a 'list of bank accounts or banking transactions' in any case, which the accountancy firm also could not have provided.[23]

---

[23] A side issue in this case is whether the 'nature' of the body from which State Security requests a list of banking details, is decisive for determining whether Article 18/15 of the Intelligence Services Act applies. After all, the Act refers to 'banks or financial institutions'. In a previous case, the Standing Committee I decided there was a method as referred to in Article 18/15 of the Intelligence Services Act when it came to requesting data from the Central Information Point (CIP) of the National Bank of Belgium. The Committee examined the agreement of 16 November 2015 between the National Bank of Belgium (NBB) and State Security, by which the latter would be given access, on simple request, to the data included in the Central Information Point (CIP). This is a database in which all banking, exchange, credit and savings institutions must divulge the identity of their clients and their account numbers. State Security held the view that consulting such a database constituted an ordinary method (namely as provided for in Article 14 of the Intelligence Services Act). However, the Committee did not agree with this. Although the Committee found that State Security's initiative showed that the service was actively tapping into useful channels of information, it referred to Article 18/15, §1, first paragraph of the Intelligence Services Act. This article regards requesting lists of bank accounts as an exceptional method. No reservation is made in this regard about the institution from which the information is obtained. Accordingly, even if the NBB is not regarded as a 'bank' or 'financial institution' within the meaning of Article 18/5, §2 of the Intelligence Services Act, the lists are still 'protected' by the mechanism of the exceptional method. If State Security therefore wishes to obtain lists of bank accounts from the CIP, an exceptional method must first be requested. The Minister of Justice stated that, pending additional consultation, State Security must apply the SIM procedure for the purpose of searching the CIP.

II.3. MISUSE OF A SERVICE CARD BY A STATE SECURITY MEMBER

In May 2017, a State Security member approached the Standing Committee I with a complaint about a colleague. This colleague allegedly abused his capacity as a member of the intelligence service and presented his service card to an accommodation provider to obtain information about the complainant. The two had been at odds with each other for some time.

The complainant had first contacted the State Security hierarchy, which launched an internal investigation and advised him to file a criminal complaint. However, the complainant did not do this.

The Standing Committee I established that the person against whom the complaint was made had acknowledged the facts in a document that was part of civil proceedings between the two colleagues. The investigative service believed the complaint would be best dealt with by the judicial authority in view of the possible criminal nature of the facts (misuse of the official capacity of an official/service card for personal purposes).

The Standing Committee I took two initiatives. First, it informed State Security of the complaint being made, indicating that the person who was the subject of the complaint had also apparently made threats and still had his service weapon. The Committee later learnt that State Security had taken the service weapon from the person concerned and initiated a disciplinary inquiry. Second, the Committee reported the case to the Public Prosecutor under Article 29 of the Code of Criminal Procedure, who requested the Investigation Service I to carry out a number of investigative acts (Article 40 of the Review Act).

The Public Prosecutor's Office decided not to prosecute.

II.4. COMPLAINT FOLLOWING A NEGATIVE DECISION ON A SECURITY CLEARANCE

II.4.1. SUBJECT OF THE COMPLAINT

In February 2017, an oral complaint was lodged against GISS.[24] The complaint related to how the military intelligence service had conducted a security investigation for granting a 'Secret' level security clearance needed for the complainant's duties in the Ministry of Defence and the Federal Police.[25] The complainant's grievances were as follows:

---

24 The Monitoring Committee was informed of the results of this complaint inquiry on 14 December 2017.

25 For a security clearance within the Federal Police, the National Security Authority is the security authority, while for a security clearance within Ministry of Defence, this is the Head of GISS.

– the lack of transparency of the procedure for granting the security clearance;
– the lack of professionalism by the agents in charge of the dossier;
– discriminatory treatment against the complainant and his girlfriend;
– the humiliating and provocative attitude of the officers who questioned him.

II.4.2. FINDINGS

II.4.2.1. Lack of transparency of the procedure for granting the security clearance

The Act of 11 December 1998 on classification and security clearances, certificates and advice (Classification and Security Clearances Act), more specifically Articles 16 to 22, stipulates how a security investigation is to be conducted.

The applicant for the security clearance is informed of the level and purpose of the clearance, the types of information that may be examined or verified during the security investigation, the conduct of the investigation and the period of validity of the security clearance (Article 16 of the Classification and Security Clearances Act). The consent of the applicant is required before the security investigation can be carried out. This information is included in the form attached to the Royal Decree of 24 March 2000. This is the document that the applicant for the security clearance must sign for approval.[26, 27]

The Act otherwise does not provide for the application of any principle of transparency, as invoked by the complainant, during the security investigations, nor does it stipulate the need for an open debate with the applicant for the clearance prior to the security authority's decision.[28]

Since the complainant received the legal warning and consented to the security investigation, it was conducted in that respect in accordance with the rules of the Classification and Security Clearances Act. The first grievance concerning the lack of transparency of the procedure therefore proved to be unfounded.

---

26 The complainant signed a first form on 13 December 2012 and a second form on 27 October 2015.

27 The National Security Council determines the scope of the security investigation for each clearance level. Only agents of the intelligence services, the National Security Authority and the Standing Committee I are informed of the National Security Council's decision regarding the scope of the investigations (Article 18 of the Classification and Security Clearances Act).

28 However, if an appeal is lodged with the Appeal Body, the complainant and his lawyer may consult the investigation dossier or investigation report at the registry of the Appeal Body (except for certain information that must remain secret under Article 5, §3 of the Act establishing an Appeal Body); the complainant did that in October 2016 and January 2017.

II.4.2.2. Lack of professionalism by the agents in charge of the dossier

The investigation revealed that the periods laid down in Article 25 of the Royal Decree of 24 March 2000 implementing the Classification and Security Clearances Act had not been observed. An abnormally long time elapsed between the first security clearance application (November 2012) and the GISS's first decision refusing to grant the complainant a security clearance (May 2016).

There were several reasons for this significant delay. The Standing Committee I established that the complainant's first appeal to the Appeal Body for lack of a decision on his application for security clearance was filed in April 2016, while he had already submitted his first application in November 2012. It also showed there were actual delays and shortcomings both in the internal provision of information to GISS and in the exchange of information between GISS and other services. The second grievance was therefore partially well-founded.

II.4.2.3. Discriminatory treatment against the complainant and his partner

The complainant found it 'discriminatory' that his partner, with whom he did not cohabit, had to undergo a security investigation and that he needed several interviews himself.

The Classification and Security Clearances Act does not make it compulsory for a security clearance applicant's partner to be interviewed if the parties do not live under the same roof. However, the legislator does not prohibit the services in charge of a security investigation from obtaining information about persons with whom a security clearance applicant associates, if they deem it useful.

Having regard to the complainant's security dossier, the Committee considered the reasons for the request to interview his partner justified and certainly not the expression of a discriminatory intention towards him or his partner. The Committee moreover found that the interview might have allowed the complainant to explain certain aspects of his private life that the service wished to clarify. However, the refusal of the complainant's partner to attend an interview could not in itself constitute a reason for the negative decision made in respect of the complainant.

The third grievance was therefore unfounded.

II.4.2.4. Humiliating and provocative attitude of the officers

The report of the contested interview showed the atmosphere was clearly tense from the outset; however, the report did not contain any statement or opinion that could be considered humiliating or provocative to anyone.

Similarly, the internal security investigation reports relating to the complainant and his partner did not contain the slightest comment indicating

that his security clearance application had not been handled in a neutral manner. On the contrary, in the Standing Committee I's opinion, all the information GISS gathered appeared to have been examined with great care and assessed impartially. Ultimately, it was GISS's continued suspicion due to a lack of information about certain aspects of the complainant's private life that led to the negative decision.

The fourth grievance was unfounded.

II.4.3. A CLEARANCE WAS NEVERTHELESS GRANTED

After the GISS Security Clearance Department had completed its security investigation, the Head of GISS refused to grant the security clearance in May 2016. The complainant lodged an appeal with the Appeal Body for security clearances, which ordered in January 2017 that a 'Secret' level security clearance should be granted to the complainant.

II.5. 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.[29] 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 as well 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 the Coordination Unit for Threat Assessment (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 parliamentary inquiry committee, which *de facto* dealt with the investigative questions, the Committees

[29] In this regard, see: STANDING COMMITTEE I, *Activity Report 2016*, 26–43 ('II.3. Information position of the two intelligence services before the Paris attacks').

no longer regarded it relevant to resume the investigation activities. In their joint meeting of 13 June 2017, the two 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.

II.6. INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2017 AND INVESTIGATIONS INITIATED IN 2017

II.6.1. INTERNATIONAL EXCHANGE OF DATA ON FOREIGN TERRORIST FIGHTERS

As early as 2016, during an international meeting with various European review bodies[30], it was decided to start a similar review investigation in all participating countries into the international cooperation between the various intelligence services with regard to the fight against foreign terrorist fighters (FTFs). This initiative subsequently received the express support of the chairperson of the Belgian Monitoring Committee. The intention was 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[31] consists of 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 2017, various investigation assignments were carried out at national and international level at both State Security and GISS. The results of the Belgian review investigation will – where possible, given restrictions due to classified information – be used as input for the international investigation. In this context, an expert meeting took place in Oslo in May 2017.

---

30 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.

