ACTIVITY REPORT 2019

ACTIVITY REPORT 2019

Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee

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 2019.
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

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

AD	Analysis Director
Appeal Body Act	Act of 11 December 1998 establishing an Appeal Body for security clearances, certificates and advice
BCCP	Belgian Code of Civil Procedure
BELPIU	Belgian Passenger Information Unit
BISC	Belgian Intelligence Studies Centre
BPR	Business Process Re-engineering
BSS	British Security Service (MI5)
CCB	Centre for Cyber Security Belgium
CCIRM	Collection Coordination Information Requirement Management (GISS)
CDB HP	Common database Hate Propagandist
CDB TF	Common database Terrorist Fighters
CGRS	Commissioner General for Refugees and Stateless Persons
CHOD	Chief of Defence
CI	Counterintelligence
Classification and Security Clearances Act	Act of 11 December 1998 on classification and security clearances, certificates and advice
CNCIS	*Commission nationale de contrôle des interceptions de sécurité*
CNCTR	*Commission nationale de contrôle des techniques de renseignement*
C.O.C.	Supervisory Body for Police Information
CSA	Competent Supervisory Authority
CTG	Counter Terrorism Group
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
CUTA	Coordination Unit for Threat Assessment
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DGD	Deputy Director-General
DISCC	Defense Intelligence and Security Coordination Centre (GISS)
DPA	Data Protection Authority

DP Act	Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data
DPA Act	Act of 3 December 2017 establishing the Data Protection Authority
DPO	Data Protection Officer
ECHR	European Court of Human Rights
EION	European Intelligence Oversight Network
FANC	Federal Agency for Nuclear Control
FIPU	Financial Intelligence Processing Unit
FPS	Federal Public Service
FTF	Foreign Terrorist Fighter
GCCR	Governmental Coordination and Crisis Centre
GCHQ	General Communications Headquarters
GDPR	General Data Protection Regulation
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*)
HP	Hate Propagandist
HTF	Homegrown Terrorist Fighter
HUMINT	Human intelligence
ICP	Intelligence collection plan
ICT	Information and communications technology
IMINT	Image intelligence
INE	Intelligence Network Europe
Intelligence Services Act	Act of 30 November 1998 governing the intelligence and security services
IO	Immigration Office
IOWG	Intelligence Oversight Working Group
IR	Investigation report
ISP	Intelligence Steering Plan
ISTAR	Intelligence, Surveillance, Target Acquisition & Reconnaissance
IT	Information Technology
LTF	Local Task Force
MoU	Memorandum of Understanding
NA	*Note aux autorités*
OT	Organisational Table
NATO	North Atlantic Treaty Organisation
NCO	Non-commissioned officer
NOS	Nato Office of Security
NSC	National Security Council

NTF	National Task Force
OSINT	Open sources intelligence
Parl. Doc.	Parliamentary documents
PNR	Passenger name record
PNR Act	Act of 25 December 2016 on the processing of passenger name record
POC	Point of contact
Policing Act	Act of 5 August 1992 on the police function
PVE	Potentially Violent Extremist
RD	Royal Decree
RD Classification and Security Clearances	Royal Decree of 24 March 2000 implementing the Act of 11 December 1998 and security clearances, certificates and advice
RD CUTA	Royal Decree of 28 November 2006 implementing the Act of 10 July 2006 on Threat Assessment
RD FTF	Royal Decree of 21 July 2016 on the common database of foreign terrorist fighters and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Policing
RD HP	Royal Decree of 23 April 2018 on the common database of Hate Propagandists and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Policing Act
RD TF	Royal Decree of 23 April 2018 amending the Royal Decree of 21 July 2016 and redesigning the common database of foreign terrorist fighters as the common database of terrorist fighters
Review Act	Act of 18 July 1991 governing the review of police and intelligence services and of the Coordination Unit for Threat Assessment
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
SIM Commission	Administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services
SIS	Secret Intelligence Service (MI6)
SOP	Standard Operating Procedures
Standing Committee I	Standing Intelligence Agencies Review Committee

Standing Committee P	Standing Police Monitoring Committee
State Security	*Veiligheid van de Staat – Sûreté de l'État*
SVS	Security Verifications Service
TC	Terrorism Convict
TF	Terrorist Fighter
Threat Assessment Act	Act of 10 July 2006 on Threat Assessment

INTRODUCTION

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

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

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

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

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

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

---

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

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

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 registrar 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). From 2006, with increased globalisation in mind, the Standing Committee I wished to meet the expectations of a broader public: the sections of the activity reports that were most relevant to the international intelligence community (the review investigations, the control of special and certain ordinary intelligence methods, the recommendations), have been translated into English. As a result, seven reports (the first seven as books) have been published in English by the Standing Committee I (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,* the *Activity Report 2016,* the *Activity Report 2017* and the *Activity Report 2018* (see www.comiteri.be).

Given the new assignments that have been entrusted to the Standing Committee I, the Committee considered it useful to translate the entire report. Being all faced with similar challenges, the Committee felt that the new translated chapters were indeed likely to interest the international audience. The Activity Report 2018 was the first to be fully translated into English and was the first to be presented in a new format. The reports are now only available in pdf format on www.comiteri.be.

Serge Lipszyc, Chairman
Pieter-Alexander De Brock, Counsellor
Laurent Van Doren, Counsellor
Wauter Van Laethem, Acting registrar

28 October 2020

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

PREFACE

In its first activity report published in September 1994, the Standing Committee I already pointed to the shortage of personnel at State Security and the General Intelligence Service (later GISS).[1] Twenty-six years later, this observation unfortunately still holds true.

The Committee notes that the intelligence community is not given its rightful place in Belgium in practice. This is because of the imbalance between the obligations and expectations the two services have to meet and their structural understaffing. But this is not necessarily an unsolvable problem!

The Committee's activity reports, like those of the inquiry committees, can no longer be a catalogue of memories or recommendations. And, '*shortly after the attacks, some at home and abroad labelled Belgium a failed state. Months of hard work in the Parliamentary Inquiry Committee made clear this is a gross exaggeration. As the chair of the Inquiry Committee put it, most things did and do run like a well-oiled machine, but there was and still is sand in that machine here and there. The Parliamentary Inquiry Committee's recommendations are aimed precisely at getting that sand out of the machine*'.[2]

Like most European countries, Belgium faces a wide range of threats today. There is no doubt that jihadist or far-right terrorism exists. And there are worrying developments of interference and espionage activities by foreign powers. These threats require our services to be able to respond. They all have the same goal: combating attacks on the democratic foundation of our State.

Is there valid reason to complain? Not all is a source of concern. We can see that the Committee's successive reports to those responsible in Defence have ensured the introduction of change management that has been become essential at GISS.

But this significant improvement is not enough to provide satisfaction. The review investigation into security screenings at Belgian intelligence services undeniably points to a real problem. Despite the recommendations of the Parliamentary Inquiry Committee on the Terrorist Attacks, how can we accept that new information in possession of the police, justice and security services is not shared in real time, but only much later, based on requests to extend security clearances, certificates or advice? This information remains stored in hermetically sealed silos for an unacceptable length of time. This finding is more than worrying.

---

1 STANDING COMMITTEE I, *Activity Report 1994*, 50.

2 BELGIAN CHAMBER OF REPRESENTATIVES, *Parliamentary Inquiry Committee on the Terrorist Attacks of 22 March 2016 Summary of work and recommendations*, 2018, 13.

The Parliamentary Committee's recommendation on this point remains a dead letter: '*Relevant information must flow smoothly from one policy level to another, from one public service to another. This smooth flow of information must also exist between the Belgian services and their international counterparts. This must enable security services to detect potential terrorists early, consult quickly, and define flexible priorities.*'[3]

The attacks in Paris and Brussels have spurred an avalanche of legislative initiatives. Both intelligence services and the Committee have seen their powers expanded accordingly. For the Committee, this expansion is undoubtedly a guarantee for the protection of privacy, citizens' rights and the proper functioning of the institutions. Unfortunately, these legal measures were adopted without considering the actual capacity of the institutions that must implement them. The Committee views it as its duty to regularly revisit this principle and to ensure that the legislative and executive branches also give due effect to these legislative developments.

Our role today is all the more important because the newly granted powers require effective monitoring. Without this monitoring, we cannot fulfil our role as guardians of democracy. The Committee is tasked not only with carefully monitoring the two intelligence services, but also, depending on a complex division of authority – either with the Standing Committee P or with the Supervisory Body for Police Information – with monitoring the proper functioning of the Coordination Unit for Threat Assessment (CUTA), its databases and support services.

Since 2018, the Committee has been the data protection authority in the area of intelligence. It thus became the guardian and protector of citizens' data. In a world where databases and metadata are becoming legion, the Committee's role is expanding. The Committee must be able to monitor the databases, their security flaws and the use of cyber. And the Committee must also monitor the issue of establishing a crossroads bank for security.

In addition to these duties, is it therefore not obvious that the Committee should also be responsible for monitoring other public services that perform intelligence work outside any monitoring or legal framework?

Besides monitoring the intelligence services, the Committee's role in supporting the Appeal Body – an administrative tribunal – is of the utmost importance. In this way, the Committee can ensure that it plays a role as 'a judicial public service' in the area of day-to-day security.

---

3 Ibid., 38 (free translation).

In light of these threats, new powers, and the many recommendations that are not put into practice, can we simply remain passive? The Committee believes that the general context in which GISS and State Security perform their daily assignments requires strong commitments to promoting security.

Serge Lipszyc
Chairman of the Standing Intelligence Agencies Review Committee
26 October 2020

CHAPTER I.
REVIEW INVESTIGATIONS

Various institutions or persons can refer a review investigation to the Standing Committee I: the Parliamentary Monitoring Committee, the Ministers in charge or any (legal) person wishing to make a complaint or report. The Committee can also take the lead itself. In 2019, the Standing Committee I finalised six review investigations (I.1 to I.6). Two of these investigations were started at its own initiative, two investigations were carried out at the request of the Parliamentary Monitoring Committee and, lastly, two investigations started from an individual complaint.[1] The Committee also opened seven new investigations in 2019. A brief description of the investigations still in progress and/or started follows in I.7. The recommendations made following the review investigations have been collected together in Chapter XI.

The Committee received a total of 90 complaints or reports in 2019.[2] After a brief preliminary investigation and after verifying some objective information, the Committee rejected 82 complaints or reports because they were evidently unfounded[3] (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 (Standing Committee P, the Federal Police, the Public Prosecutor or other bodies). Six of the eight complaints handled could be completed in 2019.

Besides review investigations, the Standing Committee I opens "information dossiers", which must enable a response to questions about the operations of the intelligence services and CUTA.[4] Where such dossiers reveal indications of dysfunctions or aspects of the operations of the intelligence services that require

---

1 A protocol was concluded with State Security in January 2019 under which the service grants access to its central database to individually mandated members of the Investigation Service I for consultations relating to the Committee's statutory duties or the security of performing assignments.

2 First the admissibility of the complaint is examined, after which it is processed by the Investigation Service I. If a general problem arises, the Committee may decide to open a review investigation, Otherwise the inquiry will be limited to the complaint *per se* (a complaint inquiry).

3 The Committee receives quite a few whimsical complaints and reports.

4 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, etc.

further examination, the Committee may open 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 objectives, the information dossier will not be followed up. Among other topics, the information dossiers opened in 2019 were about social consultation within the intelligence services, security risks and possible dysfunctions within GISS, and the work of the Parliamentary Inquiry Committee on Terrorist Attacks.[5]

I.1. SECURITY SCREENINGS CONDUCTED BY THE INTELLIGENCE SERVICES

Each year, State Security and GISS investigate several thousand people looking to obtain some kind of permit or authorisation or that wish to hold a certain position. The aim of these investigations is to check whether these people offer sufficient guarantees in terms of their trustworthiness and security.

The role that intelligence services play in the context of these 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 try to find 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 the authorisation.

Based on an individual complaint, the Committee considered it legitimate to open a wider investigation into how intelligence services perform security screenings[6].[7]

---

5 Full description: "Parliamentary inquiry into the circumstances that led to the terrorist attacks of 22 March 2016 at Brussels National Airport and at Maelbeek metro station in Brussels, including the development of and the approach to combating radicalism and the terrorist threat".

6 A "security screening" is defined as: *'an assessment imposed by or pursuant to the law that an administrative authority carries out based on its own data or on personal or other data submitted to it, which is used to determine whether the profile of a private person (natural or legal person) indicates a risk that they will or could inappropriately use a certain authorisation and, in so doing, could jeopardise certain fundamental State or other interests, thus enabling that authority or another national or foreign authority to make an informed decision about whether to grant, withdraw or restrict that authorisation*' (free translation). This definition taken is from W. VAN LAETHEM, "Veiligheidsscreenings" (Security Screenings), Practice Seminar, 22 November 2016 (Brussels, Politeia).

7 "Review investigation into how State Security and GISS perform security verifications, assess the information needed to issue security certificates or formulate advice, under Articles 22*bis* to 22*sexies* of the Act of 11 December 1998 on classification and security clearances, certificates and advice (Classification and Security Clearances Act)". The investigation was opened in February 2017 and closed in March 2019.

I.1.1. THE LEGAL FRAMEWORK

I.1.1.1. Statutory duties

The Act of 30 November 1998 has strictly defined the two intelligence services' duties and powers. The Intelligence Services Act specifies these duties for State Security and GISS in Articles 7 and 11 respectively. Besides intelligence assignments (Article 7, 1 and 3/1) and conducting security investigations (Article 7, 2), State Security may perform other assignments only if they have been '*entrusted to it by or pursuant to the law*' (Article 7, 4 of the Intelligence Services Act). The legislator was even stricter towards GISS as the Act does not give it the possibility of performing duties '*pursuant to the law*'. In relation to screenings performed by the intelligence services or which they cooperate in by transmitting data to other authorities, the above thus means there must be a specific legal basis that allows these activities.

In this respect, many statutory provisions allow State Security and/or GISS (GISS is not involved in some procedures) to forward the intelligence they have to various authorities that assess it on this basis. However, legal analysis has shown that all these regulations differ – sometimes fundamentally, sometimes superficially.

Apart from this, the Committee found that both intelligence services sometimes took inadequate or no account of these different regulations (see below). It was also clear that the services did not have adequate knowledge of the legislation and/or were not critical enough when it came to asking whether their cooperation in certain screenings was legally permitted (and, if so, under what conditions). And it transpired that the intelligence services were still referring to Article 19 of the Intelligence Services Act, even though the Committee had previously stated[8], in the context of screenings, that this article provided no legal basis for the systematic transmission of data to other authorities for the purpose of assessment.[9]

I.1.1.2. Adapted legislation

At the time of the review investigation, there was no legal basis for screening certain sensitive positions and sectors (e.g. prison officers). The Act of 23 February 2018 amended the legislation on security verifications during the investigation phase[10], resulting in an increasing number of requests for verifications (e.g. public transport, private security sector, and so on). The same legislation also created a

8 STANDING COMMITTEE I, *Activiteitenverslag 2003* (Activity Report 2003), 278-288. The Committee warned of potential legal problems if an authority continues to base its decisions on information it obtains as part of a systematic screening process from State Security or GISS without a specific legal basis. The investigation showed that this situation was still ongoing.

9 This analysis moreover led to the Act of 3 May 2005, which created a broad framework for screenings in the most diverse areas in the Classification Act of 11 December 1998.

10 Act of 28 February 2018 amending the Act of 11 December 1998 on classification and security clearances, certificates and advice, *Belgian Official Journal* 1 June 2018.

new duty for State Security and GISS: the services became responsible for assessing the threat of espionage in various sectors.

I.1.2. SECURITY SCREENINGS AT STATE SECURITY

I.1.2.1. Organisation

Applications for security verifications at State Security are initially handled by the Security Verifications Service (SVS). This service comes under the hierarchical responsibility of the Deputy Director-General (DGD). The analysis services, which come under the responsibility of the Analysis Director (AD), deal with certain types of screenings in a second phase.