31 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.

II.6.2. REVIEW INVESTIGATION INTO HOW THE GISS'S COUNTERINTELLIGENCE (CI) DEPARTMENT OPERATES

Under Article 32 of the Review Act, the Minister of Defence requested the Standing Committee I to conduct an investigation into how the GISS's Counterintelligence (CI) Department operates at the end of December 2016. After all, '*a dysfunctional service raises questions that necessitate an independent investigation*' (free translation), according to the minister. The direct reason for this decision was a letter of mid-December 2016 from a large number of CI managerial staff. This letter informed the minister of concerns about how the service operated and the circumstances under which they had to perform their statutory assignments.

The Standing Committee I opened its review investigation on 13 January 2017.[32]

The investigation ran from January 2017 to April 2018. In July 2017, an interim report was sent to the Committee chairman and the Minister of Defence. This report covered the service's staff situation (including the issue with regard to status), inadequate infrastructure, ICT and material conditions and, lastly, the procedures, organisation and gradual loss of autonomy. The final report was completed in May 2018.

The Standing Committee I was clearly confronted with an organisation in transition during its review investigation: the National Strategic Intelligence Plan was in full preparation, the structure was being redesigned (again), additional personnel were being recruited and the recommendations of the parliamentary inquiry committee into the terrorist attacks had to be implemented. The Standing Committee I stated first and foremost that national security requires a strong and reliable military intelligence service. That is also why the Committee is convinced that the CI Department has an interest in an organisation and management that meets the standards of an effective and efficient public service. The first interim report showed those standards were not being met.

---

32 In 2010, the Committee, supported by what was then the Monitoring Committee of the Senate, had conducted a similar audit. This 'performance audit' provided insight into the situation within the entire military intelligence service and wanted to create a dynamic that would lead to real change and improvement, where necessary. STANDING COMMITTEE I, *Activity Report 2011*, 99–101 ('II.1. Audit of the military intelligence service'). The Committee formulated a detailed number of recommendations (172–175, 'IX.2.1. Recommendations relating to the audit at GISS').

II.6.3. SECURITY VERIFICATIONS CONDUCTED BY THE INTELLIGENCE SERVICES

Each year, State Security and GISS investigate several thousand people wanting to obtain some kind of permit or authorisation or hold a certain position. The aim of those investigations is to check whether the persons concerned offer sufficient guarantees in terms of their trustworthiness.

The role that intelligence services play in the context of trustworthiness investigations is not always the same. Sometimes it is limited to passing on personal data in their possession to other authorities. Sometimes they actively look for additional information. Sometimes they give a reasoned opinion and, in some specific cases, they also take the final decision (alone or as part of a security authority) on whether to grant or revoke the permit or authorisation.

In this case, a complaint resulted in a review investigation. An employee at Brussels National Airport had his access badge revoked after a negative decision[33] from the National Security Authority. He lodged an appeal with the Appeal Body on security clearances, certificates and advice and brought an action for annulment and suspension before the Council of State. The Appeal Body ruled that the complaint was inadmissible because it was lodged against the decision of the FPS Mobility and Transport and not against the National Security Authority's opinion. The Council of State also rejected the complaint. The complainant then turned to the Standing Committee I, however without defining the subject of the complaint. He stated he did not understand why a negative opinion had been issued, as a result of which he lost his job and had his pilot licence suspended.

Based on this individual complaint, the Committee considered it legitimate to open a wider investigation into how intelligence services perform security verifications.[34] Due to other priorities, the first investigative acts could only be carried out in October 2017.

II.6.4. SUPPORTING SERVICES OF CUTA

The Threat Assessment Act of 10 July 2006 established the Coordination Unit for Threat Assessment (CUTA). This body aims to provide the political, administrative and judicial authorities with the most accurate possible picture of

---

33 The decision read as follows: '*whereas the person concerned has contacts with a radical family environment; whereas those contacts pose a potential security risk*' (free translation).

34 'Review investigation into how State Security and GISS perform security verifications, evaluate the data needed to issue security certificates or formulate security recommendations, under Articles 22*bis* to 22*sexies* of the Act of 11 December on classification and security clearances, certificates and advice (Classification and Security Clearances Act)' (free translation). The investigation was opened on 13 February 2017.

the terrorist or extremist threat in or against Belgium so they can react appropriately.[35] Its core task is to make ad hoc or strategic evaluations. This task is entrusted to analysts and experts (seconded from the 'supporting services'). Those supporting services, which are the coordination unit's most important source of information, include State Security, GISS, the local and federal police services, the Customs and Excise Administration of the FPS Finance, the Immigration Service of the FPS Home Affairs, the FPS Mobility and Transport and the FPS Foreign Affairs (Article 2, 2. of the Threat Assessment Act). They are very diverse services, each with their own culture and size.[36]

In 2010, the Standing Committee I and Standing Committee P carried out a joint review investigation into the information flows between CUTA and the supporting services, paying particular attention to the two intelligence services and the federal and local police.[37]

At the joint plenary meeting in December 2017, it was decided to open a review investigation into the 'other' supporting services.[38] With this joint investigation, the Standing Committees I and P wanted to draw up a *status quaestionis* of the information flows between CUTA and four other supporting services, based on an extensive survey.

---

35 W. VAN LAETHEM, 'Het coördinatieorgaan voor de dreigingsanalyse: een punctuele analyse' (The coordination unit for threat assessment: an ad hoc analysis), *Vigiles*, 2007, Vol. 4, 109–127. Also see: BELGIAN STANDING COMMITTEE I, *All Source threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, Antwerp, Intersentia, 2010, 220 p.

36 The legislator allowed other institutions to be added to the list of 'supporting services'.

37 In this regard, see STANDING COMMITTEE I, *Activity Report 2010*, 52 ('II.12.6. Communication of intelligence to CUTA by the supporting services) and the more detailed *Activity Report 2011*, 117–125 ('II.4. The information flows between CUTA and its supporting services').

38 Review investigation into the CUTA supporting services excluding the integrated police and intelligence services.

CHAPTER III
CONTROL OF SPECIAL AND CERTAIN ORDINARY INTELLIGENCE METHODS

This chapter summarises the use of special intelligence methods by State Security and GISS in 2017, and the manner in which the Standing Committee I has performed its jurisdictional monitoring assignment in this regard. 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.

The report includes further statistics on the use of special and certain ordinary methods by State Security and the General Intelligence and Security Service, and on the manner in which the Standing Committee I performs its jurisdictional monitoring of the special methods.

However, reference should first be made to the important legislative amendment that entered into force in 2017 (more specifically on 8 May 2017) regarding the tasks and powers of the intelligence services in general, and the use of specific and exceptional methods in particular. The Act of 30 March 2017 (*Belgian Official Journal* of 28 April 2017) substantially amended the Act of 30 November 1998 governing the intelligence and security services, including with regard to the use of special intelligence methods. Overall, it can be stated that State Security and GISS have been given more powers. It is impossible to comment on every amendment within the scope of this activity report. However, to the extent that an amendment has affected (the use of) specific and exceptional intelligence methods, it will be considered in the following sections.

III.1. STATISTICS RELATING TO THE SPECIFIC AND CERTAIN ORDINARY METHODS

Between 1 January and 31 December 2017, a combined total of 1,923 authorisations was granted by the two intelligence services for the use of special intelligence methods: 1,822 by State Security (of which 1612 were for specific and 210 were for exceptional methods) and 101 by GISS (of which 79 were for specific and 22 were for exceptional methods).

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
2017	79	22	1,612	210	1,923

These tables show that the number of methods used by GISS remains low and shows a decreasing trend, while the increase at State Security continues. We see the same picture with the ordinary method of requests made to operators to identify certain means of communication. State Security made no fewer than 4,327 requests compared to 257 requests by GISS.[39]

	Requests by GISS	Requests by State Security
2016	216	2,203
2017	257	4,327

Four categories are distinguished for each service below: the statistics for certain ordinary methods, statistics for specific methods, statistics for exceptional methods, and statistics for the interests and threats justifying the use of the special methods (statistics on the interests and threats relating to ordinary methods are not yet available).

III.1.1. METHODS WITH REGARD TO GISS

III.1.1.1. Ordinary methods

Under the Act of 5 February 2016 amending criminal law and criminal procedure and regarding various provisions in the matter of justice (*Belgian Office Journal* of 19 February 2016) – following the recommendations of the Standing Committee I[40] – the identification of the user of telecommunication, such as a telephone number or IP address, or of a used means of communication is regarded as an ordinary method to the extent that this happens through a

[39] No bank details were requested in relation to the prepaid card issue (also see further under III.1.1.1.).

[40] STANDING COMMITTEE I, *Activiteitenverslag 2012* (Activity Report 2012), 69.

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 is made with the help of a technical device – and thus not through a request to an operator – the collection remains a specific method. Article 18/7 §1 of the Intelligence Services Act was amended for this purpose.

The 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.[41] Under Article 35 §2, first paragraph, of the Review Act of 18 July 1991, the Committee reports on this to the Chamber of Representatives in its annual report.