The Committee found that SVS personnel received no specific training. Besides basic training on State Security's general structure and duties, they have the same, rather generic, training opportunities as other administrative staff. However, according to the head of the SVS, no gaps in training needs were identified in the past. The specific, task-related training is done on the job.

The Directorate-General of State Security views carrying out screenings as a specific assignment and would therefore like to have them all handled centrally within this service. State Security intended to restructure how its screenings assignment is carried out. Specifically, everything about screenings will be centralised within the SVS. In the course of the investigation, a working group started to look at the future of the SVS, and at creating a "Security and Advice" pillar that would group the SVS, SIs (security investigations) and SO (security office) together. The Directorate-General's decision to centralise handling all security verifications in one service in future increased workforce.

I.1.2.2. Quantitative data

State Security's figures[11] showed a steady increase in the number of verifications carried out. The increase in the number of naturalisations and declarations of nationality and the sharp rise in the number of verifications requested by the Immigration Office (IO) and the Office of the Commissioner General for Refugees and Stateless Persons (CGRS) were particularly striking. Another quantitatively

[11] The figures are merely indicative. The method used does not allow statistics about the exact number of positive verifications or hits to be generated. Therefore, it is not possible to monitor the services results (in the longer term). This also has an impact on strategy development in the sense that it is difficult to set objectives (and allocate resources or determine a substantiated workload distribution between the SVS and the analysis services).

important category of security screenings relates to the issue of access badges to certain parts of airports.

State Security applies a certain standard of how many verifications can be carried out. It exceeded this standard by 12% in 2017. Exceeding this standard implied the risk of a backlog problem if one or more employees were absent, as there would be no reserve to cover absenteeism.

I.1.2.3. Work processes

When conducting screenings, State Security acts both as an information provider to other authorities and as a security authority.[12]

SVS initially handles all requests for screenings. The Committee noted the legality of the request was not checked when the lists of names were received, which is nevertheless necessary in some cases (e.g. non-routine questions), although the SVS immediately performs a verification in State Security's database. If an individual is unknown, the employee handling the request replies directly to the competent authority/client. A positive hit is presented to the head of the service, who assesses the available information and then prepares a response for the requesting authority/client.

For screenings where the National Security Authority (NSA) is the competent security authority (e.g. for security verifications leading to a security certificate or advice), all relevant information is discussed collegially with all services involved at the NSA. A complete, contextualised memorandum is communicated to the NSA only in appeal procedures.

A different procedure is used for requests relating to a naturalisation application and requests by the IO or CGRS. If there is a hit in these cases, the request is sent to the geographically competent analysis service, which assesses the available information in the database and prepares a response in the form of a contextualised memorandum. The analysis services handled several thousand cases in 2017.[13] In some cases, the field services responsible for collecting information decided to investigate further (e.g. when the information available on a person was uncertain (unconfirmed) or outdated). Such additional investigation was not a priority for the collection services.

These processes were not described in writing in service memoranda or a handbook.

The Committee's investigation showed that the SVS conducts screenings without being able to clearly state the legal basis for it (see above). In some cases, the exact purpose of the request is unclear. In other words, whether it is a security

---

12 The latter applies when temporary personnel (e.g. for maintenance work) must be given access to the service's buildings and when the service itself organises events.

13 At the time of the investigation, no standardised criteria were in operation to prepare a response in relation to screening. Each service (SVS or analytical service) prepared a response as it saw fit.

screening or another check in State Security's database. [14] For this purpose, State Security (erroneously, see above) systematically referred to Article 19 of the Intelligence Services Act. Although it may be useful and advisable for the Belgian services to be consulted about Belgian residents who might be granted access to the facilities of international institutions based in Belgium, a legal mandate is required for this purpose.[15]

Lastly, the Committee found the relationship with the foreign partner services to be lacking during screenings. Because of the high workload, it is impossible to question foreign authorities in relation to screenings. However, this weakens State Security's information position and there is a risk that foreigners will slip through the net during security verifications. Conversely, the SVS responds to questions from foreign intelligence services, even though the legal basis is unclear in these cases too.

I.1.2.4. Resources

State Security believes its responsibility when screening on behalf of other security authorities is limited to checking whether the entity (person) is known in its own documentation (internal database).

State Security uses one central database for this purpose. During the investigation, it became clear that the inaccuracies that SVS had noted in this database had not been corrected.[16] When this databank was developed, the existence of the SVS or its assignment was hardly or not taken into account. As a result, because of the way the database is structured, the SVS can prepare its own documents (e.g. internal reports of consultative meetings it participates in with external partners) and enter them in the database, but these documents are visible only to the employees of the SVS itself.

As for in-house IT resources, improvements will be made to the database structure for screening assignments. However, these improvements are part of the more general reform of the service, the exact timing of which is unclear.

---

14 For example, screenings are conducted at the request of NATO's security service, the NATO Office of Security (NOS). This is a screening of individuals who are granted or denied access to NATO installations.

15 Such screenings were made possible by the Act of 23 February 2018. Before security verifications can be requested for an international institution, an agreement must be concluded between the competent administrative authority and the institution involved, and a threat, risk and impact analysis must be performed (Act of 23 February 2018 amending the Act of 11 December 1998 on classification and security clearances, certificates and advice).

16 It should be mentioned that the reason for the review investigation, namely a complaint from someone whose naturalisation procedure had a negative outcome, was because information was used that could not be fully substantiated, or at least was not up to date. The presence of incomplete or incorrect identities in State Security's database increases the risk of "false" results during security verifications. Failing to supplement information runs counter to the principles of personal data protection.

The adapted legislation on security verifications (see above) provided that 25% of the fee payable by the applicant for a security certificate and advice will go to the service(s) carrying out the verification.[17] These funds can be invested in additional resources.

I.1.2.5. Improvement plan

State Security saw several opportunities for improvements regarding screenings.

One of the most useful and necessary improvements is the creation of a flagging system that identifies everyone known in the database who are or who have been the subject of a screening. This would allow the analysis and field services to put any new, relevant information relating to that person in a security verification, and bring it to the SVS's attention.

The service would also consider it a positive development if an agreement could be reached with the "clients" on a uniform template for requests.

Another possible improvement is the creation of an IT portal for entering requests for security verifications.

State Security also strives for better alignment of screenings with the needs of "clients". For example, consultations were held with the public prosecutor's offices in Antwerp and Liège with the aim of finding out how to better determine which intelligence is relevant for procedures to acquire nationality.

Lastly, a handbook is also being developed, formalising the internal procedures to be followed during screenings.

The Standing Committee I considered it advisable to also develop these initiatives for other beneficiaries.[18] State Security saw a crucial role for the National Security Authority (NSA) in implementing such improvement initiatives.

I.1.2.6. Special attention

The investigation again showed there is no active, systematic follow-up over time of the situation of a person for whom a screening was conducted. This implies risks, not least for the service that requested the screening and might have employed someone based on a favourable assessment. For example, an access badge to an

---

17 Royal Decree of 8 May 2018 determining the amounts of fees due for the security clearances, security certificates and security advice issued by the National Security Authority and for the security certificates issued by the Federal Agency for Nuclear Control as well as the distribution formulas referred to in Art. 22septies, sixth and eighth paragraphs, of the Act of 11 December 1998 on classification and on security clearances, certificates and advice (*Belgian Official Journal* 1 June 2018).

18 The Standing Committee I pointed out that the various regulatory provisions allowing screenings include elements specifying which information is relevant when assessing a person's reliability for the relevant authorisation, permit, function, and so on. Better knowledge of these regulatory provisions is therefore crucial to provide various clients with the correct information.

airport's grounds is issued for five years, which is a relatively long period. During this five-year period, a new verification will be done only if the person concerned moves to a new position.

There is also a process aspect to this: because of the structure of State Security's database, the SVS is not automatically notified of new negative information about someone who has previously been the subject of a security verification.[19]

I.1.3. SECURITY SCREENINGS AT GISS

I.1.3.1. Organisation[20]

The Screenings Unit, established in 2015[21], is formally located in GISS's structure under the hierarchical responsibility of the head of the Collection Coordination & Information Requirement Management (CCIRM), which was responsible at the time for registering and assigning all incoming and outgoing information. The unit consists of only a few non-commissioned officers (NCOs) and is in an ambiguous situation: after all, the employees' administrative manager was the head of the S(ecurity) Directorate and their functional manager was the head of the CCIRM. They did not have a designated contact in the hierarchy if they had questions or problems or for when a decision was needed.

The Screenings Unit operated very autonomously; there was no supervision of its operations from the hierarchy and the unit received no or hardly any instructions from above. This ambiguous situation also raised questions about final responsibility within GISS and the internal quality control.

There were insufficient employees to perform the tasks. An ever-increasing number of verification requests has led to a backlog of cases. Although the organisational table (OT) made provision for reinforcements, these have not yet materialised. These plans were moreover made only to tackle the existing workload and did not anticipate an expected ever-growing workload.

As already mentioned, the Screenings Unit's operations in GISS have evolved rather "organically", with no clear guidelines from the hierarchy. The employees never received specific training in legal aspects or in using the available technical

---

19 A flagging system can be helpful here.

20 The investigation was based on the period January to April 2018 and did not take account of the Defence Intelligence and Security Coordination Centre (DISCC) established within GISS's structure. This DISCC was given extensive powers. Among other things, it became the single point of entry and exit, registering all incoming and outgoing information of GISS and assigning it to the appropriate Directorate. Since June 2018, the Screening Unit has been administratively and functionally accountable to the Head of the DISCC. The DISCC combines the CCIRM, the CTR (GISS's communication centre) and a central secretariat.

21 Before May 2015, an employee of the Database Unit, a section that is part of the Support to Operations pillar of the CI Directorate (Counterintelligence) handled screenings for GISS.

resources. They have learnt how to perform their tasks on the job and from daily practice.

Lastly, the Committee found no centralised registration and management of verification requests and the responses to them by GISS. This meant no later monitoring was possible, which implied risks, not least for the service that requested the screening and might have employed someone based on a favourable screening.

I.1.3.2. Quantitative data

The Standing Committee I found that GISS does not keep comprehensive statistics on the security verifications and screenings it conducts. This means that no opinion can be formed about the service's core results or what resources it needs to successfully complete its assignment. Without insight into the results and required resources, strategy development and good planning are problematic.

Following the review investigation and the request for figures, the Screening Unit took the initiative of requesting statistics from the J6 Staff Service (ICT). This resulted in some figures on the number of searches carried out using one search method in one GISS database, namely the CI Directorate's database. The number of searches would roughly correspond to the number of entities to be verified. This figure was inexplicably high compared to State Security's figures.

When the Screening Unit was established, the number of requests to be processed was quite manageable, but there has been an ever-increasing rise in requests since the end of 2016. This has led to a backlog in processing the requests and to certain types of screenings being ignored. The Screening Unit decided itself which screenings to prioritise at its own discretion.

I.1.3.3. Work processes

All types of screenings

Requests for screenings arrive at the Screening Unit through various channels: the classified network (through the CCIRM), through other services (e.g. the S Directorate) or through the unclassified network (directly from the "client").[22]

This unit's role is limited to checking whether an entity (person) is known in GISS's databases. It does this initially by carrying out a search using a search programme. If no information is available on the person concerned, the service sends a 'nothing significant to report' (NSTR) reply directly to the requesting authority/client. A positive hit specifies the directorate at which and the database in which the information on the entity is available. The unit can then perform an

[22] The Screenings Unit proposed (to the CCIRM) to simplify this process and to ensure that all requests be submitted to it through one and the same route, i.e. through the CCIRM.

additional search in the relevant database. However, for a substantive overview of the available information, the Screenings Unit approaches the competent analysis service that entered the information into the database, which then processes it further. If worrying information comes to light during a security verification, the analysis services transmits it by memorandum, depending on the case, to either the National Security Authority or the Federal Agency for Nuclear Control (FANC). If less serious information is involved, it is transferred to the oral consultation unit at the NSA.

According to GISS's analysis services, they are aware that the information they communicate about an individual can have far-reaching consequences for that person. They say they are careful when providing information. The service states that the information provided relates, in principle, only to the individual who is the subject of the verification or screening. In certain cases, pertinent information about the person's immediate environment will also be given to provide context. However, no uniform criteria have been established at the analytical services as to which information is communicated and in what form.[23] The decision whether to disclose certain information depends on the individual analyst's judgement.

Excluding candidate military personnel

The above procedure is applied to all types of screenings except one. If a verification is part of a security advice for candidate military personnel, the "client" is a service within the Ministry of Defence itself, namely the Directorate-General for Human Resources (DG HR). In this case, it is the Security Clearances Service of GISS's S(ecurity) Directorate that coordinates formulating the security advice, and also makes inquiries for this purpose at State Security and the Federal Police.

The Screening Unit receives the request for these security verifications – as lists of names – both directly from DG HR and through the Security Clearances Service. The Unit proceeds with the verifications in the databases only once the Security Clearances Service has given its authorisation. Any hits are communicated to this Security Clearances Service. When GISS acts as the security authority itself, the head of GISS delegates the decision-making power in this regard to the head of the S(ecurity) Directorate.

Except for offences related to possessing, using and trafficking drugs, GISS has not formally defined any criteria for determining the basis on which candidate military personnel receive a positive or negative advice. In practice, it considers whether the offences are serious, and whether the person was a minor or an adult

[23] It was suggested that criteria should be defined jointly with the other services involved, including State Security, the Federal Police and CUTA. This applies all the more because the February 2018 legislation also provided for the services to prepare threat assessments as part of security verifications.

when these offences were committed. Another criterion is how recent any offences are.

If negative information exists about candidate military personnel, the head of the S Directorate and two other officers of the Security Clearances Service ultimately make a collegial decision.[24]

No legal basis

The investigation showed that the Screenings Unit is also frequently asked to conduct screenings without a clear legal basis. These includes requests from CUTA, the DJSOC Terro Service of the Federal Police, the External Relations Office (ERO) of GISS itself (e.g. regarding foreign Defence attachés stationed in Belgium), the Financial Intelligence Processing Unit (FIPU), NATO Office of Security (NOS), Europol/Interpol, and so on.

The question of who in GISS decides which type of searches the Screenings Unit must perform in the databases was not answered satisfactorily. In most cases, the CCIRM simply forwards these incoming messages to the Screenings Unit for processing. The legal basis of the request for information is not verified.

The Screenings Unit members appeared to have limited knowledge of the legal basis of their work. GISS hierarchy or legal service also does not systematically keep the Unit informed of legal amendments and/or new developments that relate to performing its duties or of protocol agreements concluded with partners. The Unit has to search for this information on its own.

Although the Unit systematically receives the Appeal Body's decisions, it does not process them. In other words, these decisions are not analysed. The Unit does not consider this to be its task.[25]

With the DISCC's establishment in mind (see below), an exercise to reflect on how the Screening Unit could function better in the future was initiated. This was aimed at refining the working procedures in use, which would also be outlined at a later stage.

I.1.3.4. Resources

Previous review investigations by the Standing Committee I into the functioning of GISS have shown that it uses different databases. The S(ecurity) Directorate alone used at least five different databases. And the other directorates (I, CI) each had their

[24] A negative decision is made in around 5% of cases. There are also an estimated 15% of "doubtful cases" in which negative information about the candidate exists but they are still admitted as military personnel. The security officer of the future unit is asked to pay increased attention to this person for the first months after their assignment to the unit.

[25] Even though the Screenings Unit has already raised the fact with the hierarchy that the Appeal Body's decisions only reach it, and it does not (or cannot) use them, no action has been taken in this regard.

own databases. This made the Screenings Unit's work time-consuming and very difficult to coordinate the screenings assignment centrally. The Screenings Unit had to use multiple search tools for each verification. In this context, the Committee also pointed out the weakness it found in this regard in an earlier investigation[26], which revealed the service concerned had delayed entering relevant information in the database. The risk also arose here that certain existing, relevant information – in this case, the most up-to-date information – was not found during screening, with possible consequences both for the person concerned and for the service that requested the screening. This also did not help with the service's reliability towards its partners.

Besides the lack of personnel, the Screenings Unit's employees cited the lack of high-performance technical resources as the main obstacle to performing their work. The Screenings Unit could use a new search engine, which would allow searches both in the databases and directly in documents in the I Directorate's directory structure. This was part of improving GISS's overall information management.