The Act of 1 September 2016 (*Belgian Official Journal* of 7 December 2016) also introduced a new ordinary method in the same Article 16/2 of the Intelligence Services Act: '*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 – keep a register of all requested identifications. Under Article 35 §2, first paragraph, of the Review Act of 18 July 1991, the Committee must also report on this to the Chamber of Representatives in its annual report.[42]

The table below summarises (1) the number of requests to operators (in 2017 there were no direct accesses (3) or requests to banking institutions (4)) and (2) the number of requested numbers (one request sometimes involves dozens of numbers).

---

41 In practice, the Committee receives a monthly letter with the number of requests. The Committee decided it could support this approach but adds that it will, on the one hand, monitor how the intelligence services monitor the use of this method internally and, on the other hand, randomly check a number of requests each year. This implies that the services must always keep the data obtained through requests available for the Standing Committee I.

42 The Act of 25 December 2016 (*Belgian Official Journal* of 25 January 2017) introduced the possibility for State Security and GISS to access the information of the Passenger Information Unit (Article 16/3 of the Intelligence Services Act). The Committee will be informed of this method and may prohibit it, where appropriate. Unlike for the methods included in Article 16/2 of the Intelligence Services Act, no provision was made for mandatory reporting to Parliament; after all, Article 35 §2 of the Review Act was not amended. The Standing Committee I still recommends doing this, all the more so because retrieving transport and travel data under Article 18/6/1 of the Intelligence Services Act must be reported as it constitutes a specific method. The Committee further believes that such reporting is also appropriate for the possibility introduced by the Act of 21 March 2018 (*Belgian Official Journal* of 16 April 2018) of using camera images saved in data files (Article 16/4 of the Intelligence Services Act).

	Identifications relating to telecommunication			Identification relating to telecommunication through direct access (3)	Identification relating to prepaid cards (4)
	Number of methods	Number of requests (1)	Number of requested numbers (2)		
2013	66	Not known	Not known	Not applicable	Not applicable
2014	67	Not known	Not known	Not applicable	Not applicable
2015	55	Not known	Not known	Not applicable	Not applicable
2016	Not known	216	Not known	0	Not applicable
2017	Not known	257	1,058	0	0

III.1.1.2. Specific methods

The table below shows the statistics for the specific methods applied by GISS. First, the different categories are explained. Seven specific methods can be distinguished. In view of the legislative amendment, the scope of each method was modified as from 8 May 2017 (read: broadened). However, so as not to make the matter unnecessarily complex, the statistics from before and after the legislative amendment have not been broken down.

A. Before 8 May 2017 – Entry into and surveillance of or in places accessible to the public using a technical device (Article 18/2 §1, 1 and 18/4 of the Intelligence Services Act)
   After 8 May 2017 – Surveillance in places accessible to the public using a technical device or surveillance in a place that is inaccessible to the public and not hidden from view whether or not using technical resources (Article 18/4 of the Intelligence Services Act);
B. Before 8 May 2017 – Entry into and searching of places accessible to the public using a technical device (Article 18/2 §1, 2 and 18/5 of the Intelligence Services Act);
   After 8 May 2017 – Searching of places accessible to the public using a technical device, searching the content of locked objects or removing these objects (Article 18/5 of the Intelligence Services Act);
C. Before 8 May 2017 – Inspection of identification data for postal traffic and requesting the cooperation of a postal operator (Article 18/2 §1, 3 and Article 18/6 of the Intelligence Services Act);
   After 8 May 2017 – Inspection of identification data for postal traffic and requesting the cooperation of a postal operator (Article 18/6 of the Intelligence Services Act);

D. Before 8 May 2017 – No provision made;
   After 8 May 2017 – Requesting transport and travel data from private transport and travel services (Article 18/6/1 of the Intelligence Services Act);
E. Entire 2017 – the identification, with the help of a technical device, of the electronic communication services and resources to which a specific person has subscribed or that are usually used by a specific person and 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 (Article 18/7 of the Intelligence Services Act);
F. Entire 2017 – Tracing the call-associated data of electronic communication devices and requesting the cooperation of an operator (Article 18/8 of the Intelligence Services Act);
G. Entire 2017 – Monitoring of localisation data for electronic communications and requesting the cooperation of an operator (Article 18/8 of the Intelligence Services Act).

Specific methods (GISS)	Number of authorisations
Surveillance	7
Searching	0
Identification of postal traffic	0
Transport and travel data	0
Identification of subscriber, means of communication or payment instrument	4
Tracing call-associated data	36
Monitoring of localisation data	32
TOTAL	**79**

There are no notable trends to report regarding the GISS's use of specific methods.

III.1.1.3. Exceptional methods

The exceptional methods were also amended in some areas by the Act of 30 March 2017. These amendments are set out clearly below.

A. Before 8 May 2017 – Surveillance, whether or not using technical resources, in private places which are inaccessible to the public, in homes or enclosed outbuildings to a home within the meaning of Articles 479, 480 and 481 of

the Criminal Code, or in premises used for business purposes or as a place of residence by a lawyer, a doctor or a journalist, and to enter these places in the course of surveillance to install, repair or retrieve a technical device (Article 18/2 §2, 1 and 18/11 of the Intelligence Services Act);
After 8 May 2017 – Surveillance, whether or not using technical resources, in places that are inaccessible to the public and hidden from view and entering places that are inaccessible to the public, whether or not hidden from view for surveillance, installing a technical device, opening or removing an object (Article 18/11 of the Intelligence Services Act);

B. Before 8 May 2017 – Searching these places, whether or not using technical resources (Article 18/2 §2, 2 and Article 18/12 of the Intelligence Services Act);
After 8 May 2017 – Searching places that are inaccessible to the public, whether or not using technical resources, as well as objects located there, whether or not locked (Article 18/12 of the Intelligence Services Act);
C. Before 8 May 2017 – Establishing or using a legal person to support operational activities and using agents of the service, under cover of a fictional identity or capacity (Article 18/2 §2, 3 and 18/13 of the Intelligence Services Act);
After 8 May 2017 – Using a legal person as referred to in Article 13/3 §1 of the Intelligence Services Act to collect data (Article 18/13 of the Intelligence Services Act);
D. Entire 2017 – Opening and inspecting post, whether or not entrusted to a postal operator (Article 18/14 of the Intelligence Services Act);
E. Entire 2017 – Collecting data concerning bank accounts and banking transactions (Article 18/15 of the Intelligence Services Act);
F. Entire 2017 – Penetrating a computer system (Article 18/16 of the Intelligence Services Act);
G. Entire 2017 – Listening to, intercepting and recording communications/ wiretapping (Article 18/17 of the Intelligence Services Act).

Exceptional methods (GISS)	Number of authorisations
Surveillance	7
Searching	10
Fictitious legal person	0
Opening post	0
Collecting banking details	2
Penetrating computer systems	1
Wiretapping	1
TOTAL	**22**

III.1.1.4. Interests and threats justifying the use of special methods[43]

Since the entry into force of the Act of 29 January 2016 amending the Act of 30 November 1998 governing the intelligence and security service, on monitoring the activities of foreign intelligence services in Belgium, GISS may use specific and exceptional methods in relation to four assignments. This means that these methods cannot be used alone for security investigations or other assignments entrusted to GISS by special laws (e.g. performing security verifications for candidate military personnel). However, the Act of 30 March 2017 made changes to these four assignments, which can now be summarised as follows:

1. **Intelligence assignment (Article 11, 1 of the Intelligence Services Act)**
   - Collecting, analysing and processing intelligence relating to the factors that affect or could affect national and international security to the extent that the Armed Forces are or could be involved in providing intelligence support to their current or any future operations.
   - Collecting, analysing and processing intelligence relating to any activity which threatens or could threaten these interests:
     - the inviolability of the national territory or the continued existence of all or part of the population;
     - military defence plans;
     - the scientific and economic potential at the level of defence;
     - the fulfilment of the armed forces' assignments;
     - the safety and security of Belgian nationals abroad.
2. **Task of ensuring the preservation of military security (Article 11, 2 of the Intelligence Services Act)**
   - the military security of personnel who come under the Minister of Defence;
   - the military installations, weapons, ammunition, equipment, plans, texts, documents, computer and communications systems or other military objects;
   - in the context of cyberattacks on military computer and communication systems or systems controlled by the Minister of Defence, to neutralise the attack and identify the perpetrators, without prejudice to the right to immediately respond with its own cyberattack, in accordance with the legal provisions on armed conflicts.
3. **Protection of military secrets (Article 11, 3 of the Intelligence Services Act)**
   The protection of secrecy required which, in accordance with the international commitments of Belgium or in order to ensure the inviolability of the national territory and the execution of the assignments of the armed forces, relates to military installations, weapons, munitions, equipment, to plans, text, documents or other military objects, to military intelligence and

43 Each authorisation may involve multiple interests and threats.

communications, as well as to military computer and communications systems or systems managed by the Minister of Defence.

4. **Collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory' (Article 11, 5° of the Intelligence Services Act).**

Since the entry into force of the Act of 30 March 2017, the use of special methods is no longer limited to Belgian territory (Art. 18/1, 2 of the Intelligence Services Act).