The Screenings Unit members were unaware of any initiatives with external partners for using common technological resources. As for external databases, the Screenings Unit has access only to the National Register, and then for one employee only. The Screenings Unit does not believe other accesses to external databases are necessary.

Another problem is that requests arrive at the Screenings Unit in all kinds of formats (Excel lists, PDF documents, and so on). In other words, there is no standardised template in use for security verification requests.

I.2. EXAMINING THE FUNCTIONING OF THE HUMINT DEPARTMENT AT THE MILITARY INTELLIGENCE SERVICE

Human intelligence (HUMINT) is an essential tool for intelligence and security services in their information gathering. The HUMINT Department of the Intelligence Division (I/H Department) is tasked with establishing networks of sources and informants that enable GISS to gather intelligence on foreign phenomena.

The Committee previously dealt with a specific complaint concerning how this department functions, more specifically about how certain assignments are performed abroad.[27] After all, the I/H Department has informants abroad to

---

26 *'Review investigation into how GISS's Counterintelligence (CI) Directorate operates'*.

27 The complaint was simultaneously the subject of a review investigation and a judicial enquiry by the federal public prosecutor's office. See STANDING COMMITTEE I, *Activity Report 2017*, 12-19 ('A complaint about three GISS operations').

gather information about matters of interest to the military intelligence service. Several dysfunctional aspects were identified in this regard. The description of assignments, the strategic management, the skills and quality of personnel and tradecraft, among other things, were critically examined.[28]

Following that complaint inquiry, the Standing Committee I decided at the end of April 2018 to open a review investigation into the functioning of the I/H Department. The report was completed in November 2019.

I.2.1. HUMAN INTELLIGENCE

Article 18 of the Intelligence Services Act stipulates that '*the intelligence and security services may call upon human intelligence to gather information on events, subjects, groups and natural or legal persons who are of demonstrable importance for the execution of their assignments in accordance with the guidelines.*[29] Information supplied to an intelligence and security service, regardless of the means of communication, and which does not fall within the scope of other articles of the Intelligence Services Act[30], will be considered human intelligence. This includes individuals with very different profiles, who may be seen once for a debriefing, sporadically or on a very regular basis, for short or long periods, regardless of their information position and the sensitivity of the information they convey. Reliance on these sources is a general method of data collection.[31]

NATO, for its part, defined HUMINT as '*a category of intelligence derived from information collected and provided by human sources*'.[32] NATO divides HUMINT into three categories.[33] HUMINT is classified as 'open' if the intelligence collection is carried out through sources that do not hide their true role. If the intelligence collection is carried out through human intelligence sources that hide their true function and purpose, the HUMINT is considered 'discreet'. Lastly, HUMINT is classified as 'clandestine' for activities carried out in secret, especially to protect sources.

---

28 The I/H Department was also mentioned in the investigation into the functioning of the Counterintelligence Directorate (I.6): it was clear that there was at least a risk that the two services would work in parallel to each other because of a lack of clear agreements and guidelines.

29 In March 2019, the National Security Council (NSC) validated the draft directive that State Security and GISS had jointly proposed. Because of this validation, the handling of human intelligence now has a full legal framework, consisting of four levels: the Organic Act, the National Strategic Intelligence Plan (NSIP), the NSC's directive and internal instructions.

30 Such as, for example, Article 14 of the Intelligence Services Act which stipulates that the services can call on the judicial authorities, civil servants and agents of the public services for the purpose of their intelligence assignment.

31 Based on the principles of subsidiarity and proportionality, this means that this method must take precedence over the specific or exceptional methods (known as the special intelligence methods or SIMs).

32 NATO, *Glossary of terms and definitions (AAP-6)*, ed. 2015.

33 NATO, *Allied Joint Publication (AJP) 2.3. and STANAG 2578*.

I.2.2. EXAMINATION OF THE I/H DEPARTMENT OF GISS

I.2.2.1 Collection body with a staff shortage

The I/H Department – which has no monopoly on human intelligence management within the military intelligence service – represents only a small proportion of the total staff of the Intelligence Directorate. Besides a high staff turnover (rotation), the Committee was able to identify a 25% net staff loss (outflow) for 2017-18. The Committee pointed out several risks relating to discontinuity and loss of knowledge because of the rotation and outflow of staff at the I/H Department. In January 2019, the Standing Committee I noted that the I/H Department was facing a 22% staff shortage compared to the organisational table (OT). In other words, the personnel situation is precarious.

Even so, the I/H Department has developed a network of hundreds of human intelligence sources distributed worldwide. About half of these sources provide intelligence on only one or two countries; on average, one source provides intelligence on five countries.

I.2.2.2 Management from various levels

For HUMINT activities abroad, the National Strategic Intelligence Plan provides that GISS, like State Security, must draw up lists of the countries in which they are active in relation to HUMINT.[34] The same plan also determines how their source management must be communicated.

GISS's Intelligence Directorate draws up an Intelligence Steering Plan, in turn, every three years. This plan must manage the intelligence cycle and is updated every year.[35] Specific actions and priorities for collection and analysis are determined for the departments on this basis, including the I/H Department. An 'Intel Focus' containing operational objectives is also drawn up.

Lastly, each collection body in the field, including the I/H Department, is requested to complete collection plans (known as Intelligence Collection Plans or ICPs). The ICPs for the I/H Department contain concrete questions for the sources through which information can be collected about various threats. The Committee noted that the ICPs contained many different specific themes, which is not illogical given the diversity of geopolitical contexts. However, the ICPs of the Intelligence Directorate's other collection bodies are not structured in the same way and the

---

34 Based on these lists, four categories of countries are drawn up: countries of interest only to GISS, countries of interest only to State Security, countries of interest to both, and non-priority countries.

35 The Committee could identify few differences between the 'Intelligence Steering Plan 2013-2014' and the 'Intelligence Steering Plan 2015-2018'. Only a few strategic objectives were prioritised differently because of the altered geopolitical context.

periods covered by the plans were not systematically specified. The Committee felt that standardisation and synchronisation of collection plans, and the avoidance of conflicts in source management by the various services, were in order.

The review of the sources further showed that the I/H Department did not align fully with certain strategic objectives as defined in the Intelligence Steering Plan. Information was also collected about certain countries, even though they are not directly and immediately of strategic importance to Belgian national defence from the outset. According to GISS, this finding must be viewed in light of the overall functioning of the Intelligence Directorate and GISS. The I/H Department provides only part of the information for each of the relevant countries. Information that is not a priority for Belgian interests may moreover be of particular interest to a partner intelligence service and thus feed the international exchange of information. While it may be more difficult for Belgium to recruit and manage sources for a country of interest, it can enjoy the reciprocity of international exchange.[36]

I.2.2.3. Reliability of the source and credibility of the information provided

Managing human intelligence is an essential task of the I/H Department. It is a series of processes which involves 'spotting', approaching and evaluating sources (recruitment), then processing their intelligence and ultimately 'archiving' the sources. Most of these processes are subject to internal guidelines. However, in 2018, the new management decided to completely revise the internal guidelines. The Committee found that no guidelines existed yet for certain processes (e.g. archiving).

The reliability of the source and the credibility of the information obtained should obviously be evaluated periodically. NATO's system for evaluating the sources and information it collects is structured as follows:

Reliability of the source		**Credibility of the information**	
A	Completely reliable	1	Confirmed by other sources
B	Usually reliable	2	Probably true
C	Fairly reliable	3	Possibly true
D	Not usually reliable	4	Doubtful
E	Unreliable	5	Improbable
F	Reliability cannot be judged	6	Truth cannot be judged

[36] After all, recruiting and managing a source is a multi-year investment. A source in a country that is of limited strategic importance today may prove to be crucial in the future.

The Standing Committee I established at the start of its investigation that the reliability of a significant proportion of the sources had not been determined.[37] During the investigation, the I/H Department successfully initiated a process to rectify this situation: all sources were evaluated and, if necessary, reoriented, reactivated or archived.

The information obtained from human intelligence must also be evaluated. Several thousand information bulletins were produced in two years (2017–2018).[38] The Committee found that the analysis services gave no formal feedback for most of the information bulletins. This was a disturbing finding for the intelligence cycle; after all, it is crucial for the analysis services to be able to guide the collection services towards achieving the intelligence objectives.

I.2.2.4. Management of source files

Source files are managed administratively on 'paper' and electronically. Because of the investigation, it was possible to identify problems with administrative management and to define corrective measures to remedy the identified shortcomings. However, the Committee found documents were still missing (e.g. documents relating to the 'request to approach a source', the 'approach phase report' or the 'recruitment report') from a series of files.

I.3. INTERNATIONAL EXCHANGE OF INFORMATION ON FOREIGN TERRORIST FIGHTERS

I.3.1. CONTEXTUALISATION

As early as 2016, during an international meeting with various European review bodies[39], it was decided to open a similar review investigation in all participating countries into the international cooperation between the various intelligence

---

37 The reliability of the source is not determined based only on their past performance. They do not in themselves influence the credibility of the information. An 'unreliable source' can provide information that is judged to be excellent in terms of credibility. However, the reliability of sources in general will influence the choices made for the purpose of the collection plan. This requires feedback between the analyst and the person collecting the information, to then be able to evaluate the source.

38 Analysing the content of those intelligence bulletins and evaluating their relevance to strategic objectives were not part of the investigation.

39 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, *Activiteitenverslag 2015* (Activity Report 2015), 80-81.

services with regard to the fight against foreign terrorist fighters (FTFs[40]). The intention was for every review body to study this topic from its own perspective and authority but based on the same philosophy and with a certain common approach.

The aim of the Belgian part of the investigation was to obtain the most clear and comprehensive insight 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 FTFs.

The ultimate aim was to assess the exchange of information and, if necessary, to make recommendations to optimise this in order to improve the information position of the services involved, without compromising the fundamental rights of citizens.

The Committee's own investigation was suspended. This was partly because of other urgent assignments – especially after the terrorist attacks in France and Belgium – but also because of the interaction with the international project. As a result, the Standing Committee I decided in January 2019 to conclude the investigation with a concise final report and not with the usual extensive report with descriptions, conclusions and recommendations.

I.3.2. RESULTS OF THE INVESTIGATION

First, the investigation showed that the international exchange of information on foreign terrorist fighters between intelligence services had not only increased significantly from 2015 onwards, but had also changed in nature. While the exchange of information was mainly reactive and bilateral before the FTF issue, the proactive and multilateral exchange gained more and more ground. One example of this is the cooperation in the Counter Terrorist Group (CTG).[41] After the Paris attacks in 2016 and under Dutch chairmanship, a permanent operational platform (formally opened in early 2017) and a common database were established in the CTG to exchange information on confirmed and suspected jihadists. This development also meant implementing the 'need to share' principle at international level between the countries concerned. The importance of this cannot be underestimated as the cooperation in the CTG can form the basis for general and structural cooperation among European intelligence services.

---

40 As defined in UN Resolution 2178 of 24 September 2014: '*Individuals who travel to a State other than their State of residence or nationality for the purpose of perpetration, planning or preparation of, or participating in, terrorist acts or the providing or receiving of terrorist training, including in connection with armed conflict*'.

41 The CTG was established after 9/11, is a specialised group and is an informal consultative body of mostly EU countries.

The mainly military intelligence services have also established a multilateral platform to coordinate their SIGINT activities and analyses.

The messages exchanged, which the Committee examined on a sample basis, showed that these communications were relevant, proportionate and in accordance with the services' statutory duties, but occurred outside the context of international institutions (EU, UN, and so on) or of formal, legally binding agreements (such as treaties). But the Committee found there was a long delay in implementing the National Security Council's directive of September 2016 concerning relations with foreign intelligence services.[42] This directive implements Article 20 of the Intelligence Services Act, which further regulates international cooperation with foreign services.

Lastly, reference was made to the increasingly complex regulations, specifically at international level and the rulings of international courts (soft law), but also at national level. Among other things, it must be investigated which collection methods are compatible with national law or international treaties, and developments in personal data protection should be strictly monitored.

I.4 INFORMATION POSITION OF THE INTELLIGENCE SERVICES CONCERNING THE PAKISTANI NUCLEAR SCIENTIST KHAN

In mid-January 2018, an article appeared in the press[43] about the North Korean nuclear programme. Reference was made, among other things, to the Pakistani nuclear weapons programme and the late Professor Martin Brabers (KU Leuven) as well as Abdul Qadir Khan, the Pakistani scientist who lived in Belgium in the late 1960s and early 1970s and is regarded as the father of the Pakistani atomic bomb.

One of the questions raised was whether the Belgian intelligence services had monitored this issue at the time. The Monitoring Committee of the Chamber of Representatives commissioned a study of the issue. In early July, the '*review investigation into the information position of the intelligence services concerning a Pakistani scientist who was active in Belgian academic circles, and the high-tech*

---

42 On 26 September 2016, the Ministers of Justice and National Defence presented the 'Directive on the relationships between Belgian intelligence services and foreign intelligence services' classified as 'Confidential Act 11.12.1998' in a memorandum to the National Security Council. However, the forwarding of information/personal data to foreign services was only dealt with very briefly in this directive.

43 M. RABAEY, *De Morgen*, 13 January 2018 ('De Belgische bommen van Kim Jong-un'). The article makes frequent reference to Luc BARBÉ (L. BARBÉ, *België en de bom. De rol van België in de proliferatie van kernwapens* [Belgium and the bomb. Belgium's role in the proliferation of nuclear weapons], June 2012), which calls for a wide-ranging independent scientific inquiry within academic circles and at State Security about the nuclear sector in Belgium.

knowledge he acquired of weapons of mass destruction which were ultimately used to develop nuclear weapons in Pakistan' was initiated.[44]

I.4.1. THE BELGIAN PART OF THE KAHN CASE

Abdul Qadir Khan played an important role in expanding Pakistan's nuclear programme. He studied and worked in Europe between 1961 and 1975, where he acquired a great deal of knowledge that may later have been used in the developing Pakistan's atomic bomb. Although Khan lived mainly in the Netherlands[45], he studied in Belgium from 1968, where he obtained his PhD in Physics from KU Leuven in 1972, supervised by Prof. Brabers.[46]

The review investigation focused on the Belgian part of the Khan case and whether the Belgian intelligence services had paid attention to his presence in Belgium during that period, and to the possible threats that he could have represented concerning the distribution of technology used to develop weapons of mass destruction.

I.4.2. INFORMATION POSITION OF THE INTELLIGENCE SERVICES

As far as State Security is concerned, Khan and the persons or entities associated with him were monitored both because of the threat of proliferation and espionage. To the extent that nuclear technology would or could be used for producing and proliferating nuclear weapons, the military intelligence service also had an adequate ground of jurisdiction to monitor this problem when the offences occurred. The Standing Committee I was therefore able to conclude that both State Security

---

44 The investigation was completed at the beginning of 2019.

45 In 1980, an investigative report on the Khan affair was drawn up in the Dutch Chamber of Representatives (*'De Zaak KHAN*, Chamber of Representatives 1979-1980, Special Ter Beek Committee, Parliamentary Paper number 16082'). In 1983, Khan was convicted in the Netherlands for espionage (for offences dating back to 1974 and 1975), but he was acquitted on appeal in 1985.

46 A great deal of national and international literature has already appeared about the subject(s) concerned (L. BARBÉ, *op. cit,* 2012; F. DOUGLAS and C. COLLINS, *The Nuclear Jihadist* New York, Twelve, 2007; C. COLLINS and F. DOUGLAS, *De Khan-code. Spionage, falende inlichtingendiensten en de handel in atoomgeheimen*, [Espionage, failing intelligence services and trade in atomic secrets], Balans, 2011; etc.).

and GISS were competent to monitor the issue – even before the 1998 Act was enacted.[47]

I.4.2.1. State Security

From 1979 to 1996 (and thus after Khan's departure from Belgium), State Security collected around 100 documents on Khan and Prof. Brabers, mainly from open sources. The service also received more than 50 documents from its correspondents. State Security prepared about 40 reports, in addition to 20 memoranda for Belgian or foreign correspondents.

Around 20 investigation reports (IRs) were drawn up after 1996 (and thus after State Security became computerised).

The investigation found a clear increase in the exchange of information as from 2004. These were information reports drawn up by State Security's external services. It is important to note that these reports focused on the proliferation issue in Pakistan and that Khan was of course also prominently mentioned. Some 20 memoranda were sent to federal and/or regional political authorities; several summary memoranda were addressed to State Security's management.[48]

State Security reported that there was no evidence that Prof. Brabers played a role in Khan's procurement network or actively contributed towards developing Pakistan's atomic bomb. However, there was no active and regular review of Prof. Brabers' activities or contacts.

I.4.2.2. GISS

GISS had no specific information in its various databases about Pakistani nuclear scientist Khan or Prof. Brabers for the 1960s and 70s. The service said it detected a lot of results for the name Khan in the period that followed. However, it did not include these results in its answer because they did not relate to the period when Khan was working in Europe.

---

47 In the preparatory works for enacting the Act of 30 November 1998 and more specifically in the discussions about the range of duties of the intelligence services and their role in the context of the scientific and economic potential (SEP), explicit reference was also made to the Khan case: '*... Economic and scientific espionage is evolving. Although the intention is not to serve a company, one must know the elements that play a role in its activity and, above all, who could hinder this activity abroad (see Pakistani trainees - Mr Khan's competence in the civil use of nuclear materials [emphasis added]). Knowing the scientific and economic potential in depth and supporting its development can therefore be very useful. This is certainly the most modern aspect of the intelligence services' current functions' (free translation)*. In: Bill governing the intelligence and security services, *Parl. Doc.* Senate 199798, no. 1-758/10, 101.

48 Only a few memoranda were communicated to foreign correspondents during the last ten years. State Security pointed out that this is consistent with the reduced importance of Khan and his (former) procurement network.

I.4.3. CONCLUSIONS

The 'Belgian part' of the Kahn case occurred from 1968 to 1972. At the time, although not always explicitly, both intelligence services had a general assignment concerning this matter.

Whether the Belgian services had a direct reason to monitor Khan is another question. After all, his stay in Belgium was relatively short. Apparently he did not stand out and he was not the only Pakistani student working in the field of nuclear technology. The field in which he conducted his research (metallurgy) was also not directly linked to nuclear research. Khan gained most of his knowledge in the Netherlands (from 1972), when he started working in a research laboratory there after completing his PhD. The Dutch investigation (above) showed that was also where he misappropriated data. The Dutch partner service did not inform State Security until 1979, when Kahn had already been away from Belgium for seven years, that they had been monitoring him.

The Dutch Prof. Brabers, who taught at Tilburg University as well as KU Leuven, only came to State Security's attention in 1987. No charges of aiding proliferation or espionage have ever been raised or substantiated against him.

Given the available information or indications, the Standing Committee I's opinion was that neither Kahn nor Prof. Brabers need have attracted the immediate attention of the Belgian intelligence services or should have been considered an important, let alone priority, target. It could be argued in hindsight that everyone involved in nuclear research was certainly worthy of the intelligence services' attention. As State Security reported, more attention was paid to this issue from the 1980s.

As a final assessment, the Standing Committee I stated that the fact that the Belgian intelligence services had not monitored Khan during his stay in Belgium or Prof. Brabers as a priority was not unreasonable, given the time frame and the data known at the time.

I.5. PUIGDEMONT AND POSSIBLE ACTIVITIES BY FOREIGN INTELLIGENCE SERVICES IN BELGIUM

I.5.1. CONTEXTUALISATION

On 27 October 2017, Carles Puigdemont, the president of Catalonia's regional government, who caused the Catalan Parliament to declare independence, was stripped of his office by the Spanish institutions. He then fled to Belgium. At the beginning of November 2017, a European arrest warrant for him was issued by the Spanish judicial authorities.

On 9 February 2018, Puigdemont filed a complaint with the Belgian authorities concerning violation of his privacy, following the discovery a few days earlier of a hidden tracking beacon under his vehicle.[49] After they had found the device, Puigdemont's advisers informed the Waterloo local police zone. According to open sources, Puigdemont's drivers had noticed prior to the discovery of the geolocation beacon that they were being watched. Cars with German number plates had been noticed shadowing them.

At its meeting of 12 June 2018, the Monitoring Committee asked the Standing Committee I to open a review investigation into the information position and the Belgian intelligence services' reaction to any activities of foreign intelligence services on Belgian territory during Puigdemont's stay in Belgium.

I.5.2. LEGAL ASPECTS

Under Article 7, 1 and Article 8, paragraph 1, 1, g) of the Intelligence Services Act, State Security is tasked with collecting, analysing and processing intelligence relating to any activity that threatens or could threaten the external security of the State and international relations; activities resulting from espionage (collecting or providing information not accessible to the public [...]) or interference (the attempt to use illegal, fraudulent or clandestine means to influence decision-making processes).

In addition, under Article 7, 1 and Article 8, paragraph 1, 2, a) and b) of the Intelligence Services Act, State Security is tasked in particular with collecting, analysing and processing intelligence relating to any activity that threatens or could threaten the internal security of the State and maintenance of democratic and constitutional order; activities resulting from violations of human rights and fundamental freedoms, or offences against the safety and physical and moral integrity of persons and the protection of property.

Moreover, under Article 7, 3/1 and Article 11, § 1, 5 of the Intelligence Services Act, State Security has been tasked since January 2016 with collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory. The same duty was added for GISS in 2016 (Article 11, § 1, 5 of the Intelligence Services Act). This is a general power which, when being exercised, must not involve a threat.

For the purpose of organising how the duties of collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory are to be divided, Article 20, § 4 of the Intelligence Services Act

---

[49] See open sources: Y.N. with Belga, *La Libre Belgique*, 28 March 2018 ('Carles Puigdemont porte plainte en Belgique: sa voiture était pistée avec des balises de traçage'). Including the following: '*The former Catalan president's security personnel inspected the vehicle and found a tracking device attached to its underside*' *(free translation).*

stipulates that State Security and GISS are to conclude a cooperation agreement based on directives from the National Security Council (NSC). The Standing Committee I is unaware of any directive of the National Security Council or of a cooperation agreement concluded pursuant to this decision (or of any such draft).[50]

As for communicating data to foreign intelligence and security services, Article 19 of the Intelligence Services Act states: '*the intelligence and security services communicate the intelligence referred to in Article 13, paragraph 2 only to the relevant Ministers and to the relevant judicial and administrative authorities, to the police services and to any competent bodies and persons in accordance with the objectives of their assignments and to bodies and persons who are the subject of a [threat] as referred to in Articles 7 and 11*'. (free translation) The preparatory work for Article 19 of the Intelligence Services Act[51] mentions the possibility of communicating information to foreign intelligence and security services.

In the same context, Article 20, § 1 of the Intelligence Services Act states that the Belgian intelligence services must also ensure effective cooperation with foreign intelligence and security services.

Under Article 20, paragraph 3 of the same Act, the terms of this cooperation must be laid down in a National Security Council directive. On 26 September 2016, the Ministers of Justice and Defence submitted such a memorandum to the National Security Council.

To fully outline the legal framework (but considering that these decisions had not yet entered into force in October 2017), it is necessary to refer to Articles 92–94 of the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data. These articles provide specific arrangements for the handling of personal data by intelligence and security services, including the communication of data to countries that are not EU Member States or to international organisations.

I.5.3. FINDINGS

As regards the authority of the Belgian intelligence and security services

The Strategic Intelligence Plan approved by the National Security Council does not mention the division of tasks between State Security and GISS for monitoring foreign intelligence and security services in Belgian territory. And the two services also did not conclude an agreement under Article 20, § 4 of the Intelligence Services Act.

---

50 The Strategic Intelligence Plan, approved by the National Security Council in 2018, addresses this specific issue only briefly (using a table). Both services have the authority to act.

51 *Parl. Doc.* Chamber of Representatives, 1995-96, no. 49-638/1, 19.

Although State Security contended that it had no authority, the Committee pointed out that State Security and GISS have been tasked with collecting, analysing and processing intelligence relating to the activities of foreign intelligence services in Belgian territory since January 2016. The Standing Committee I was of the opinion that State Security's legal analysis needed adjusting to comply with the provisions of Article 20, § 4 of the Intelligence Services Act.

The Standing Committee I questioned GISS about its information position on Carles Puigdemont. Did this service take certain actions in connection with his stay in Belgium and/or did it cooperate in an operation carried out by the foreign partner service A? GISS replied that it did not have any information on Puigdemont, that it had not cooperated with the foreign partner service A in connection with Puigdemont's stay in Belgium, and that since he did not pose a threat to Belgian interests or NATO, the service had not undertaken any activities against him. Considering its specific authority linked to a threat of a 'military' nature, GISS, as far as it was concerned – and rightly so – had no reason to show interest in the Puigdemont case.

As regards the evaluation of the risk linked to any development of intelligence activities and of interference by one or more foreign intelligence or security services

Considering the aim of the investigation, the Standing Committee I found that State Security was wrong not to collect, analyse and process information on the exercise of certain activities in Belgian territory by a foreign intelligence and security service relating to Carles Puigdemont's stay in Belgium, between 2017 and the end of the review investigation.

State Security was not requested to provide technical assistance to analyse the locator beacons.

With a risk that was classified as unlikely and the 'level 1' threat assessment prepared by CUTA, Puigdemont was not the subject of operations by either GISS or State Security. In this context, the Standing Committee I found that the various files relating to CUTA's threat assessment of Puigdemont's presence made no reference to any risk linked to possible intelligence activities or interference by one or more foreign intelligence or security services. Although this risk does not fall under CUTA's authority, it is up to the Standing Committee I to at least check the presence or absence of such a reference linked to the risk.

When asked about its own evaluation methodology regarding the stated threat (or absence of it), State Security stated it has since adopted the 'lead phase investigative model' methodology. This must allow the service to decide whether it needs to open a file and/or take measures after a risk analysis to determine the credibility, possible actions to be taken and the proportionality. This methodology will be the subject of monitoring at State Security and will also be proposed to GISS.

The Standing Committee I concluded that the presence of such a personality in Belgian territory required a specific formal analysis and evaluation by the services of State Security, in light of the specific threats falling within its authority, and thus not merely in light of threat assessments drawn up by CUTA, which do not have the same purpose.

As regards the exchange of information

State Security disclosed personal data (even though these came mainly from open sources and/or were not confidential) to a foreign European intelligence service classified as a 'reliable' partner.[52]

State Security did in fact receive requests for information from the foreign partner service A about Puigdemont's whereabouts. In response, State Security provided answers based on open sources and unclassified police information. State Security did not question the partner service A about the immediate reason for these requests and did not weigh up the interests of the service against the interests of the persons concerned (e.g. the fundamental right to privacy or the right to association). For the Standing Committee I, this case shows the importance of clear rules on exchanging information between Belgian and foreign intelligence services.

The Committee also regretted the fact that the competent minister was not informed of the foreign partner service A's request.

As regards the formal consultation arrangements between the Belgian intelligence services and foreign intelligence and security services

The Standing Committee I found that no formal consultation arrangements were made between the Belgian intelligence services and one or more foreign intelligence services or security services regarding Carles Puigdemont. Although the foreign partner service A initiated informal contacts, State Security did not follow up on them. The Standing Committee I refrained from commenting on this part.

As regards State Security's response to the foreign partner service A and the foreign police service

The Standing Committee I noted that the Director-General temporarily froze bilateral cooperation with the foreign partner service A – which had addressed certain grievances to State Security – at some point. Relations between State

[52] Although the National Security Council's directive is dated September 2016, State Security already carried out an analysis (taking account of the principles set out in a draft directive that it had prepared itself) of its relations with the foreign partner service A on 25 November 2015. This service was classified as a reliable partner. GISS had not yet implemented this directive.

Security and the foreign partner service A were normalised shortly afterwards, following a meeting between the two heads of service. But the file did not show that the competent minister had been informed about the temporary freezing of this relationship.

After discovering the beacons, State Security wrongly considered that the police information – which stated that a foreign police force was monitoring the Puigdemont case and asking Belgian police certain questions about his movements – did not constitute a threat in relation to the exercise of intelligence activities by foreign intelligence or security services in Belgian territory. The Committee was also of the opinion that the information, claiming that a foreign police force was monitoring Carles Puigdemont's case, merited a formal analysis and specific evaluation by the services within State Security.

I.6. FUNCTIONING OF THE COUNTERINTELLIGENCE (CI) DIRECTORATE OF GISS FOLLOWING-UP THE RECOMMENDATIONS

I.6.1. CONTEXT AND PURPOSE

Under Article 32 of the Review Act, the Minister of Defence asked the Standing Committee I at the end of December 2016 to conduct an investigation into how the Counterintelligence (CI) Directorate (one of the four directorates of GISS at that time) operates. The immediate reason for this was a letter from a large number of CI personnel, expressing their concerns about how the service operated and the circumstances under which they had to perform their statutory duties.

The Standing Committee I opened its review investigation in January 2017[53]; it was completed in February 2018.[54] The investigation provided an insight into the seriousness, complexity and multifaceted nature of the shortcomings within the CI Directorate. The Committee stated first and foremost that national security requires a strong and reliable military intelligence service. That is also why the Committee was convinced that the Directorate CI had an interest in an organisation and management that meets the standards of an effective and efficient public service. The investigation showed that these standards were not being met.

---

53 The Committee conducted a similar audit on a previous occasion: STANDING COMMITTEE I, *Activity Report 2011*, 7-14 ('II.1. Audit of the military intelligence service') and 104-107 ('IX.2.1. Recommendations with regard to the audit of GISS').

54 STANDING COMMITTEE I, *Activity Report 2018*, 2-17 ('I.1. Operations of the Counterintelligence (CI) Directorate of GISS').

The investigation into the functioning of the CI Directorate gave rise to extensive recommendations.[55] With regard to the implementation dates, priorities were specified ranging from 'very high' (to be done by the end of 2018), to 'high' (to be done by the end of June 2019) to 'moderate' (to be done by the end of December 2019).

By the end of January 2019, the Standing Committee I had already opened a follow-up investigation looking at the extent to which all the recommendations formulated in the above audit had been implemented. At the end of February 2019, the Standing Committee I was invited by its Parliamentary Monitoring Committee to exchange views on this issue. This was done in preparation for the hearing[56] behind closed doors with the Head of GISS, the Chief of Defence and the then Minister of Defence, since it appeared that the problems in the military intelligence service were dragging on.

I.6.2. LAUNCH OF A BUSINESS PROCESS RE-ENGINEERING (BPR)

In response to the CI Directorate's audit, the Head of GISS decided to launch a Business Process Re-engineering (BPR) in early June 2018.[57] This management technique had to allow a fundamental restructuring of business processes. Besides its effect on the organisational structure, this methodology aims to change the management style and organisational culture. The strategic option was taken to place the reflection on the responses to the recommendations concerning the functioning of the CI Directorate within a broader exercise concerning the entire functioning of GISS. After all, GISS command also wanted to consider the conclusions formulated by the Parliamentary Inquiry Committee on 'terrorist attacks'. Although the Committee believed this would make the CI Directorate's reform process more onerous, it was considered a valid choice.

However, a conflict arose between GISS command and the head of the CI Directorate at the end of October 2018. The proposals developed in response to

---

55 STANDING COMMITTEE I, *Activity Report 2018*, 128-132 ('XII.2.1. Various recommendations for GISS arising from the review investigation into how the Counterintelligence Directorate operates').

56 Special Committee tasked with the parliamentary monitoring of the Standing Committees P and I, Exchange of views with Lieutenant-General Claude Van de Voorde, Head of GISS, General Marc Compernol, Chief of Defence, and the Deputy Prime Minister and Minister of Foreign Affairs and European Affairs, and of Defence, tasked with Beliris and the Federal Cultural Institutions, on the situation at GISS's Counterintelligence (CI) Directorate, 18 March 2019 (meeting behind closed doors).