Bearing in mind that various threats may be at play for each authorisation, these statistics can be recorded:

NATURE OF THE INTEREST	NUMBER IN 2017
Intelligence assignment	48
Military security	2
Protection of secrets	5
Monitoring the activities of foreign services in Belgium	46

NATURE OF THREAT	NUMBER IN 2017
Espionage	77
Terrorism (and radicalisation process)	16
Extremism	4
Interference	4
Criminal organisation	0
Other	0

In this reference year, statistics are available for the first time on monitoring the activities of foreign services in Belgium. The number is immediately very high. However, it cannot be deduced from this that GISS will monitor a new type of threat in 2017. After all, monitoring of foreign services was more quickly linked in the past to the 'intelligence assignment' within the context of the fight against 'espionage'.

III.1.2. METHODS WITH REGARD TO STATE SECURITY

III.1.2.1. Ordinary methods

The table below summarises (1) the number of requests to operators (in 2017 there were no direct accesses (3) or requests to banking institutions (4)) and (2) the number of requested numbers (one request sometimes involves dozens of numbers).

	Identifications relating to telecommunication			Identification relating to telecommunication through direct access (3)	Identification relating to prepaid cards (4)
	Number of methods	Number of requests (1)	Number of requested numbers (2)		
2013	66	Not known	Not known	Not applicable	Not applicable
2014	67	Not known	Not known	Not applicable	Not applicable
2015	55	Not known	Not known	Not applicable	Not applicable
2016	Not known	2,203	Not known	0	Not applicable
2017	Not known	4,327	21,566	0	0

Apart from the fact that it is almost impossible to compare the statistics on identifications over the years, the Committee cannot ignore the finding that the number of identifications has increased considerably since the introduction of the streamlined procedure under Article 16/2 of the Intelligence Services Act. Based on its general powers of review, the Committee will request State Security to internally investigate the extent to which this high number of requests is caused, or partly caused, by the streamlining of the procedure. Attention must also be paid to the nature of the threats that justify the requests and to whether and to what extent such requests are made at the behest of foreign authorities/partner services.

III.1.2.2. Specific methods

Specific methods (State Security)	Number of authorisations
Surveillance	121
Searching	0
Identification of postal traffic	0
Transport and travel data	54
Identification of subscriber, means of communication or payment instrument	49
Tracing call-associated data	708
Monitoring of localisation data	680
TOTAL	**1,612**

Although comparing the above figures with previous years is not clear cut due to the legislative amendment, it can still be said that the increase in the number of specific methods is mainly due to the sharp rise in the number of 'localisations' (680 compared to 596 last year).

III.1.2.3. Exceptional methods

Exceptional methods (State Security)	Number of authorisations
Surveillance	9
Searching	22
Fictitious legal person	0
Opening post	15
Collecting banking details	10
Penetrating computer systems	35
Wiretapping	119
TOTAL	**210**

The large number of attacks, both in Belgium and abroad, turned the decrease noted in the number of applied exceptional methods in 2015 into a sharp increase in 2016. This trend continued in 2017. The number of tapping measures stagnated.

III.1.2.4. 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). Since 8 May 2017, exceptional methods may also be used in the context of extremism and interference; previously, this was not possible.

The Act uses the following definitions:

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;

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;

3. Extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or aims, regardless whether they are of a political, ideological, religious or philosophical nature, which in theory or in practice conflict with the principles of democracy or human rights, with the proper functioning of democratic institutions or with other foundations of the rule of law;
4. Proliferation: trafficking in or transactions with respect to materials, products, goods or know-how which can contribute to the production or the development of non-conventional 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;
5. Harmful sectarian organisations: any group with a philosophical or religious purpose or which appears to be such and which, in terms of its organisation or practices, carries out harmful illegal activities, causes harm to individuals or society, or violates human dignity;
6. Interference: an attempt to use illegal, fraudulent or clandestine means to influence decision-making processes;
7. Criminal organisations: any structured association of more than two people that endures over time, aiming to carry out criminal acts and offences by mutual agreement, in order to 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 30 March 2017, the special methods may also be used '*from the territory of the Kingdom*' and therefore no longer only '*within*' the territory (Article 18/1, 1 of the Intelligence Services Act).

Bearing in mind that various threats may be at play for each authorisation, these statistics can be recorded:

NATURE OF THREAT	NUMBER IN 2017
Espionage	308
Terrorism (radicalisation process)	678
Extremism	63
Proliferation	4
Harmful sectarian organisations	0
Interference	9
Criminal organisations	0
Monitoring the activities of foreign services in Belgium[44]	308

The above figures show that 'terrorism' remains 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:

1. The internal security of the State and maintenance of democratic and constitutional order, namely:
   a) the security of the institutions of the State and the protection of the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to every constitutional state, as well as human rights and fundamental freedoms;
   b) the safety and physical and moral protection of persons and the safety and protection of goods;
2. 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;
3. Safeguarding the key elements of the scientific or economic potential.

NATURE OF INTEREST	NUMBER IN 2017
Internal security of the State and maintenance of democratic and constitutional order	1,053
External security of the State and international relations	1,024
Safeguarding the key elements of the scientific or economic potential	17

44 This power was introduced by the Act of 29 January 2016.

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

III.2.1. STATISTICS

This section deals with the activities of the Standing Committee I in relation to specific and exceptional intelligence methods. Attention will only be paid to the jurisdictional decisions made in this regard and not to the operational information. 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. Since 2017, a member of the Investigation Service has also attended the fortnightly meetings at which State Security informs the SIM Commission about the implementation of the exceptional methods. A report on this subject is prepared for the Standing Committee I, giving it a better understanding of these methods.[45]

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

1. At its own initiative;
2. At the request of the Privacy Commission;
3. As a result of a complaint from a citizen;
4. 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;
5. 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 specific or exceptional methods that have produced intelligence and that are used in a criminal case. The decision to ask for an opinion rests with the examining or criminal courts. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

[45] The Committee also recommended that GISS organise such fortnightly meetings. After all, this is a statutory obligation (Article 18/10 §1, third paragraph of the Intelligence Services Act and Article 9 of the Royal Decree of 12 October 2010).

METHOD OF REFERRAL	2013	2014	2015	2016	2017
1. At its own initiative	16	12	16	3	1
2. Data Protection Commission	0	0	0	0	0
3. Complaint	0	0	0	1	0
4. Suspension by SIM Commission	5	5	11	19	15
5. Authorisation by Minister	2	1	0	0	0
6. Pre-judicial consulting body	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**

The number of decisions taken by the Committee decreased in 2017, despite the increase in the number of methods and a new, complex legislative amendment that entered into force in mid-2017. All but one of the referrals result from a suspension by the SIM Commission.

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). This period was observed in all dossiers.

NATURE OF DECISION	2013	2014	2015	2016	2017
Decisions prior to the referral					
1. Invalid complaint	0	0	0	0	0
2. Manifestly unfounded complaint	0	0	0	0	0
Interim decisions					
3. Suspension of method	0	3	2	1	0
4. Additional information from SIM Commission	0	0	0	0	0
5. Additional information from intelligence service	0	1	1	4	0

6. Investigation assignment of Investigation Service	50	54	48	60	35
7. Hearing of SIM Commission members	0	0	2	0	0
8. Hearing of intelligence service members	0	0	2	0	0
9. Decision regarding investigative secrecy	0	0	0	0	0
10. Sensitive information during hearing	0	0	0	0	0
Final decisions					
11. Discontinuation of method	9	3	3	6	9
12. Partial discontinuation of method	5	10	13	4	6
13. Lifting or partial lifting of ban imposed by SIM Commission	2	0	4	11	0
14. No legal competence	0	0	0	0	0
15. Lawful authorisation / No discontinuation of method / Unfounded	7	4	6	2	1
Pre-judicial opinion					
16. Pre-judicial opinion	0	0	0	0	0

III.2.2. DECISIONS

The final decisions delivered by the Standing Committee I in 2017 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 because some of the decisions were classified.

The decisions were divided into three categories:

- Legal or procedural requirements prior to the implementation of a method;
- Legality of the method in terms of the applied techniques, data collected, duration of the measure, and nature of the threat;
- Consequences of an unlawful method or an unlawfully implemented method.

III.2.2.1. Legal or procedural requirements prior to the implementation of a method: prior decision of the head of service and notification of the SIM Commission

A specific method may be used only after the SIM Commission has been notified of the head of service's authorisation (Article 18/3, §1, second paragraph

of the Intelligence Services Act). Doubts about this arose in dossier 2017/5650. The SIM Commission noticed that the head of service had extended camera surveillance using a specific method, but that a number of days had elapsed between the end of the first period and the start of the second. It therefore suspended the method for the short period between the two valid authorisations. The service concerned also could not rule out for the Standing Committee I that no data had been collected during those few days. The Committee therefore concluded: '*indeed, any use of the specific method does not result from a decision (by the head of service) with notification to the SIM Commission; that, where applicable, any data collected are unlawful and the statutory procedure provided for in the Intelligence Services Act applies, even if [the service] considers destroying any data collected.*' (free translation). In another case, the SIM Commission established that an intelligence service had been using a technical device to carry out surveillance of a house for several days (Article 18/4 of the Intelligence Services Act) without the required permission (dossier 2017/5807). The period before and afterwards was covered by a valid authorisation. In all probability, it was a mere oversight. The Committee nonetheless held that '*it is undeniably certain that the prevailing statutory provisions for implementing a SIM were not observed. The statements of the [service] – asserting that the method, namely carrying out surveillance on a house, produces good results – do not alter this fact. The importance of the dossier likewise cannot correct this illegal situation*.' (free translation). The Committee therefore ordered the destruction of the illegally obtained intelligence.