57 A core team, consisting of the Deputy Assistant Chief of Staff, the Civilian and Military Advisors of GISS command, two representatives of the staff services, and the heads of GISS's five directorates at the time (CI, I, S, Cy, ERO and DISCC), was created to steer this BPR in the right direction.

the recommendations in the CI 2018 audit report could not be integrated further in the BPR. This gave rise to a situation in which synchronisation between the two improvement processes was lost (October 2018 – January 2019). At the start of February 2019, CI's command was taken over and it aimed to follow the general BPR process again.

I.6.3. IMPLEMENTING THE RECOMMENDATIONS OF THE 2018 AUDIT: STATE OF AFFAIRS

Based on documentary research, interviews and other material, the Committee tried to form a picture of how much significant progress had been made with the recommendations. Its investigation showed that by the start of March 2019, significant progress had been made in one-third of the recommendations classified as very high priority; progress was visible but insufficient to fully restore operability for half of the recommendations; some recommendations had not been implemented at all.

The Committee found that:

- the CI Directorate's role in the fight against terrorism was clarified: State Security takes the lead in terrorism of a 'civilian' nature. Personnel and resources were transferred to a common CounterTerro platform at State Security under a protocol. A 'horizontal' CounterTerro coordinator (from CI) was appointed at GISS. Their task was incorporated in the DISCC to improve intra-GISS cooperation;
- the CI directorate's very precarious situation in terms of infrastructure was resolved; in March 2019, the service was able to move into a renovated building equipped with all the necessary security features;
- better coordination was established between the CI Directorate and the 'J6' staff department, GISS's ICT manager. A clear point of contact was established and the ICT needs were inventoried;
- conceptual work was done on mission and vision, even though this still had to be validated and finally formalised. Once done, intelligence requirements and intelligence collection plans can be drawn up at all levels;
- in terms of the organisation chart and determination of resource needs (personnel), there were proposals, which also still had to be validated and formalised (scheduled for the second quarter of 2019);
- steps have also been taken regarding the cooperation between the analysis and collection services; the situation in which there were collectors for certain subject areas but no analysts, or vice versa, must thus be a thing of the past.

However, it is important to note that the CI Directorate has little or no control itself over some recommendations to move the matter forward (and neither does GISS sometimes) and that the solution lies mainly in the hands of other echelons (e.g. creating an 'intelligence' specialisation).

The Standing Committee I undertook to continue closely monitoring the implementation of the recommendations.

I.7. REVIEW INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2019 AND INVESTIGATIONS OPENED IN 2019

I.7.1. 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 insights possible of the terrorist or extremist threat in or against Belgium so as to allow them to respond appropriately. Its core task is to make ad hoc or strategic assessments. This task is entrusted to analysts and experts (seconded from the 'supporting services') (Article 2, 2. of the Threat Assessment Act). Those supporting services, which are CUTA's most important source of information, include very diverse, each with their own culture and size.

In 2010, the Standing Committees I and P carried out a joint review investigation into the information flows between CUTA and the ingervices, paying particular attention to the two intelligence services and the federal and local police.[58]

At the joint plenary meeting in December 2017, it was decided to open a review investigation into the 'other' supporting services, namely the Immigration Service (Home Affairs FPS), the Mobility FPS, the Foreign Affairs FPS and the Customs and Excise Administration (Finance FPS). With this joint investigation, the Standing Committees I and P wanted to draw up a *status quaestionis* of the information flows between CUTA and the other supporting services.

In the course of 2019, various investigative actions were carried out. The report was finalised at the end of 2019. The Parliamentary Monitoring Committee, which took note of the report in 2020, immediately requested a follow-up investigation and an expansion of the scope to include the supporting services added in 2018 – the Governmental Coordination and Crisis Centre (Home Affairs FPS), the Directorate-General of Penal Institutions (Justice FPS), the Department of Worship

[58] In this regard, see STANDING COMMITTEE I, *Activity Report 2010*, 52 ('II.12.6. Communication of information to CUTA by the supporting services), and, in more detail, *Activity Report 2011*, 117-125 ('II.4. Information flows between CUTA and its supporting services').

and Secularism (Justice FPS) and the General Administration of the Treasury (Finance FPS).[59]

I.7.2. APPLICATION OF NEW (INCLUDING SPECIAL) INTELLIGENCE METHODS

The entry into force of the Act governing the intelligence gathering methods used by the intelligence and security services (SIM Act) in 2010 significantly expanded GISS's and State Security's opportunities to collect information. Since then, the services have been able to use ordinary, specific and exceptional methods. The classification reflects the degree of intrusiveness of the measures.[60] Given the legislative amendments in the meantime, the scope of some methods has been modified – i.e. expanded – some 'special' methods have become 'ordinary' methods and new ordinary methods have been added.

The Committee has recently been given a number of monitoring options for some 'ordinary' methods, although these are regulated differently for almost every method. These include monitoring the identification of telecommunication users (Article 16/2 of the Intelligence Services Act), access to PNR data (Article 16/3 of the Intelligence Services Act), access to police camera images (Article 16/4 of the Intelligence Services Act), or the monitoring before interceptions, penetrations in a computer system and the recording of moving images (Article 44/3 of the Intelligence Services Act).

The Committee has decided to examine this issue in its review investigation opened in 2019 into '*the intelligence services' application of and internal controls over the use of methods and instruments recently introduced or adapted by Parliament with respect to which the Standing Committee I has been allocated a special supervisory role.*' This investigation is to be completed in the second half of 2020.

---

59 Royal Decree of 17 August 2018 implementing Article 2, first paragraph, 2, g) of the Threat Assessment Act of 10 July 2006, *Belgian Official Journal* 12 September 2018.

60 But the logic and classification of the methods is under pressure. In this regard, see: W. VAN LAETHEM, *Enkele reflecties over tien jaar BIM-controle door het Vast Comité I* [Some reflections on ten years of SIM monitoring by the Standing Committee I], in J. VANDERBORGHT, (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers* [Special intelligence methods in the spotlight], Antwerp, Intersentia, 2020, 70 *et seq*.

I.7.3. BREXIT AND THE RELATIONSHIP BETWEEN THE BELGIAN AND BRITISH INTELLIGENCE SERVICES

In June 2016, the United Kingdom held a referendum on leaving the European Union. A small majority voted to leave and protracted exit negotiations began some time later. The United Kingdom finally left the European Union on 31 January 2020.

This process – which commonly became known as Brexit – raised certain questions about the possible consequences of the British withdrawal from the European Union in terms of cooperation between the two Belgian (and other European) intelligence services and the three British (civilian) intelligence services: the British Security Service (BSS, also known as MI5), the Secret Intelligence Service (SIS, also known as MI6) and the Government Communications Headquarters (GCHQ).

In May 2019, the Standing Committee I opened a review investigation into the effects of Brexit on cooperation between the Belgian (State Security and GISS) and the British intelligence services. In particular, the Committee wanted to consider whether there was a risk of Brexit jeopardising this cooperation. The way in which the Belgian intelligence services prepared for Brexit was also discussed.

Because of the conflicting and unclear situation in the UK, there was no certainty about the timing or the exact circumstances of the exit when the review investigation was carried out (October – November 2019).[61] The Committee paid attention to the legal basis for international cooperation, tested several hypotheses about the impact of the Brexit, and studied the Belgian intelligence services' assessment of the consequences of the Brexit. The report was completed in the first quarter of 2020.

I.7.4. THE POSSIBLE INTERFERENCE OF FOREIGN SERVICES/ STATES IN BELGIAN ELECTIONS

Although the results of the investigation into this interference were not made public fully in the United States, there are strong suspicions that foreign services/ States (specifically Russia) attempted to influence the 2016 US presidential election through cyber resources. This is also conceivable in Europe, and thus in Belgium.

[61] Several scenarios remained possible for a long time: Brexit based on the agreement negotiated in October 2019 between the EU and the UK government, Brexit based on an agreement yet to be amended, Brexit without an agreement (no-deal Brexit), or even the cancellation of Brexit after possible elections (or a new referendum) in the United Kingdom.

In view of the elections on 26 May 2019, this was a particularly topical theme.[62] Holding open and fair elections goes to the core of democracy. State Security is tasked with identifying certain threats against the Belgian institutions and informing the competent authorities accordingly. For example, reference can be made in this case to 'interference' as a threat (Article 8, paragraph 2, g) of the Intelligence Services Act), i.e. '*the attempt to influence decision-making processes by illegal, fraudulent or clandestine means*'. Interference can take various forms: not only disinformation and targeted publicity through social media, but also outright cyberattacks. But there are also points of departure in this for GISS, whose authority in this matter is less evident at first sight.

At the start of 2019, the Committee therefore decided to open an review investigation[63] into how the Belgian intelligence services react (by collecting intelligence, issuing warnings, cooperating internationally, possibly disruption[64], and so on) to possible interference by foreign services/States in Belgian elections. The investigative questions were as follows:

- How can the threat be characterised (what forms does it take and what instruments are used) and what are the recent precedents?
- What is the legal context (both for the actions of the Belgian services and the possible aspects of international law)?
- Which different actors are involved in this issue in Belgium (intelligence services, CUTA, Cybersecurity Centre, and so on) and how is their authority divided?

The investigative report was completed at the beginning of 2020.

62 In mid-October 2018, a high-level conference on this theme was held in the run-up to the May 2019 European elections under the auspices of the EU by the European Political Strategy Center ('Election Interference in the Digital age : building resilience to cyber-enabled Threats'). See https://eceuropa.eu/epsc/events/election-interference-digital-age-building-resilience-cyber-enabled-threats-en

63 Full description: 'Review investigation into how the intelligence services monitor possible interference by foreign services in Belgian elections, try to counter any threats, report on this to the authorities, and in particular on the danger of cyber interference or cyber attacks in this area'.

64 State Security also sees disruption as part of its remit. Disruption means that an intelligence service not only discreetly performs intelligence operations, but possibly also tries to actively counter the threats it detects through different means (e.g. by making them public; cf. the Dutch General Intelligence and Security Service's reaction after it emerged that the Russian GRU had tried to hack an international institution in The Hague).

I.7.5. MONITORING OF RIGHT-WING EXTREMISM BY THE TWO INTELLIGENCE SERVICES

Various sources indicate that far-right groups and movements have a firm foothold in Europe and are expanding their influence. In recent years, several attacks and actual and planned acts of violence have also been attributed to right-wing extremists. Events like these have also occurred in Belgium. In May 2019, the Standing Committee I therefore decided to open a review investigation into how the intelligence services monitor the threat from the phenomenon of right-wing extremism in Belgium today and report on it to the authorities. The Committee wished to investigate whether and how the intelligence services are fulfilling their statutory duty to monitor extremism, and more specifically right-wing extremism, in Belgium. The investigative questions were defined as follows:

- How do the intelligence services define the phenomenon of right-wing extremism: do State Security and GISS use a definition to delineate right-wing extremism and focus their attention on it? Do the Belgian intelligence and security services use a common definition within the framework of the Radicalism Plan? Do these definitions fit in the legal context?
- What is the legal context? What are the instructions of the competent ministers, the National Security Council or other bodies?
- Can the intelligence services contextualise and quantify the phenomenon? What form does right-wing extremism take in Belgium and where?
- How do the services monitor the phenomenon? How is it determined which groups and situations to actively monitor? How are the services organised to perform this monitoring? What priorities have been set? What resources (personnel, techniques, and so on) and methods (ordinary methods, special intelligence methods, and so on) are used? What estimates are made (analysis), how are these reported to the authorities, and what feedback is given on this?

In the course of 2019, various investigative actions were undertaken. The investigation will be continued in 2020.

I.7.6. INFORMATION AND COMMUNICATION TECHNOLOGY IN THE INTELLIGENCE PROCESS

Information and communication technology (ICT) play an increasingly important role in intelligence processes, both in collecting and analysing basic information and distributing intelligence. Information can come from human intelligence (HUMINT), from partners, or from digital sources such as open sources (OSINT),

interception operations (SIGINT), imagery (GEOINT), and so on. The constant growth of data flows requires appropriate systems capable of absorbing them and of enabling correct, quick and effective analysis. The IT environment must therefore be a stable and future-oriented tool that can support the different actors involved in the intelligence cycle. This environment – both hardware and software – must comply with the relevant standards and good ICT practices, while also taking account of new and future technological developments[65], such as big data.[66]

In previous investigations, the Standing Committee I found that the intelligence services are facing huge challenges in this area. The past has shown, particularly with regard to GISS, that ICT is a sore point. The Committee found that the intelligence activities were not (or no longer) sufficiently supported by ICT. The conditions for proper information management were not (or were no longer) being fully met.[67], [68]

In May 2019, the Standing Committee I informed the President of the Chamber of Representatives of the start of the 'Review investigation into the ICT resources used by the Belgian intelligence services to collect, analyse and communicate information as part of the intelligence cycle'. The scope of the investigation was clearly defined at the outset. The investigation focuses on the ICT resources used specifically to support the elements of the intelligence cycle. These include the systems used to collect data or specific analysis tools and databases.[69] The Standing Committee I does not investigate the generic/standard office automation facilities used by the services (e.g. Windows, Word, Excel, and so on), insofar as they are not specific to the intelligence services. Nor does the Committee conduct a detailed examination of the computer equipment (hardware) at the services' disposal, unless it is specific to the intelligence services. The investigation aims to identify the risks faced by the services and to reduce these risks through appropriate recommendations.

---

65 The oversight bodies also play an important role in this context. In this context, see: K. VIETH and T. WETZLING, *Data-driven Intelligence Oversight. Recommendations for a System Update*, StiftungNeueVerantwortung, November 2019, 63 p.

66 Big data refers to the science of collecting and analysing large volumes of data to try and discover certain interesting patterns based on a ranking ('clustering') and statistical analyses that can aid decision-making. These data are usually characterised by great variety, speed and volume.

67 STANDING COMMITTEE I, *Activity Report 2011*, 99-106 ('II.1. Audit of the military intelligence service'); *Activity Report 2018*, 2-17 ('I.1. Functioning of the Counterintelligence (CI) Directorate of GISS').

68 The Parliamentary Inquiry Committee's report on the attacks in Zaventem and Maelbeek also recommended improving the information management of the services to keep information overload ('infobesity') under control. See 'Parliamentary Inquiry Committee on the Terrorist Attacks of 22 March 2016. *Parl. Doc.* Chamber of Representatives, 2016-2017, no. 54-1752/008, 15 June 2017, p. 53 and 180 *et seq.*

69 At GISS, these are called 'weapon systems' – by analogy, for example, with systems integrated into the defence platforms at National Defence (e.g. the software for the radar systems or 'battle management').

A first module (GISS) was completed in mid-2020. The results of the investigation at State Security are expected at the start of 2021.

I.7.7. STATE SECURITY'S MONITORING OF RELEASED TERRORISM OFFENDERS

Some 400 people have been convicted of terrorist offences in Belgium since 2015.[70] As some of them were convicted by default, they could not be detained. Some of those convicted have meanwhile served their sentences in prison or have been released conditionally (before the end of their sentences) after a decision by the sentencing court.

A prisons computer system (SIDIS Suite[71]) ensures several authorities (State Security, Federal Police, and so on) are informed whenever a radicalised convict leaves prison. In mid-2019, the Committee decided to open a review investigation into '*how the Belgian intelligence and security services ensure the monitoring of (i) persons suspected of having committed terrorist offences in Belgium or elsewhere who benefit from a measure provided for in the Act of 20 July 1990 and (ii) of persons convicted of terrorist offences in Belgium who leave the Belgian prison under one of the measures provided for in the Act of 17 May 2006, or who are released permanently (Article 71 of this Act)*'.

I.7.8. RISK OF INFILTRATION AT THE TWO INTELLIGENCE SERVICES

In recent years, the international intelligence community has been shaken by several cases of infiltration (and insider threat). In 2019 the Committee took the initiative to start a review investigation into how the two intelligence agencies deal with the risk of infiltration: what risks are recognised and what countermeasures are taken to manage and to respond to them if they materialise.

---

70 Combined questions to the Minister for Justice on 'the release of terrorists' (Proceedings Chamber of Representatives 2019-20, 4 June 2020, CRIV55COM043, 16, Q. Nos 550000781P and 550000786P).

71 The SIDIS Suite database processes the data about individuals who have been given a prison sentence, are subject to a custody order pending trial or an involuntary commitment order and have therefore been sent to a prison, institution or a secure unit within a prison (for involuntary commitment) or a community institution for minors. SDIS Suite facilitates the necessary information exchange and data flows between the authorities.

Several working meetings were held with GISS and State Security on the subject of 'mapping and risk assessment of infiltration in the ranks of the intelligence services'. The risk management process as set out in ISO 31000 formed the starting point for this purpose.[72]

72 www.iso.org:fr/iso-31000-risk-management.html

CHAPTER II.

CONTROL OF SPECIAL AND CERTAIN ORDINARY INTELLIGENCE METHODS

This chapter includes statistics on State Security's and the General Intelligence and Security Service's (GISS) use of specific and exceptional methods (known as the 'special methods') and of the ordinary methods in which the Committee was assigned a specific role. It also describes the manner in which the Standing Committee I performed its jurisdictional control of these methods. Besides several figures on the number of decisions and how the referral was made to the Committee, the essence of the legal precedents of the Standing Committee I is also presented. The case law has been stripped of operational data; only those elements relevant to the legal issue are included.

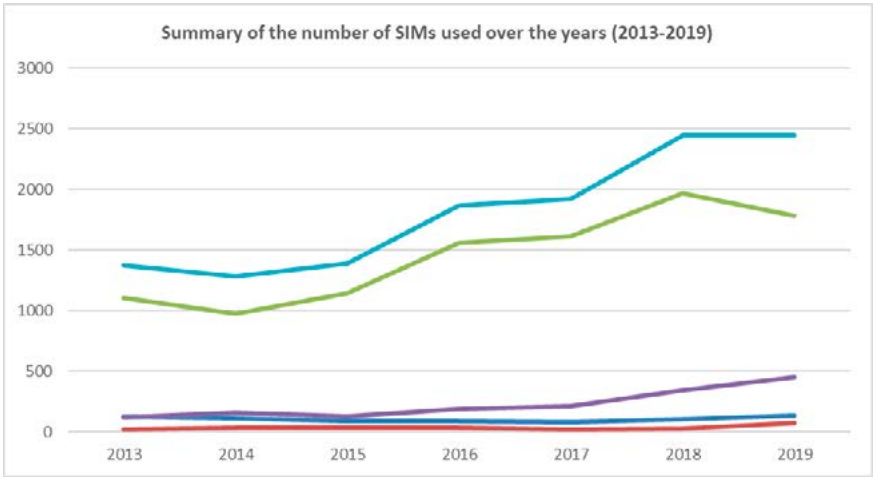
II.1. FIGURES ON SPECIFIC AND CERTAIN ORDINARY METHODS

Between 1 January and 31 December 2019, a combined total of 2,444 authorisations for the use of special intelligence methods were granted by the two intelligence services: 2230 by State Security (of which 1781 for specific methods and 449 for exceptional methods) and 214 by GISS (of which 138 for specific methods and 76 for exceptional methods).

The following table provides 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
2018	102	28	1,971	344	2,445
2019	138	76	1,781	449	2,444

This can be represented graphically as follows:



The blue line shows the evolution of the specific methods used by GISS over the years, whereas the green line shows the evolution the specific method used by State Security. The red line shows the evolution of the exceptional methods used by GISS, whereas the green line shows the evolution of the exceptional method used by State Security. Finally, the total is represented by the turquoise line.

After a constant increase in the number of SIMs used in recent years, a stagnation can be observed for the first time: the total number of methods used remained stable in 2019 compared to 2018. It is worth noting that for each authorised method, multiple targets (such as persons, organisations, places, subjects, means of communication, etc.) may be permitted.

State Security continues to account for the lion's share of the methods used (91.2%).

But if these figures are broken down, we can see an appreciable increase in both the specific (from 102 to 138) and exceptional (from 28 to more than double at 76) methods used at GISS. State Security recorded an appreciable increase in the number of exceptional methods used (from 344 to 449). Despite all these increases, an overall stagnation was observed because of a sharp drop in the number of specific methods used (from 1,971 to 1,781) in 2019. The Committee confines itself below to presenting raw statistics and refrains from commentary. The Committee intends to consult the relevant services in order to be able to interpret the figures presented responsibly.

Ordinary methods involving requests made to operators to identify certain means of communication recorded a decrease of approximately 12% compared to recent years (60 fewer requests by GISS compared to 2018, with more than 800 fewer requests by State Security).

	Requests by GISS	Requests by State Security
2016	216	2,203
2017	257	4,327
2018	502	6,482
2019	442	5,674

The Committee previously stated[73] that it could not *'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'*. Although the number of requests decreased in 2019, it remains quite a large number. The Committee investigated the reasons for this using its general powers of review; the results were included in its review investigation opened in 2019 into '*the intelligence services' application of and internal controls over the use of methods and instruments recently introduced or adapted by Parliament with respect to which the Standing Committee I has been allocated a special supervisory role*' (cf. I.7.2).

II.1.1. METHODS USED BY GISS

II.1.1.1. Ordinary methods

Identification of a telecommunication user

Identifying a telecommunications user (such as a mobile phone number or IP address) or a used means of communication is regarded as an ordinary method if it happens through a request or direct access to an operator's customer database.[74] The regulation imposes an obligation on State Security and GISS to keep a register of all requested identifications and of all identifications made through direct access. It has also been stipulated that the Committee should receive a monthly list of the identifications requested and of each instance of access. In practice, the Committee only received the number of requests every month.[75] This point also formed the subject of the review investigation opened in 2019 (see above).

---

73 STANDING COMMITTEE I, *Activity Report 2017*, 50-51.

74 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 using technical means – and thus not through a request to an operator – the collection remains a specific method (Art. 18/7 § 1 of the Intelligence Services Act).

75 This situation was regularised in the course of 2020.

Identification of a prepaid card holder

Just as when a telecommunications user or a used means of communication is identified, State Security and GISS must keep a register of all requested identifications of another ordinary method introduced since 2016. After all, Article 16/2 of the Intelligence Services Act stipulates: '§ 2. *For the purpose of performing their assignments, the intelligence and security services may request a bank or financial institution to cooperate in identifying the end user of the prepaid card referred to in Article 127 of the Act of 13 June 2005 on electronic communications, based on the reference of an electronic bank transaction that relates to the prepaid card and that is communicated in advance by an operator or provider pursuant to section 1*' (free translation). As in 2018, neither intelligence service made use of this.

Access to PNR data

In early 2017[76] the possibility for the intelligence services of accessing the information held by the Passenger Information Unit by means of targeted searches was introduced (Article 16/3 of the Intelligence Services Act and Article 27 of the PNR Act of 25 December 2016). The Committee will be informed of the use of this method and may prohibit it, where appropriate.[77]

The PNR rules also allow for a so-called 'prior assessment' to be carried out in which the entered PNR data is automatically checked against lists of names or databases of the intelligence services and in which information based on validated hits is forwarded (Article 24 of the PNR Act).

Use of police camera images

The Act of 21 March 2018 (*Belgian Official Journal* of 16 April 2018) amended the Act of 30 November 1998 governing the intelligence and security services so as to allow the intelligence services to use police camera images. A new general observation method was introduced to this end (Art. 16/4 of the Intelligence

76 Act of 25 December 2016 (*Belgian Official Journal* 25 January 2017).

77 Unlike for the methods included in Article 16/2 of the Intelligence Services Act, no provision was made for mandatory reporting to Parliament, as Article 35 § 2 of the Review Act was not amended. At the suggestion of the Monitoring Committee, the Committee decided to include these figures in its annual reporting and not to wait for a possible change in the law. The first two discontinuations were ordered only in 2020.

Services Act).[78] In the absence of an implementing decree, this provision has not yet entered into force.[79]

Figures

Ordinary methods (GISS)	Number of authorisations
Identification of a telecommunication user	442
Identification of a prepaid card holder	0
Targeted PNR data searches	18 in 2018, now 38
Referral of PNR data on basis of hits	Not provided
Use of police camera images	Not in force

II.1.1.2. Specific methods

The table below shows the figures for the use of specific methods by GISS. Seven specific methods are distinguished.

Specific methods (GISS)	Number of authorisations
Surveillance in places accessible to the public using technical means or surveillance in a place that is inaccessible to the public and not hidden from view whether or not using technical means (Art. 18/4 of the Intelligence Services Act)[80]	12
Searching of places accessible to the public using technical means, searching the content of locked objects or removing these objects (Art. 18/5 of the Intelligence Services Act)	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator (Art. 18/6 of the Intelligence Services Act)	0
Requesting transport and travel information from private transport and travel services (Art. 18/6/1 of the Intelligence Services Act)	0

78 The same Act expanded the existing specific and exceptional observation possibility (Articles 18/4 § 3 and 18/11 § 3 of the Intelligence Services Act).

79 At the beginning of 2019, the Council of Ministers approved a draft Royal Decree on this subject, which was submitted to the Standing Committee I for an advisory opinion. This opinion 002/VCI-BTA/2019 of 9 April 2019 can be consulted on the Committee's website (www.comiteri.be).

80 The Act of 21 March 2018 (*Belgian Official Journal* 16 April 2018) added a new paragraph to Article 18/4 of the Intelligence Services Act to allow the intelligence services to use police camera images to perform real-time observations. This method, which requires direct access to the information in question, has not yet been put into operation.

Identification using technical means of the electronic communication services and tools 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 method and the date of payment for the subscription or for the use of the electronic communications service (Art. 18/7 of the Intelligence Services Act)	0
Tracing the traffic data of electronic means of communication and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act)	63
Monitoring of localisation data for electronic communications and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act).	63
TOTAL	**138**

II.1.1.3. Exceptional methods

GISS can authorise various exceptional methods in connection with its duties referred to in Articles 11, § 1, 1° to 3° and 5°, and § 2 of the Intelligence Services Act:

Exceptional methods (GISS)	**Number of authorisations**
Surveillance, whether or not using technical means, 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 technical means, opening or removing an object (Art. 18/11of the Intelligence Services Act) [81]	3
Searching places that are inaccessible to the public, whether or not using technical means, as well as objects located there, whether or not locked (Art. 18/12 of the Intelligence Services Act)	3
Using a legal person as referred to in Art. 13/3 § 1 of the Intelligence Services Act to collect data (Art. 18/13 of the Intelligence Services Act)	0
Opening and inspecting post, whether or not entrusted to a postal operator (Art. 18/14 of the Intelligence Services Act)	2
Collecting data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act)	20
Penetrating a computer system (Art. 18/16 of the Intelligence Services Act)	8
Tapping, intercepting and recording communications (Art. 18/17 of the Intelligence Services Act)	40
TOTAL	**76**

[81] The Act of 21 March 2018 (*Belgian Official Journal* 16 April 2018) added a new paragraph to Article 18/11 of the Intelligence Services Act to allow the intelligence services to use police camera images to perform real-time observations. This method, which requires direct access to the information in question, has not yet been put into operation.

II.1.1.4. Interests and threats justifying the use of ordinary and special methods[82]

GISS may use specific and exceptional methods in respect of four of its roles, taking various threats into account.

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 assignments of the armed forces;
   - the safety and security of Belgian nationals abroad.
2. **Ensuring military security (Article 11, 2 of the Intelligence Services Act)**
   - the military security of personnel under the authority of 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 managed 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 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 fulfilment 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 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 on Belgian territory (Article 11, 5° of the Intelligence Services Act).**

82 Each authorisation may involve multiple interests and threats.

These methods can therefore not be used for security investigations or other assignments entrusted to GISS by special laws (e.g. performing security verifications for candidate military personnel). However, 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). Practice shows that various threats may be involved for each authorisation.

Two-thirds of the specific and exceptional methods are used by GISS in the context of the role of 'collecting, analysing and processing intelligence relating to the activities of foreign intelligence services on Belgian territory' (Article 11, 5° of the Intelligence Services Act). However, it cannot be inferred from this that since 2017 GISS has been monitoring a 'new type' of threat, as the monitoring of foreign services was more readily linked in the past to the intelligence role within the context of the fight against espionage.

NATURE OF THE THREAT	NUMBER IN 2019
Espionage	165
Terrorism (and radicalisation process)	6
Extremism	5
Interference	38
Criminal organisation	-
Other	-
Total	**214**

Unlike for the use of special methods, the Committee does not have any figures on the perceived threat and interests to be defended for ordinary methods as referred to in this chapter. In its previous activity report, the Committee recommended that the services also record this data and make it available.[83] As this has not yet happened, the Committee repeats its earlier recommendation in that regard.

II.1.2. METHODS USED BY STATE SECURITY

II.1.2.1. Ordinary methods

Ordinary methods (State Security)	Number of authorisations
Identification of a telecommunication user	5674
Identification of a prepaid card holder	0
Targeted PNR data searches	27
Referral of PNR data on basis of hits	Not provided
Use of police camera images	Not in force

83 STANDING COMMITTEE I, *Activity Report 2017*, 50-51.

As stated, the Committee will examine in more detail the way in which this method is used in its review investigation launched in 2019.

II.1.2.2. Specific methods

Specific methods (State Security)	Number of authorisations
Surveillance in places accessible to the public using technical means or surveillance in a place that is inaccessible to the public and not hidden from view whether or not using technical means (Art. 18/4 of the Intelligence Services Act)	311
Searching of places accessible to the public using technical means, searching the content of locked objects or removing these objects (Art. 18/5 of the Intelligence Services Act)	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator (Art. 18/6 of the Intelligence Services Act)	0
Requesting transport and travel information from private transport and travel services (Art. 18/6/1 of the Intelligence Services Act)	48
Identification using technical means of the electronic communication services and tools 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 method and the date of payment for the subscription or for the use of the electronic communications service (Art. 18/7 of the Intelligence Services Act)	50
Tracing the traffic data of electronic means of communication and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act)	700
Monitoring of localisation data for electronic communications and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act).	672
TOTAL	**1,781**

II.1.2.3. Exceptional methods

Exceptional methods (State Security)	Number of authorisations
Surveillance, whether or not using technical means, 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 technical means, opening or removing an object (Art. 18/11 of the Intelligence Services Act)	26
Searching places that are inaccessible to the public, whether or not using technical means, as well as objects located there, whether or not locked (Art. 18/12 of the Intelligence Services Act)	13
Using a legal person as referred to in Art. 13/3 § 1 of the Intelligence Services Act to collect data (Art. 18/13 of the Intelligence Services Act)	0
Opening and inspecting post, whether or not entrusted to a postal operator (Art. 18/14 of the Intelligence Services Act)	12
Collecting data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act)	95
Penetrating a computer system (Art. 18/16 of the Intelligence Services Act)	48
Tapping, intercepting and recording communications (Art. 18/17 of the Intelligence Services Act)	255
TOTAL	**449**

II.1.2.4. Interests and threats justifying the use of ordinary and 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 the context of all threats within its competence (Article 8 of the Intelligence Services Act). 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;
   Process of radicalisation: a process whereby an individual or a group of individuals is influenced in such a manner that this individual or group of individuals is mentally shaped or is prepared to commit terrorist acts;
3. Extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or intentions, whether 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, the following figures were recorded:

NATURE OF THE THREAT	NUMBER IN 2019
Espionage	777
Terrorism (and process of radicalisation)	1118
Extremism	291
Proliferation	2
Harmful sectarian organisations	0
Interference	87
Criminal organisations	0
Monitoring the activities of foreign services in Belgium	(included in above figures)
TOTAL	**2,230**

The above figures show that 'terrorism (and the process of radicalisation)' remains the absolute priority at State Security for the use of SIM methods in 2019.

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.

As at GISS, the State Security combines various interests. However, it can be confirmed that 'safeguarding the key elements of the scientific or economic potential' did not feature as an interest in the figures.

As stated (see II.1.1.4.), the Committee does not have any figures on the perceived threat and the interests to be defended in relation to the ordinary methods referred to in this chapter.