The Committee had to take identical decisions in dossiers 2017/5832 and 2017/5843. The same issue of a 'non-consecutive extension' arose in those cases: the service had neglected to grant authorisation between two valid authorisations for a period of three and six days respectively. The Committee also held here that '*the importance of the dossier cannot correct the cited illegal situation*'. (free translation).

When the SIM Commission learnt from the head of an intelligence service that surveillance had occurred during a month without lawful authorisation, it ordered: '*the use of the data collected in this way is prohibited*' (free translation) (dossier 2017/5900). The Commission could only confirm this decision.

In dossier 2017/5998, the service itself noted that a specific method had continued after the expiry of the time limit specified in the authorisation. The service notified the SIM Commission, which prohibited the use of the data collected in that way. The Committee, under a referral made on its own initiative, confirmed the Commission's decision since *'the data were collected outside the period provided for in the head of service's decision; that these data were not collected in accordance with the law in the absence of the head of service's consent'* (free translation).

III.2.2.2. Legality of the method in terms of the techniques applied, data collected, duration of the measure, and nature of the threat

III.2.2.2.1. Retrieval of telephone data

In three identical cases, an intelligence service wanted to inspect call-associated data and locate a certain mobile telephone (dossiers 2017/5573, 2017/5574 and 2017/5575). It transpired from additional information requested by the SIM Commission that the service had come across that number by using an ordinary method (Article 16/2 of the Intelligence Services Act), even though the request to the operator showed it was not about the simple identification of a number but '*based on identification made through a technical operation, such as consulting information received via a mast*' (free translation). The method applied required the use of a specific method (Article 18/8 §1, 1 and 2° of the Intelligence Services Act) (also see III.2.3. in this regard).

On 3 April 2017, an intelligence service decided in two related dossiers (2017/5776 and 2017/5777) to obtain information on the call data of a telephone number, for the previous nine months, based on Article 18/8 of the Intelligence Services Act. Having regard to the threat involved, the law allows this for a maximum of '*nine months prior to the decision*.' (free translation). However, it transpired that the service wished to obtain information from 1 July 2016. The Committee held that '*the earliest date on which the nine-month period can start – considering that the date of the decision was 3 April 2017 – is 2 July 2016 and not 1 July 2016*' (free translation). The collection of telephone data on 1 July 2016 was therefore not covered by a legal method.

Dossier 2017/5916 was identical in this respect. The service wanted to access call and localisation data (Article 18/8 §1 of the Intelligence Services Act) for the period from 19 May 2016 to 16 May 2017. However, under Article 18/8 §2 of the Intelligence Services Act, '*the collection of such data may not exceed a period of 12 months prior to the date of the decision*' (free translation). As this decision was taken on 23 May 2017, '*the maximum period for retroactive data collection may extend from 22 May 2016 to 22 May 2017*' (free translation). The head of service's decision was therefore set aside with regard to the data collection from 19–21 May 2016.

This case law was subsequently repeated in two other dossiers.

Article 18/8, §2 of the Intelligence Services Act stipulates that '*for a potential threat concerning an activity that could relate to terrorism or extremism, […] the head of service, in his decision, may only requisition telephone or other data for a period of twelve months prior to the decision*' (free translation). In this case, the decision date was 27 December 2017. It follows from this that the method could cover the period from 26 December 2016 to 26 December 2017. However, the service had requested data from 20 December 2016 until 20 December 2017. The

Committee therefore concluded that '*this method […] started six days too early from a legal perspective. It should only have been activated as from 26 December 2016*' (free translation) (dossier 2017/6611).

As the threat in dossier 2017/6612 was 'espionage', telephone data could be requested only '*for a period of nine months prior to the decision*' (free translation) (Article 18/8 §2, 2 of the Intelligence Services Act). The head of service's decision did not respect that limit and therefore was partially unlawful.

When the SIM Commission asked the intelligence service concerned which request had been sent to the telecommunications operator under a perfectly legal authorisation to inspect call data, it established that localisation data had also been requested (dossier 2017/5994). Since requesting those data was not included in the authorisation, the Committee decided that '*any localisation data received from the operator were obtained illegally*' (free translation).

III.2.2.2.2. Retrieval of travel data

An intelligence service wished to examine the air travel of a target in contact with a person thought to have established a terrorist cell abroad (dossier 2017/6208). The method covered a period of more than two and a half years. The Committee held that '*the method is determined by Article 18/6/1 of the Intelligence Services Act, which does not set a time limit*' (free translation). However, the Committee noted that the legislator had set time limits for the method envisaged in Article 18/8 of the Intelligence Services Act. For example, the possibility to request telephone data was limited to six, nine or twelve months prior to the head of service's decision, depending on the nature of the threat. The Committee added, however, that '*placing time limits on requests to retrieve travel data, with reference to Article 18/8, would mean adding an unforeseen condition to Article 18/6/1.*' (free translation). But this does not mean that such a method can be used without limitation: *'all intelligence methods, whether specific or exceptional, must respect the principles of subsidiarity and proportionality; The Standing Committee I has previously applied this principle to place a time limit on specific surveillance provided for in Article 18/4 (see Activiteitenverslag 2010, page 68)*[46]*; Whereas, in this case, the nature and seriousness of the threat as described in the decision […] are such that a travel data request for a period of 32 months […] does not violate the principle of proportionality.*' (free translation).

III.2.2.3. Consequences of an unlawful method or an unlawfully implemented method

An intelligence service wanted to inspect call-associated data and locate a certain mobile telephone (dossiers 2017/5573, 2017/5574 and 2017/5575). It

46 See *Activity Report 2010 (i.e. the chapters translated into English)*, 74.

transpired from additional information requested by the SIM Commission that the service had come across that number by using an ordinary method (Article 16/2 of the Intelligence Services Act), even though the request to the operator showed it was not about the simple identification of a number. The method applied required the use of a specific method (Article 18/8 §1, 1 and 2° of the Intelligence Services Act). '*Whereas the mobile numbers were therefore obtained in a manner contrary with the law; Whereas this unlawfulness can only lead to the illegality of the methods based on a method considered to be illegal; Whereas the method described here therefore can only be illegal.*' (free translation).

III.3. CONCLUSIONS AND RECOMMENDATIONS

The Standing Committee I has formulated the following general conclusions and recommendations:

- The number of special methods used by State Security continues to rise sharply. As far as 2017 is concerned, this was explained by the increased intelligence activities due to the continuing terrorist threat. The increase was mainly due to the sharp rise in the number of 'localisations'.
- Despite the continuing terrorist threat, the already low number of special methods used by GISS decreased again.
- In relation to GISS, the Committee emphasises compliance with the statutory obligation to inform the SIM Commission every two weeks about implementing exceptional methods (Article 18/10 §1, third paragraph of the Intelligence Services Act and Article 9 of the Royal Decree of 12 October 2010).
- As always, GISS focused on 'espionage' for the use of SIM methods, while the focus for State Security was on 'terrorism'.
- Apart from the fact that it is almost impossible to compare the statistics on identifications over the years, the Committee cannot ignore the finding that the number of identifications has increased considerably since the introduction of the streamlined procedure under Article 16/2 of the Intelligence Services Act. Based on its general powers of review, the Committee will request State Security to internally investigate the extent to which this high number of requests is caused, or partly caused, by the streamlining of the procedure. Attention must also be paid to the nature of the threats that justify the requests and to whether and to what extent such requests are made at the behest of foreign authorities/partner services.
- Unlike for the use of special methods, the Committee does not have the statistics for the perceived threat and interests to be defended in relation to

ordinary methods under Article 16/2 of the Intelligence Services Act. The Committee recommends the services also record these data and provide them to the Standing Committee I.

– The Act of 25 December 2016 (*Belgian Official Journal* of 25 January 2017) introduced the possibility for State Security and GISS to access the information of the Passenger Information Unit (Article 16/3 of the Intelligence Services Act). The Committee will be informed of this method and may prohibit it, where appropriate. Unlike for Article 16/2 of the Intelligence Services Act, no provision was made for mandatory reporting to Parliament; after all, Article 35 §2 of the Review Act was not amended. The Standing Committee I still recommends doing this, all the more so because retrieving transport and travel data under Article 18/6/1 of the Intelligence Services Act must be reported as it constitutes a specific method. The Committee further believes that such reporting is also appropriate for the possibility introduced by the Act of 21 March 2018 (*Belgian Official Journal* of 16 April 2018) of using camera images saved in data files (Article 16/4 of the Intelligence Services Act).
– The Committee found illegality in 15 dossiers only. As an analysis of the case law shows, these are mainly dossiers in which the intelligence service concerned had neglected to grant authorisation to perform a method for what was sometimes a short period between two valid methods.

CHAPTER XII
RECOMMENDATIONS

Based on the review investigations, controls and inspections concluded in 2017, 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 (XII.1), the coordination and efficiency of the intelligence services, CUTA and the supporting services (XII.2) and, finally, the optimisation of the review capabilities of the Standing Committee I (XII.3).