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

II.2.1. CONTROL OF CERTAIN ORDINARY INTELLIGENCE METHODS

The control of certain ordinary methods is settled differently for each of those methods.

Regarding the identification of a telecommunication user (or the identification of a prepaid card user), the law did not introduce any specific control. Article 16/2 § 4 of the Intelligence Services Act merely stipulates that the Committee must be provided with a monthly list of the requested identifications and of instances of direct access. As stated above, the Committee only receives the number of requests

in this context. The Committee had decided to carry out random checks on a number of requests every year.[84] This started in 2020. The Committee has therefore decided to include this issue in its review investigation opened in 2019 into '*the intelligence services' application of and internal controls over the use of methods and instruments recently introduced or adapted by Parliament with respect to which the Standing Committee I has been allocated a special supervisory role.*' (free translation).

With regard to access to PNR data held by the Passenger Information Unit, Article 16/3 of the Intelligence Services Act provides that such access may only be obtained after a decision by the head of service and '*provided that there is satisfactory justification*'. The Committee must be informed of this and '*prohibits the intelligence and security services from using data collected in circumstances that do not comply with the legal conditions*' (free translation). No such prohibition was issued by the Committee in 2019.

Finally, special control arrangements have been granted to the Committee in connection with the possibility for the intelligence services of accessing information from police camera images (Article 16/4 of the Intelligence Services Act): an *a priori* check[85] and an *a posteriori* check.[86] As the intelligence services were not yet able to use this method, the Committee did not have to take any action in this area.

II.2.2. CONTROL OF SPECIAL METHODS

II.2.2.1. Figures

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. 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

---

84 STANDING COMMITTEE I, *Activity Report 2017*, 33, footnote 41.

85 '*The assessment criteria referred to in the first paragraph, 2°, shall be submitted to the Standing Committee I in advance.*'

86 *'The Standing Committee I shall be informed of the duly justified decision of the head of service or his representative as soon as possible. The decision may concern a set of data relating to a specific intelligence investigation. In this case, a list of uses of targeted access shall be sent to the Standing Committee I once a month. The Standing Committee I shall prohibit the intelligence and security services from using data that was collected in circumstances that do not comply with the legal conditions.*' and '*any list on the basis of which the correlation referred to in the first paragraph, 1°, is carried out shall be communicated to the Standing Committee I as soon as possible. The Standing Committee I shall prohibit the intelligence and security services from using data that was collected in circumstances that do not comply with the legal conditions*' (free translation).

is prepared for the Standing Committee I, giving it a better insight into the use of these methods.[87]
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 Data Protection Authority;
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* of the Code of Criminal Procedure). In that case, the Committee gives its opinion on the legitimacy of the specific or exceptional methods that have produced intelligence in a criminal case. The decision to ask for an opinion rests with the investigating or criminal courts. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

METHOD OF REFERRAL	2013	2014	2015	2016	2017	2018	2019
1. At its own initiative	16	12	16	3	1	1	4
2. Data protection authority	0	0	0	0	0	0	0
3. Complaint	0	0	0	1	0	0	0
4. Suspension by SIM Commission	5	5	11	19	15	10	12
5. Authorisation by Minister	2	1	0	0	0	0	0
6. Pre-judicial consulting body	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**

The number of decisions taken by the Committee continues to fall, despite the significant increase (+ 27%) in the use of SIM methods. All but one of the referrals resulted from a suspension by the SIM Commission.

Once the referral has been made, the Committee may make various kinds of interim or final decisions.

87 The Committee also recommended in 2017 that GISS also hold 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). Since the end of January 2018 – in view of the infrequent use of SIM methods – there have been monthly meetings and (in principle) fortnightly reports.

1. Decision to declare the complaint 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 assignments of the intelligence service (Article 43/5, § 4, third paragraph of the Intelligence Services Act);
11. Discontinuation of a method if it is still in use or has been suspended by the SIM Commission and an order stating that the information obtained through this method may not be used and must be destroyed (Article 43/6, § 1, first paragraph of the Intelligence Services Act);
12. Partial discontinuation of an authorised method. This refers to a situation in which, for example, the use of a method is limited in time, and not to the situation in which several methods have been approved in a single authorisation by a head of service and the Committee discontinues only one of them.
13. Total or partial lifting of the suspension and ban imposed by the SIM Commission (Article 43/6, § 1, first paragraph of the Intelligence Services

Act). This means that the method authorised by the head of service was found to be (partially) 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. Opinion as a pre-judicial consulting body (Articles 131*bis*, 189*quater* and 279*bis* of the Code of Criminal Procedure).

NATURE OF THE DECISION	2014	2015	2016	2017	2018	2019
Decisions prior to the referral						
1. Complaint deemed null and void	0	0	0	0	0	0
2. Manifestly unfounded complaint	0	0	0	0	0	0
Interim decisions						
3. Suspension of method	3	2	1	0	0	0
4. Additional information from SIM Commission	0	0	0	0	0	0
5. Additional information from intelligence service	1	1	4	0	0	0
6. Investigation assignment of Investigation Service	54	48	60	35	52	52
7. Hearing of SIM Commission members	0	2	0	0	0	0
8. Hearing of intelligence service members	0	2	0	0	0	1
9. Decision regarding investigative secrecy	0	0	0	0	0	0
10. Sensitive information during hearing	0	0	0	0	0	0
Final decisions						
11. Discontinuation of method	3	3	6	9	4	11
12. Partial discontinuation of method	10	13	4	6	6	4
13. Lifting or partial lifting of ban imposed by SIM Commission	0	4	11	0	0	0
14. No legal competence	0	0	0	0	0	0
15. Lawful authorisation / No discontinuation of method / Unfounded	4	6	2	1	1	0
Pre-judicial opinion						
16. Pre-judicial opinion	0	0	0	0	0	0

II.2.2.2. Decisions

The final decisions delivered by the Standing Committee I in 2019 are briefly discussed below. The summaries have been stripped of all operational information. Only those elements with legal relevance have been included.

The decisions were divided into four categories:
– Legal or procedural requirements prior to the implementation of a method;
– Proportionality and subsidiarity;

- Legality of the method in terms of the applied techniques, data collected, duration of the measure, and nature of the threat;
- The legality of the implementation of a lawful method.

Legal or procedural requirements prior to the implementation of a method

Requests to foreign communication service providers

Dossier 2019/8254 concerned an intelligence service's request to a social media platform to access the content of two profiles' communications. Because the media platform concerned did not respond, the service sent a request to a foreign intelligence service asking it to contact the platform. The service's initiative related to an imminent threat; there was no discussion about that. Since the intelligence service considered this to be an ordinary method, no SIM decision was drawn up. Both the SIM Commission, which had been informed of the request to the foreign intelligence service through another case, and the Standing Committee I were of the opinion that this was an exceptional method. Because of the importance of this statement, the essence of the Committee's decision is reproduced at length: '*Whereas the Act of 13 June 2005 on electronic communications, and more specifically its Articles 9 and 122–127, lays down the procedures in which the police services and the intelligence and security services have access to electronic communications. The Royal Decree of 12 October 2010, and more specifically its Article 5, lays down the terms for requests concerning electronic communications by the intelligence and security services. Whereas the Court of Cassation's judgment of 1 December 2015 (Yahoo case, P.13.2082.N) confirms that a measure consisting of the obligation to provide requested data is adopted in Belgian territory with regard to any operator or provider whose economic activities are actively directed at consumers in Belgium. Whereas Article 3, 11/1 was moreover amended to that effect and the term 'communications service provider' was further defined. Whereas [...] is therefore subject to Belgian law and can be confronted by the [intelligence service concerned] under Belgian law. Whereas the [intelligence service concerned], in its request [...] to [...], repeated through its request [...] to the [foreign intelligence service], therefore had to comply with Belgian law. Whereas in this case, Article 18/17 of the Intelligence Services Act had to be observed. Indeed Article 18/17 and not Article 18/16 of the Intelligence Services Act applies, because Article 18/17 refers to 'intercepting communications' and 'examining them', while Article 18/16 refers to 'gaining access to a computer system' (...) Whereas the Standing Committee I also emphasises, contrary to what the [intelligence service concerned] maintains in its letter of [...] to the SIM Commission, that the inquiries at the [foreign intelligence service] cannot be regarded as an ordinary method. On the contrary, these inquiries must be seen as a second attempt (after the request to [...]) to obtain the content of the communication.*' (free translation).

Insufficient justification

In the context of a specific method suspended by the SIM Commission, the Committee requested additional information from the intelligence service. The intelligence service gave only a brief reply, citing, among other things, the third-party agency rule. However, it added that it accepted the SIM Commission's decision to suspend. The Committee found '*that under these circumstances, the intended method must be discontinued and all the intelligence obtained through the method must disappear*' (free translation) (dossier 2019/8418).

The lack of proper motivation of the decision was also an issue in another dossier. In dossier 2019/8768, the intelligence service wanted to obtain data on telephone communications of a certain person for twelve months prior to the date of the head of service's decision. But the Committee ruled that the reasons given in the SIM decision made it impossible *'to decide whether the applied SIM meets the legal requirements, in terms of the service's scope of competence and proportionality of the method*' (free translation). It moreover appeared that (free translations):

- *'the two threats to be monitored by law are not referred to anywhere in the SIM decision';*
- *'the actual activity that the service regards as a threat to be monitored and for which a specific method is requested, is not clearly or unambiguously defined, is not supported by facts and in certain respects exceeds the scope of competence of an intelligence service. It has not been sufficiently demonstrated whether and how the envisaged method can make a real contribution to some of the purposes assumed in the decision';*
- *'the Committee points out that "pacifism" in itself cannot constitute a threat to be monitored. After all, it is nothing more than a world view that seeks lasting peace and, from that perspective, is perfectly legitimate in a democratic society';*
- *'strictly speaking, the definition of extremism does not apply to GISS as it is included in Articles 7 and 8 of the Intelligence Services Act that apply only to State Security. However, since the application of the method described in Article 18/8 of the Intelligence Services Act requires a reference to one of the threats listed in Articles 7 and 8 of the Intelligence Services Act to justify the maximum duration of the method, this definition also applies to GISS';*
- *'it is also not clear from the facts reproduced in the SIM decision that the person concerned constitutes an extremist or other threat*'; '*the Standing Committee I refers to Article 2 § 1, paragraph 2 of the Intelligence Services Act: 'In the execution of their assignments these services are responsible for compliance with and contribute to the protection of individual rights and freedoms and to the democratic development of society.' In this context, the Committee stresses the importance of freedom of association and freedom of expression as fundamental values of our Western society. It points out that government interference in these rights and freedoms is possible in exceptional circumstances only. These*

circumstances are by no means evident from this case file. From this perspective, the wording used, the reasoning by which an even more uncertain hypothesis is built from very uncertain facts (if A were true – but there are almost no indications of this – then B might be possible...) and the unsubstantiated suspicions and doom scenarios (even using the term terrorism) are unacceptable.';

– *'lastly, the SIM decision mentions the purpose of the method in some places even though this purpose cannot be demonstrably achieved through the envisaged methods.'*

The Committee intervened at its own initiative and asked several additional questions of the intelligence service concerned. The following decision of the Committee was taken in the 2020 operating year.

Difference between the period in the draft authorisation and in the final authorisation

The SIM Commission gave its assent to a draft authorisation to use an exceptional method for '*a period of two weeks, starting from my authorisation*' (free translation). However, the final authorisation refers to a period of two months. The SIM Commission suspended the authorisation beyond the two weeks from the date of the head of service's authorisation. The Standing Committee I agreed with that suspension (dossier 2019/8421).

Failure to notify the SIM Commission in time

An intelligence service wished to extend an ongoing method in two cases (dossiers 2019/8788 and 2019/8968). But the SIM Commission was informed of the extension only a few days after the expiry of the initial decision. The new method therefore was not covered by a valid decision in the interim period. After all, *'the extension of the method could start only from the moment notice was served'*. In dossier 2019/8788, the intelligence service itself kept these unlawfully obtained data '*in quarantine*'. But the Committee stressed that '*the fact that the data is "quarantined" and not available for use does not change the relevant statutory provisions. Whereas the SIM Commission therefore issued a ban on the use of the data under Article 18/3 § 6 of the Intelligence Services Act.*' (free translation).

Proportionality and subsidiarity[88]

An intelligence service wished to access call and localisation data of three targets' means of communication (dossier 2019/8150). For one of them, this did not

[88] However, there was one case that did not give rise to a jurisdictional decision, in which the emphasis was placed on the principle of subsidiarity.

present a problem: '*whereas with regard to the main target in this case, the head of service's decision is sufficiently justified and the measure is proportionate to the threat*' (free translation). But this was not the case for the other two people. They turned out to be relatives of the first target who did not even reside at the same address. Moreover, there was no evidence that these people were involved in their family member's activities, nor that the target would use their means of communication. '*Whereas the mere fact that there is a family relationship between these persons is insufficient to justify an intrusion into their private lives*' (free translation). The method was therefore unlawful.

When an intelligence service wanted to observe a location where an extremist meeting would be held on a specific day for two months, first the SIM Commission and then the Standing Committee I intervene: '*Whereas the decision on the specific method is disproportionate because it does not mention how the observation can be carried out for two months, while the alleged threat refers to an event with a fixed date, on one day*' (free translation). The measure taken was not disproportionate for the day of the meeting itself: '*Whereas the decision was motivated by the need to identify persons from [an extremist group] who would participate in a meeting, the place and date of which were mentioned, and during which [extremist] speakers would take the floor; the information cannot be collected by an ordinary method, the use of technical resources is justified because of the difficulty of observing the envisaged place*' (free translation) (dossier 2019/8224). The conclusion therefore was that the method was legal only on the day of the meeting.

As part of controlling a specific method, the SIM Commission requested more information about the stated threat of espionage and the alleged link between the target and that possible threat (dossier 2019/8377). When the service replied that it did not have the requested information, the SIM Commission suspended the method. At the request of the Standing Committee I '*to further substantiate certain aspects of the specific method because how the decision was substantiated did not allow for confirmation that the method complied with the legal requirements of legality, proportionality and subsidiarity*' (free translation), the intelligence service concerned also essentially repeated what had been included in the original authorisation. The service itself acknowledged that the few additional details '*do not remedy the inadequate proportionality*' and that it readily accepted the suspension by the SIM Commission. The Committee therefore found that the method was not lawfully authorised.

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

Unclear subject

The intelligence service concerned wanted to observe several targets of foreign origin in '*places not accessible to the public and not hidden from view*', without entering these places (Article 18/4 § 2 of the Intelligence Services Act). The intention was to use technical resources for this purpose. The case involved (mobile) cameras and CCTV, while the head of the service's decision mentioned the installation of a beacon. In addition, only the car of one target was known. The SIM Commission asked for further clarification from the service concerned. It was still not sufficiently clear which vehicles the beacons would be placed on. Placing a beacon under the vehicles of the other targets was therefore ordered to stop (dossier 2019/8109).

An exceptional rather than a specific method

An intelligence service requested the technical cooperation of an operator to obtain call-associated data of a certain person through a specific method. However, the Standing Committee I noted that the operator could not retrieve that data through its own files, but only through a file located at the person concerned: *'Considering that the data [...] are available only by penetrating the computer system in which they are stored, namely [at] the person who is the subject of special intelligence methods. Considering that such penetration is an exceptional intelligence method provided for in Article 18/16 of the Intelligence Services Act'* (free translation). The method was therefore destroyed (dossier 2019/8446).

Diplomatic immunities

The method envisaged in dossier 2019/8483 consisted of listening to communications for two months from the date of the head of service's authorisation (and after the Commission's assent). However, the method turned out to involve telephone numbers registered in the name of a permanent mission at an international institution based in Belgium.

The protection offered under the Vienna Convention on Diplomatic Relations of 18 April 1961 did not apply in this case. After all, this treaty deals with traditional diplomatic bilateral missions. But the international institution is subject to its own rules that oblige Belgium to respect the customary diplomatic immunities. These rules refer to the immunities and privileges under the Vienna Convention.