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

XII.1.1. INVESTIGATION INTO THE SHARP RISE IN THE NUMBER OF ORDINARY IDENTIFICATIONS[47]

Since introducing the streamlined procedure under Article 16/2 of the Intelligence Services Act, by which certain identifications of communications are no longer considered a specific method, the number of requests sent to operators for identifications has risen sharply. Based on its general powers of review, the Committee recommends State Security internally investigate the extent to which this high number of requests is caused, or partly caused, by the streamlining of the procedure. Attention must also be paid to the nature of the threats that justify the requests and to whether and to what extent such requests are made at the behest of foreign authorities/partner services.

47 See 'Chapter III. Control of special and certain ordinary intelligence methods'.

XII.1.2. RULES OF CONDUCT FOR CONTACT WITH CITIZENS[48]

The Committee emphasised that intelligence agents may not wrongly create the impression they have certain powers or possibilities at their disposal. They must further consider how people who are not familiar with an intelligence service's operations could experience a personal meeting. The Committee recommends that State Security and GISS include this in their training, pay specific attention to it in their guidelines and, when inspectors deal with external parties, they clearly set out their powers and the rights and obligations of the person concerned. State Security and GISS could design certain instruments (for example, a brochure about the service and its powers, a synopsis of the Intelligence Act), which – if appropriate – could be presented or handed over to inform the person concerned.

XII.1.3. PROFESSIONAL SECRECY IN RELATION TO THE INTELLIGENCE SERVICES[49]

Since 2017, Article 16 of the Intelligence Services Act has stipulated that '*without prejudice to Article 2, §2, persons and organisations belonging to the private sector may, of their own accord, pass information and personal data to the intelligence and security services that are useful for the execution of their assignments*' (free translation). Certain professionals therefore are no longer bound by their obligation of professional secrecy in relation to the intelligence services. However, the Committee recommends the legislature explicitly sets out in that provision the extent to which specific confidentiality obligations apply, or do not apply, in relation to State Security and GISS.

XII.1.4. A MORE DETAILED INTERCEPTION PLAN[50]

The SIGINT department of GISS has been working with 'project records' for some time. The organisations and institutions to be intercepted are described in far more detail in those records than in the interception plan (for example, based on selectors). In this way, the records are better aligned with the statutory requirement to draw up a motivated list of institutions and organisations. The Committee believes the current lists need to be more detailed. GISS promised to make progress in that area but stated it could not provide exhaustive lists of targets.

48 See 'Chapter II.2. Possible illegal retrieval of banking transactions and professional secrecy'.
49 See 'Chapter II.2. Possible illegal retrieval of banking transactions and professional secrecy'.
50 See 'Chapter IV. Monitoring of foreign interceptions, image recordings and IT penetrations'.

XI.1.5. A STATUTORY BASIS FOR THE NEW COMMON DATABASES

In 2017, the Standing Committee I and the Control Agency for Management of Police Information (C.O.C.) recommended necessary regulatory decisions be taken regarding the new common databases on hate preachers and homegrown terrorist fighters. This obligation was fulfilled by the Royal Decrees of 23 April 2018[51]: homegrown terrorist fighters were added to the existing FTF database and a second database was established for hate preachers. However, Article 44/11/3*bis* of the Police Function Act stipulates that the competent ministers must report a database and the proposed processing methods to the C.O.C. and Standing Committee I prior to its establishment. Those institutions then have 30 days in which to formulate their opinion. As of the close of this activity report (mid-2018), no report has been made, even though both databases are operational.

XII.1.6. THE APPOINTMENT OF A SECURITY AND PRIVACY ADVISER

The C.O.C.'s and Standing Committee I's joint control of the FTF database revealed some problems, such as the lack of monitoring of the legitimacy of access and of a security incident reporting mechanism. Those problems could possibly be explained by the fact that no security and privacy adviser had yet been appointed in 2017. As both institutions had regularly called for this, the C.O.C. and Committee recommended that the competent ministers appoint this adviser as soon as possible.

XII.1.7. THE ROLE OF THE SECURITY AND PRIVACY ADVISERS

The C.O.C. and Standing Committee I recommend that the security consultants of the various services involved in operating the FTF database regularly request logins from the Federal Police on a random basis to periodically check the legitimacy of the consultations made. They also recommend that validation systems be

51 RD 23 April 2018 on the common database for Hate Propagandists and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Police Function Act; RD 23 April 2018 amending the Royal Decree of 21 July 2016 on the common database for Foreign Terrorist Fighters, implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Police Function Act and converting the common database for Foreign Terrorist Fighters into the common database for Terrorist Fighters.

periodically evaluated, that initiatives be taken on information security (access control, training, raising awareness etc.) and that best practices be exchanged.

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

XII.2.1. RISK ANALYSIS BEFORE FOREIGN MISSIONS[52]

As part of an investigation into how GISS had prepared a mission to a conflict zone where contacts were made with a certain organisation, the Standing Committee I noted that no formal risk analyses (neither strategic political policy nor operational) had been performed. The various mission documents raised risk elements, but not in a structured and synthesised way. When starting an operation, and obviously during it, it is appropriate for GISS to perform a structured, formal risk analysis. This enables the service and the minister, each within their own sphere of authority, to list all relevant risks (including those relating to Belgian military and foreign policy), to accept or reject them and, where appropriate, to take risk-limiting measures (including preparing communication in case a foreseen risk materialises during an operation).

XII.2.2. POLITICAL COVER FOR ALLIANCES[53]

Within the context of the international alliances they enter into, GISS and State Security may make commitments and choices that require political assessment and cover. As a general principle, the Committee has already recommended that competent ministers should be adequately informed so they would be able to assume their responsibility towards Parliament.[54] The Committee repeats that recommendation and makes it more specific by providing elements that could constitute criteria for assessing whether and when the service must inform the minister. They include questions such as which agency should perform the operation; the place where an operation occurs (a conflict zone or not, a Belgian military operations area or not); the magnitude of the strategic policy risks (which are listed structurally and formally); the international context; whether there is already a connection with a judicial investigation; the damage of compromising the operation etc. This list is not exhaustive. It is up to the service and minister to supplement and elaborate further on those criteria, if necessary.

52 See 'Chapter II.1. A complaint about three GISS operations'.
53 See 'Chapter II.1. A complaint about three GISS operations'.
54 STANDING COMMITTEE I, *Activity Report 2014*, 89.

XII.2.3. COORDINATING THE INTELLIGENCE POLICY BETWEEN GISS AND STATE SECURITY[55]

The Committee recommends that when the two Belgian intelligence services maintain contact with foreign services or non-state actors, they should consult each other to coordinate their intelligence policy and thus reach a coherent outcome. The 'National Intelligence Steering Plan', which is drawn up under the National Security Council's responsibility, may provide a useful framework for that purpose.

XII.2.4. THE MANAGEMENT, STORAGE AND COMMUNICATION OF INFORMATION FROM THE FTF DATABASE

The desirability of including sensitive police information (reports given code 00 or 01) should be examined. If the answer is negative, the legal framework needs to be adapted.

The C.O.C. and the Committee also call for the development of IT applications to facilitate monitoring of data retention periods and the transmission of information cards to the mayor.

Lastly, the Committee recommends securing the communication of information cards (or extracts from them) to third parties and subjecting this to prior evaluation, paying attention to the security measures those third parties have taken.

XII.3. RECOMMENDATION RELATED TO THE EFFECTIVENESS OF THE REVIEW

XII.3.1. PROVIDING INFORMATION TO THE STANDING COMMITTEE I[56]

Unlike for the use of special methods, the Committee does not have the figures for the perceived threat and interests to be defended in relation to ordinary methods under Article 16/2 of the Intelligence Services Act. The Committee recommends the services also record those data and provide them to the Standing Committee I.

---

55 See 'Chapter II.1. A complaint about three GISS operations'.

56 See 'Chapter III. Control of special and certain ordinary intelligence methods'.

XII.3.2. EXPANDING REPORTS TO PARLIAMENT[57]

The Act of 25 December 2016 (Belgian Official Journal of 25 January 2017) introduced the possibility for State Security and GISS to access the information of the Passenger Information Unit (Article 16/3 of the Intelligence Services Act). The Committee will be informed of this method and may prohibit it, if appropriate. Unlike for Article 16/2 of the Intelligence Services Act, no provision was made for mandatory reporting to Parliament; after all, Article 35 §2 of the Review Act was not amended.

The Standing Committee I still recommends doing this, all the more so because retrieving transport and travel data under Article 18/6/1 of the Intelligence Services Act must be reported as it constitutes a specific method. The Committee further believes that such reporting is also appropriate for the possibility introduced by the Act of 21 March 2018 (*Belgian Official Journal* of 16 April 2018) of using camera images stored in data files (Article 16/4 of the Intelligence Services Act).

XII.3.3. OBLIGATION TO PROVIDE INFORMATION RELATING TO EXCEPTIONAL METHODS[58]

In relation to GISS, the Committee emphasises compliance with the statutory obligation to inform the SIM Commission every two weeks about implementing exceptional methods (Article 18/10 §1, third paragraph of the Intelligence Services Act and Article 9 of the Royal Decree of 12 October 2010).

XII.3.4. AN INSTRUMENT FOR MONITORING THE EVOLUTION OF INTELLIGENCE RECORDS IN THE FTF DATABASE

To ensure adequate monitoring of the intelligence records in the FTF database, the C.O.C. and Standing Committee I insist on an instrument being developed that must allow access to all processing operations performed in an intelligence record. They request the Federal Police, in their capacity as the database manager, to take the necessary steps in thiss regard.

---

57 See 'Chapter III. Control of special and certain ordinary intelligence methods'.

58 See 'Chapter III. Control of special and certain ordinary intelligence methods'.

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 66*bis* shall be informed of the request of the minister to the Standing Committee I and of the content of the report before the end of the term laid down in Article 35, §1, 3°.

Art. 34

Within the framework of the objectives laid down in Article 1, the Standing Committee I deals with the complaints and denunciations it receives with regard to the operation, the intervention, the action or the failure to act of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services and their personnel.

Without prejudice to the provisions of Article 46, the Standing Committee I may decide not to follow up a complaint or a denunciation that is clearly unfounded. It may delegate this responsibility to the Head of the Investigation Service for the intelligence services.

The decision of the Standing Committee I not to follow up a complaint or denunciation and to close the investigation shall be justified and communicated to the party who made the complaint or denunciation.

When the investigation is closed, the results shall be communicated in general terms.

The Standing Committee I shall inform the managing officer of the intelligence service, the director of the Coordination Unit for Threat Assessment, or the managing officer of the other support service, depending on the case, of the conclusions of the investigation.

Art. 35

§1. The Standing Committee I shall report to the Chamber of Representatives and the Senate in the following cases:

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the Chamber of Representatives and the Senate, and to the competent ministers by 1 June at the latest. In this report, the Standing Committee I shall pay special attention to the specific and exceptional methods for gathering information, as referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, as also to

the application of Chapter IV/2 of the same Act and to the implementation of the Act of 10 July 2006 on threat assessment.

2° When the Chamber of Representatives has entrusted it with an investigation.

3° When at the end of a period that it believes to be reasonable, it notes that no action has been taken concerning its conclusions, or that the measures taken are inappropriate or inadequate. This period may not be less than sixty days.

§2. The Standing Committee I shall present a report annually to the Chamber of Representatives regarding the application of Article 16/2 and Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services. A copy of this annual report shall also be provided to the Ministers of Justice and Defence, and to State Security and the General Intelligence and Security Service, who may draw the attention of the Standing Committee I to their remarks.

The report shall contain the number of clearances granted, the duration for which the exceptional methods for gathering information are applicable, the number of persons involved and, if necessary, the results obtained. The report shall also mention the activities of the Standing Committee I.

The elements appearing in the report should not affect the proper functioning of the intelligence and security services or jeopardise the cooperation between Belgian and foreign intelligence and security services.

Art. 36

In order to prepare its conclusions of a general nature, the Chamber of Representatives may request the Standing Committee I to provide each and every investigation dossier, according to the terms and conditions that they determine and which in particular aim to safeguard the confidential nature of these dossiers and to protect the privacy of individuals. If the investigation was initiated at the request of a competent minister, his consent shall be required before handover of the investigation dossier, unless the term laid down in Article 35, §1, 3° has expired.

Art. 37

After acquiring the advisory opinion of the competent ministers or the competent authority, the Standing Committee I shall decide, within a period of one month from the request for advice, to make public all or part of its reports and conclusions, according to the terms and conditions it stipulates.

The reports and conclusions made public shall include the advisory opinion of the competent ministers and the competent authorities.

Art. 38

The Prosecutor-General and the Auditor-General shall ex-officio send to the Chairman of the Standing Committee I a copy of the judgments and judicial

decisions relating to the crimes or offences committed by the members of the intelligence services and the Coordination Unit for Threat Assessment.

The public prosecutor, the labour prosecutor, the federal prosecutor or the prosecutor-general of the Court of Appeal, depending on the case, shall inform the Chairman of the Standing Committee I whenever a criminal or judicial investigation into a crime or offence is initiated against a member of an intelligence service or the Coordination Unit for Threat Assessment.

At the request of the Chairman of the Standing Committee I, the prosecutor-general or the auditor-general may provide a copy of the deeds, documents or information relating to criminal proceedings against members of the intelligence services and the Coordination Unit for Threat Assessment for crimes or offences committed in the execution of their duties.

However, if the deed, document or information concerns an ongoing judicial investigation, it may only be communicated with the consent of the examining magistrate.

The copies shall be delivered without charge.

Art. 39.
The Standing Committee I shall exercise its authority over the Investigation Service for the intelligence services, assign investigations to it, and receive reports on all investigations that are carried out.

However, when they perform a judicial police assignment, the Head and the members of the Investigation Service for the intelligence services shall be subject to review by the prosecutor-general of the Court of Appeal or the federal prosecutor.

SECTION 2 – THE INVESTIGATION SERVICE FOR THE INTELLIGENCE SERVICES

Art. 40
By order of the Standing Committee I or, except with regard to the Coordination Unit for Threat Assessment and the other support services, on its own initiative, in which case it shall immediately inform the Chairman of the Standing Committee I, the Investigation Service for the intelligence services, hereinafter referred to as the "Investigation Service I", shall supervise the operations of the intelligence services, the Coordination Unit for Threat Assessment and the other support services, through investigations, within the limits of Article 1.

It shall examine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another support service. Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them,

as well as by the methods or actions, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

On its own initiative or at the request of the competent public prosecutor, military public prosecutor or examining magistrate, it shall, together with the other officers and agents of the judicial police, and even with a right of priority over them, investigate the crimes and offences which the members of the intelligence services and the Coordination Unit for Threat Assessment are charged with. With regard to the members of the other support services, this provision only applies with respect to the obligation laid down by Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

If the person filing a denunciation so wishes, his anonymity shall be guaranteed. In this event, his identity may only be disclosed within the Service and to the Standing Committee I.

Art. 41

A person may not be appointed Head of the Investigation Service I if he has not been a magistrate or a member of an intelligence or police service for a period of five years, or if he cannot demonstrate at least five years' relevant experience as a public servant in positions relating to the activities of the intelligence or police services. At the time of his appointment he must have attained the age of 35 years.

The Head of the Investigation Service I shall be appointed by the Standing Committee I for a renewable term of five years.

Before taking up his duties, the Head of the Investigation Service I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the Chairman of the Standing Committee I.

He must have knowledge of the French and Dutch languages.

He shall retain his right to advancement and salary increase.

He may be dismissed by the Standing Committee I.

Art. 42

Without prejudice to Article 39, second paragraph, the Head of the Investigation Service I shall manage it and set out the tasks, under the collegial authority, direction and supervision of the Standing Committee I.

He shall be responsible for relations with the Standing Committee I, from which he shall receive the assignments and to which he shall send the reports.

He shall be responsible for relations with the judicial authorities, from which he shall receive the requests and to which he shall send the reports referred to in Article 46.

Art. 43

Except for the cases laid down by Articles 40, paragraph 3, and 46, the Head of the Investigation Service I shall inform the competent minister or the competent authority that an investigation is initiated.

He shall send a report to the Standing Committee I at the end of each investigation assignment.

However, in the cases referred to in Articles 40, paragraph 3, and 46, the report shall be limited to the information necessary for the Standing Committee I to perform its assignments.

Art. 44

The members of the Investigation Service I shall be appointed and dismissed by the Standing Committee I on the recommendation of the Head of the Investigation Service I.

At least half of the members, and this for a renewable term of five years, shall be seconded from an intelligence or police service or an administration in which they have acquired at least five years' experience in positions relating to the activities of the intelligence or police services.

The members of the Investigation Service I shall take the same oath as the Head of the Service.

In the service or administration that they have been seconded from, they shall retain their right to advancement and salary increase.

Art. 45

The Head and the members of the Investigation Service I shall have the capacity of judicial police officer, assistant public prosecutor and assistant military public prosecutor.

In order to be appointed, they must hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Art. 46

When a member of the Investigation Service I has knowledge of a crime or offence, he shall produce a formal report that is forthwith sent by the Head of the Investigation Service I to the public prosecutor, to the military public prosecutor, or the examining magistrate, depending on the case.

The person who lodged the complaint or filed the denunciation, or the authority who called upon the Standing Committee I, shall be informed thereof by the Head of the Investigation Service I.

Art. 47

When a member of the Investigation Service I observes facts during an investigation that could constitute a disciplinary offence, the Head of the Investigation Service I shall forthwith inform the competent disciplinary authority thereof.

SECTION 3 – INVESTIGATION PROCEDURES

Art. 48

§1. Without prejudice to the legal provisions relating to the immunity and privilege, the Standing Committee I and the Investigation Service I may summon for hearing any person they believe useful to hear.

The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services which are being heard may testify about facts covered by professional secrecy.

§2. The Chairman of the Standing Committee I may have members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services summoned through the medium of a bailiff. The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services are bound to testify after having taken the oath prescribed by Article 934, paragraph 2 of the Judicial Code.

The members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services are bound to disclose to the Standing Committee I the secrets that they know of. If these secrets relate to an ongoing criminal or judicial inquiry, the Standing Committee I shall consult the competent magistrate in advance regarding this.

If the member or former members of the intelligence service, the Coordination Unit for Threat Assessment, or the other support services is of the opinion that he must not disclose the secret he has knowledge of because its disclosure would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule, or, if it concerns a member or former member of the Coordination Unit for Threat Assessment or another support service, the Chairmen of the two Standing Committees, who shall rule jointly.

§3. The Standing Committee I and the Investigation Service I may request the collaboration of interpreters and experts. They shall take the oath in the way used in the Assize Court. The remuneration due to them shall be paid in keeping with the rates for fees in civil cases.

§4. Article 9 of the Act of 3 May 1880 on parliamentary investigations shall apply to the members and former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services who are heard or summoned by the Standing Committee I as witnesses, and to the experts and interpreters who are called upon.

The formal reports establishing the offences committed before the Standing Committee I shall be drawn up by the Chairman and sent to the prosecutor-general of the Court of Appeal in the district where they were committed.

The members or former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other support services who refuse to testify before the Standing Committee I, and the experts and interpreters who refuse to collaborate, shall be liable to imprisonment of between one month and one year.

Art. 49
The members of the Investigation Service I may request the assistance of the public power in the performance of their assignments.

Art. 50
Any member of a police service who observes a crime or offence committed by a member of an intelligence service shall draw up an information report and send it to the Head of the Investigation Service I within a period of fifteen days.

Art. 51
The members of the Investigation Service I may make all observations in any location.

They may at all times, in the presence of their Head of Department, or his substitute, and of the chief of police, director or senior civil servant concerned, or his replacement, enter the premises where members of an intelligence service, the Coordination Unit for Threat Assessment or other support service perform their duties, in order to make substantive observations. In these locations, they may confiscate any objects and documents useful to their investigation, except for those relating to an ongoing criminal or judicial investigation. If the chief of police or his substitute is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 November 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairman of the Standing Committee I, who shall rule. If the director or the senior civil servant or his replacement is of the opinion that the confiscation of classified information would constitute a threat to the performance of the assignments of the intelligence and security services referred to in Articles 7, 8 and 11 of the Act of 30 threat ass 1998 governing the intelligence and security services, or would risk exposing a person to physical danger, the question shall be submitted to the Chairmen of the two Standing Committees, who shall rule jointly. The confiscated objects and documents shall be recorded in a special register kept for this purpose.

CHAPTER IV – JOINT MEETINGS OF THE STANDING POLICE SERVICES AND INTELLIGENCE AGENCIES REVIEW COMMITTEES

Art. 52
The Standing Committees shall exchange information on their activities and send each other the reports and conclusions referred to in Articles 9, 11, 33 and 35.

At least twice a year, they shall hold joint meetings, during which additional information may be exchanged.

Art. 53
During their joint meetings, the Standing Committees shall jointly perform their assignments (laid down in Articles 9, 10, 11, 33, 34 and 35):

1° With regard to the public services that perform both police and intelligence assignments;
2° With regard to the division of the assignments and the coordination of the operation between the police services on the one hand, and the intelligence services on the other;
3° With regard to any question put to them, either by a joint request from the ministers responsible for the Interior, Justice and National Defence, or at the request of the Chamber of Representatives;
4° With regard to any question that each Standing Committee believes does not fall within its exclusive competence;
5° With regard to any question considered by a Standing Committee to be sufficiently important to warrant a joint meeting;
6° With regard to the Coordination Unit for Threat Assessment or another support service.

A report shall be produced jointly by the Standing Committees at each joint meeting. This report may include advisory opinions and recommendations. It shall be sent as stipulated in Articles 9, 11, 33 and 35.

Art. 54
These joint meetings shall be chaired alternately by the Chairmen of the Standing Committees.

The functions of the secretariat of the joint meetings shall be performed by the longest serving registrar or, in the event of equal length of service, by the youngest registrar.

Art. 55
During the joint meetings, the Standing Committees may decide to assign investigation assignments to the two Investigation Services or to either one of them. They shall receive the reports on all the investigations that are carried out.

CHAPTER V – COMMON PROVISIONS

Art. 56
Each Standing Committee shall examine the complaints that are lodged with it by its former members or by former members of the Investigation Services who believe they have been subject to prejudicial measures because of the functions they have carried out in the Standing Committees or in the Investigation Services.

Art. 57
The funds required for the operation of the Standing Committees and the Investigation Services established by this Act shall be imputed to the appropriations budget.

The Chairmen, the members and the registrars of the Standing Committees, as well as the Director-General of the Investigation Service P and the Head of the Investigation Service I shall enjoy exemption from postal charges for official business.

Art. 58
Each Standing Committee shall appoint and dismiss the members of its administrative staff, on its own initiative or at the proposal of the registrar.

Under the collegial authority and supervision of the Standing Committee in question, the registrar shall be responsible for leading and managing the members of the administrative staff and shall distribute the tasks among them.

The Director-General of the Investigation Service P and the Head of the Investigation Service I shall have authority over the members of the administrative staff, where the number of members and their job requirements shall be defined by the Standing Committee in question, which assigns these members to them.

The registrar shall have authority over the members of the Investigation Service P or I, depending on the situation, where the number of members and the job requirements shall be defined by the Standing Committee in question, which assigns these members to him.

The staff members referred to in the third and fourth paragraphs shall retain the rights and obligations specific to the statute applicable to them.

Art. 59
The travel and subsistence expenses of the Chairman, the members and the registrar of each Standing Committee, the Director-General of the Investigation Service P, the Head of the Investigation Service I and the members of these services shall be determined according to the provisions applicable to the public services.

Art. 60
Each Standing Committee shall adopt its rules of procedure. The rules of procedure for the joint meetings shall be adopted jointly by the two Standing Committees.

The rules of procedure of both Standing Committees shall be approved by the Chamber of Representatives.

In accordance with paragraph 2, the Chamber of Representatives may amend the rules of procedure after acquiring the advisory opinion of the Standing Committee concerned. The advisory opinion shall be deemed favourable if it has not been given within sixty days of the request.

Art. 61
§1. The members of the Standing Committees shall enjoy the same status as the councillors of the Court of Audit. The rules governing the financial statute of the councillors of the Court of Audit, contained in the Act of 21 March 1964 on the remuneration of the members of the Court of Audit, as amended by the Acts of 14 March 1975 and 5 August 1992, shall apply to the members of the Standing Committees.

The members of the Standing Committees shall enjoy the pension scheme applicable to the civil servants of the General Administration. The following special conditions shall also apply.

The pension may be granted as soon as the person concerned has attained the age of fifty-five years. It shall be calculated on the basis of the average remuneration of the last five years, in proportion to one twentieth per year of service as a member of the Standing Committee.

A member who is no longer able to perform his duties due to illness or infirmity, but who has not attained the age of fifty-five years, may retire irrespective of his age. The pension shall be calculated according to the method laid down in the preceding paragraph.

The services that do not fall under the regulations referred to in paragraphs two to four and that qualify for the calculation of a state pension, shall be taken into account in application of the laws governing the calculation of the pensions for these services.

§2. Unless he has been dismissed, the member of a Standing Committee shall, when his duties are terminated or if his term of office is not renewed, receive a fixed severance grant equivalent to the gross monthly salary of the last eighteen months.

If this severance grant is granted before expiry of the first period of five years, it shall be reduced accordingly.

The following are excluded from this allowance:

1° The members to which Article 65 applies.
2° The members who were members of a police service or an intelligence and security service before their appointment to the Standing Committee and who rejoin this service.

§3. The registrars of the Standing Committees shall enjoy the same statute and pension scheme as the registrars of the Court of Audit.

Article 365, §2, a), of the Judicial Code shall apply to the registrars of the Standing Committees.

Art. 61*bis*

The Chairman of each Standing Committee shall, in accordance with the principle of collective responsibility, preside the meetings of that Committee and assume the day-to-day management of its activities. He shall ensure the application of the rules of procedure, the proper functioning of the Committee, as well as the proper performance of its assignments. He shall also ensure that the performance of the judicial police assignments does not impede the performance of the investigations. To this end, he shall hold the necessary consultations with the competent judicial authorities.

For the implementation of the authorities entrusted to him, the Chairman of each Standing Committee shall be assisted by the registrar and, respectively, by either the Director-General of the Investigation Service P or the Head of the Investigation Service I.

Art. 62

Without prejudice to Article 58, the registrar shall act under the collegial authority and the supervision of the Standing Committee in question, the registrar of each Committee shall among others manage the following:

the administrative staff;

the infrastructure and equipment of the Committee;

the secretariat of the Committee meetings and the minutes of the meetings;

the sending of documents;

the preservation and protection of the secrecy of the documentation and archives.

He shall prepare the budget of the Committee and keep the accounts.

Art. 63

The members of the Standing Committees are prohibited from attending the deliberations on affairs in which they have a direct or personal interest, or in which relatives by blood or marriage to the fourth degree inclusive, have a direct or personal interest.

Art. 64

The members of the Standing Committees, the registrars, the members of the Investigation Services, and the administrative staff shall be obliged to preserve the secrecy of the information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment of between eight days to one year, and a fine between one hundred francs and four thousand francs, or only one of these penalties, if they divulge these secrets in circumstances other than those stipulated by law or by the rules of procedure.

Art. 65
§1. Articles 1, 6, 1 and 12 of the Act of 18 September 1986 instituting political leave for the members of staff of the public service shall apply, where appropriate and with the necessary adaptations, to members of the Standing Committees.

§2. Members of the judiciary may be appointed as members of the Standing Police Services Review Committee and as members of the Standing Intelligence Agencies Review Committee, and as Director-General of the Investigation Service P or Head of the Investigation Service I.

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*)

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.]

(…)