The intelligence service thought it need not take this into account because only the target used the numbers to which it wanted to apply a method. But an initial

analysis showed that the numbers were shared with people other than the target. '*Whereas the circumstances and factual account communicated through the draft authorisation to the SIM Commission [...] therefore do not correspond to reality*' (free translation). The service itself found that the conditions referred to in the assent were therefore no longer met and decided to discontinue the method. The Committee therefore stated '*that the intended method must thus be discontinued and all the intelligence obtained through the method must disappear*' (free translation).

Calculating the period 'prior to the decision'

An intelligence service decided to trace electronic means of communications and locate electronic communications for the twelve-month period preceding the decision (dossier 2019/8794). This decision was taken on day 29 of month X. The Committee stated that '*the "period prior to the decision" in this case must necessarily be between 28 X 2018 and 29 X 2019.*' (free translation). However, the service had requested data for the period from 20 X 2018 to 19 X 2019. '*It must thus be established that data was wrongly requested from 20 X 2018 to 27 X 2018, which is not in accordance with Article 18/8 § 2 of the Intelligence Services Act*' (free translation).

The same problem arose in dossier 2019/9024. *'In this case, the methods used to trace and locate electronic communications establish a potential threat linked to terrorism; Whereas in relation to a potential threat of terrorism, and under the cited article, the head of a service can request the tracing and locating of electronic communications for twelve months prior to the decision only; That the term prior to the decision must be understood to exclude the date of the decision from the calculation of the period referred to by law; That the decision in question was dated 18 X 2019, and the collection of data therefore could not exceed a period of twelve months prior to the date of the decision; That in this case, the maximum period of retroactive data collection extends only to 17 X 2018*' (free translation).

The legality of the implementation of a lawful method

Implementing a specific method prior to notifying the SIM Commission

In dossier 2019/9097, the intelligence service sent its request to the operator the day before the SIM Commission was notified. This 'substitution *[...] does not respect the conditions set out in Article 18/3, § 1 of the Intelligence Services Act; That consequently, the request addressed to the operator at 16:49 on 4 X 2019 and the results obtained on this basis must be considered as having been illegally obtained*' (free translation).

II.3. CONCLUSIONS

The Standing Committee I has formulated the following general conclusions:

- Between 1 January and 31 December 2019, a combined total of 2,444 authorisations for the use of special intelligence methods were granted by the two intelligence services: 2230 by State Security (of which 1781 for specific methods and 449 for exceptional methods) and 214 by GISS (of which 138 for specific methods and 76 for exceptional methods). After a constant increase in the number of SIMs used in recent years, a stagnation can be observed for the first time.
- State Security continues to account for the lion's share of the methods used (91.2%).
- If the overall figures are broken down, we can see an appreciable increase in both the specific (from 102 to 138) and exceptional (from 28 to more than double at 76) methods used at GISS. State Security recorded an appreciable increase in the number of exceptional methods used (from 344 to 449). Despite all these increases, an overall stagnation was observed because of a sharp drop in the number of specific methods used (from 1971 to 1781) by State Security.
- Ordinary methods involving requests made to operators to identify certain means of communication recorded a decrease of approximately 12% compared to recent years.
- In the use of SIM methods, GISS focused as always more on the threat of 'espionage', followed by 'interference'; for State Security, the nature of the threat was primarily 'terrorism (and the process of radicalisation)', followed by 'espionage'.
- Referrals were made to the Committee in sixteen dossiers, four of which were on its own initiative and twelve by operation of law after the SIM Commission had suspended a specific or exceptional method on grounds of illegality (Article 43/4 of the Intelligence Services Act). Illegalities included insufficient justification, failure to notify the SIM Commission in time, an unclear subject, or when the collection period was too long.

CHAPTER III.

MONITORING OF FOREIGN INTERCEPTIONS, IMAGE RECORDINGS AND IT INTRUSIONS

III.1. POWERS OF GISS AND MONITORING ROLE OF THE STANDING COMMITTEE I[89]

As early as 2017, the powers of GISS in connection with security interceptions were extended.[90] Since then, interceptions have been possible for communications '*transmitted or received abroad*'. This possibility applies to almost all GISS roles. It is also significant that the descriptions of GISS roles themselves were also made broader in scope. The legislator simultaneously introduced two other methods, namely 'intrusion of an IT system' (Article 44/1 of the Intelligence Services Act) and the 'capture of moving images' (Article 44/2 of the Intelligence Services Act). The way in which the Committee can monitor these methods also changed.

The review *prior* to interceptions, intrusions or image capture is done on the basis of lists drawn up annually.[91] This means that as well as in addition to an annual interception plan, a intrusion and image plan must also be drawn up by GISS.[92]

---

89 See Articles 44 to 44/5 of the Intelligence Services Act.

90 For the successive legislative amendments concerning the GISS's interception powers, see STANDING COMMITTEE I, *Activity Report 2018*, 60 *et seq*.

91 This does not imply that the Standing Committee I has the authority to approve or reject the list approved by the minister.

92 In these plans, GISS draws up a list of '*organisations or institutions that will be the subject of interception of their communications, penetrations of their IT systems or the capture of fixed or moving images during the coming year. These lists justify why each organisation or institution will be subject to an interception, intrusion or recording of fixed or moving images related to the assignments referred to in Article 11, § 1, 1 to 3 and 5, and state the anticipated duration*' (Art. 44/3 of the Intelligence Services Act) (free translation).

GISS must send these lists to the Minister of Defence for approval in December. The latter has ten working days to communicate its decision to GISS[93], which in turn sends the lists, with the minister's authorisation, to the Standing Committee I.[94]

The review *during* the interception, intrusion or recording is carried out '*at any time by means of visits to the installations where the General Intelligence and Security Service is performing these interceptions, intrusions or recordings of fixed or moving images*' (free translation).

The review *after* the use of the method is carried out '*using monthly lists of countries or of organisations or institutions that have actually been the subject of interception, intrusion or image capture during the previous month*' and that '*explain why the interception, intrusion or capture of images was carried out in connection with the roles referred to in Article 11, § 1, 1 to 3 and 5*' (free translation). These lists must be notified to the Standing Committee I. The *ex post* review is also carried out on the basis of '*the inspection of logs that are permanently kept at the location of the interception, intrusion or capture of fixed or moving images by the General Intelligence and Security Service*' (free translation). These logs must always be accessible to the Standing Committee I.

What can the Standing Committee I do if it finds an irregularity? Article 44/4 of the Intelligence Services Act states that the Committee, '*irrespective of the other powers conferred on it on the basis of the Act of 18 July 1991, has the right to stop ongoing interceptions, intrusions or image recordings if they are found to breach the legal provisions or the [ministerial] permission. It shall order that the data obtained unlawfully may not be used and must be destroyed in accordance with the more detailed rules to be determined by the king.*' (free translation). But despite the Committee's urgent recommendation[95], an interception Royal Decree has still not been issued.[96] The Committee again recommends that this be done as soon as possible.[97]

---

93 If the minister has not taken or communicated a decision to GISS by 1 January, the planned interceptions, intrusions and recordings may commence, without prejudice to any subsequent decision by the minister.

94 For interceptions, intrusions or recordings that are not included in the annual lists, but that '*prove indispensable and urgent*', the minister will be informed as soon as possible, and at the latest on the first working day after the method has started to be used. If the minister does not agree, he may call a halt to this method. This decision is communicated by GISS to the Standing Committee I as soon as possible.

95 STANDING COMMITTEE I, *Activity Report 2018*, 127.

96 The Committee must provide a detailed justification of its decision and communicate it to the minister and GISS.

97 In the same sense, a Royal Decree is also needed for the further rules governing the cooperation of network operators or electronic communication service providers (Art. 44/5 of the Intelligence Services Act).

III.2. MONITORING PERFORMED IN 2019

III.2.1. MONITORING PRIOR TO THE INTERCEPTION, INTRUSION OR RECORDING

The Standing Committee I previously made a number of important comments on the 'Interception plans'. The most important comments concerned the differences in priority between, on the one hand, the Intelligence Steering Plan[98] and, on the other, the intended SIGINT interceptions, and the fact that the definition of the organisations and institutions that were to be the object of interceptions was too general. In the 'Interception Plan 2019', which was sent to the Committee at the end of January 2019, GISS described the organisations that could be the object of interceptions in more detail. The Committee only had a few minor comments to make on the plan.

The image and intrusion plans, on the other hand, were rather scanty again. They were the subject of discussion at a work meeting between the Standing Committee I and GISS in March 2019. The Committee decided to include this issue in its review investigation opened in 2019 into '*the intelligence services' application of and internal control over the use of methods and instruments recently introduced or adapted by parliament with respect to which the Standing Committee I has been allocated a special supervisory role*' (free translation).

III.2.2. MONITORING DURING THE INTERCEPTION, INTRUSION OR RECORDING

In 2019, the Committee did not visit the facilities from which the interceptions occurred; this was postponed to the second half of 2020. However, these visits were planned as part of the above review investigation. There were several reasons for the postponement. First, the initial modules of the review investigation – namely, the study of Articles 16/2 and 16/3 of the Intelligence Services Act – required more time and resources than originally expected. The Committee was also confronted with other priorities and this monitoring proved to be technically impossible for some aspects (such as recordings).

[98] A plan prepared by the former Intelligence Directorate of GISS setting out the countries to be monitored and the prioritisation.

III.2.3. MONITORING AFTER THE USE OF THE METHOD

The Committee received eleven '*monthly lists*[99] *of countries or of organisations or institutions that have actually been the subject of interception, intrusion or image capture during the previous month*' and that '*explain why the interception, intrusion or image capture was carried out in connection with the roles referred to in Article 11, § 1, 1° to 3° and 5°*'.

As for intrusions, the Committee had to repeatedly remind GISS of its obligations and specify that the Committee must receive a monthly report, even if no intrusions were carried out. In October 2019, the Committee received a letter from GISS stating that there had been no intrusions in 2019. Following the letter, the Committee also received the monthly list of intrusions. It received a total of three lists. Monitoring the monthly intrusions and image recording lists were included in the aforementioned review investigation.

[99] The November 2019 list of interceptions and recordings was missing.

CHAPTER IV.
PARTICULAR ASSIGNMENTS

Over the years, the Standing Committee I has been assigned a number of particular assignments which do not originate from a statutory provision, but represent a response to a specific need. These additional roles have been assigned to the Committee in close consultation with it.

IV.1. REVIEW OF THE ACTIVITIES OF THE ISTAR BATTALION

Previously, the Standing Committee I took a position on the intelligence activities carried out by the ISTAR (Intelligence Surveillance Target Acquisition and Reconnaissance) battalion in the context of foreign operations. The Committee emphasised in this connection that the battalion had been formed to meet a growing need for battlefield intelligence, in view of the ever increasing number of foreign missions. However, it also reiterated that the Act of 30 November 1998 governing the intelligence and security services only recognises two intelligence services (Art. 2 of the Intelligence Services Act), and drew the attention of Parliament, the Minister of Defence and the CHOD to the fact that the battalion was – partly – engaging in intelligence activities.

As no legal or structural solutions could be found in the short term, in late April 2018 a provisional solution was worked out by means of a protocol agreement between GISS and the CHOD,[100] which among other things defined the tasks and duties of the ISTAR battalion with regard to HUMINT and analysis capabilities. In addition, the organisation of technical and legal oversight was worked out. Technical oversight is the monitoring of the correct application of the

[100] Protocol agreement of 24 May 2018 between the CHOD and GISS regarding the HUMINT and analysis capabilities of the ISTAR Bn. This was previously urged by the Parliamentary Inquiry Committee on Attacks: '*Although the Parliamentary Inquiry Committee considers ISTAR's assignments important for the safety of our military personnel, it believes that the relationship between this battalion and GISS should be formally regulated by means of a cooperation protocol, in which it is clearly described how and under which conditions ISTAR can contribute towards strengthening GISS's intelligence position. In that context, it also seems appropriate to entrust the monitoring of ISTAR's support task to the Standing Committee I*' (free translation), in *Parl. Doc.* Chamber of Representatives 2016-17, no. 54K1752/008, 306.

analysis guidelines, the HUMINT guidelines and the special agreements between the CHOD and GISS. Legal oversight means checking that the protocol is being applied correctly. These roles lie with GISS.

To this end, the ISTAR battalion provides GISS with internal rules and guidelines on its own initiative. Oversight is exercised by means of visits to the installations of the ISTAR battalion and to the zones where it carries out its operations and activities. It is also exercised on the basis of an analysis of documents and of hearings.

The protocol assigned to the Standing Committee I the task of monitoring the battalion's activities, albeit indirectly. To this end, GISS submits to the Minister of Defence, the CHOD and the Standing Committee I a three-monthly report on each investigation assignment.

The Committee received four monitoring reports in 2019. The reports showed that the ISTAR battalion engaged in few activities that were covered by the above protocol agreement. According to GISS, the intelligence activities developed by the ISTAR battalion complied with the imposed rules and directives.

The analysis of these reports will be the object of further investigation. Given that ISTAR develops few HUMINT activities, the Committee has not prioritised this.

IV.2. MONITORING OF SPECIAL FUNDS

The Court of Audit checks the legality, legitimacy and effectiveness of all expenditure. In principle, this also applies to all expenditure of the intelligence services. However, due to the sensitivity of this subject, part of the budget of State Security and GISS (in particular the 'special funds' including spending on operations and informants, for example) was not examined by the Court of Audit. For State Security, this specific expenditure was only audited by the General Policy Director of the Minister of Justice. Midway through 2018, the Court of Audit expressed its intention of also conducting a periodic audit of these funds from the closure of the 2018 account. In 2020, the Committee received a copy of the audit that the Court of Audit conducted in 2019 for the 2018 financial year.[101]

The audit of GISS special funds is conducted by a representative of the office of the Minister of Defence four times a year. On the suggestion of the Court of Audit, this has happened in the presence of the chair of the Standing Committee I since 2010. It was a consequence of the then Minister of Defence expressing the desire to no longer conduct the audit himself, as had been the case since 1962. In February 2019, the chair attended one of these audits. However, in May 2019, a letter was sent to the then Deputy Prime Minister and Minister of Foreign and European Affairs

[101] COURT OF AUDIT, *State Security. 2019 audit of special funds. Report addressed to the Minister of Justice*, 20 May 2020.

and Defence stating that the Committee would no longer perform this task. After all, '*in our opinion, this audit based on limited sampling does not meet the demands of a truly effective audit and could, moreover, lead to both ministerial responsibility and that of the Standing Committee I*' (free translation). It was also suggested, in line with the monitoring of State Security's funds, that this was a task for the Court of Audit. In February 2020, the Court of Audit endorsed this initiative and informed the Minister of Foreign Affairs and Defence of its willingness to conduct a formal audit of the accounts, for which it could rely on the technical support provided by Standing Committee I.[102] This allowed the Committee to '*perform its assignment with greater care over the use of these funds*' (free translation). It was decided in 2019 to launch a follow-up investigation into the management, use and audit of the special funds in 2020.[103]

IV.3. OVERSIGHT OF THE MONITORING OF POLITICAL REPRESENTATIVES

In the (parliamentary) debates, the question that was repeatedly asked was whether, and to what extent, Belgian intelligence services (may) monitor political representatives and which rules they must observe in that regard.[104]

Since the start of 2018, the service memorandum of 13 December 2017, classified as 'confidential', has been applied within State Security.[105] This service sends two types of reports to the Minister of Justice and the Prime minister, with copies to the Standing Committee I: occasional reports on political representatives who contribute to the creation of a threat as well as a quarterly overview of all documents in which political representatives are mentioned.[106] The Minister of

---

102 *This audit will be periodic and, besides examining the process and a cash audit, will include a formal verification, based on sampling, of the existence of supporting documents in accordance with the instructions and approved by the competent officials. The audit does not cover the accuracy or reliability of the underlying transactions and will be conducted in accordance with GISS's remit by auditors with the required security clearance*' (free translation).

103 STANDING COMMITTEE I, *Activity Report 2015*, 111 et seq ('Management, use and audit of special funds').

104 STANDING COMMITTEE I, *Activity Report 2008*, 24 et seq (II.2 'Reserved dossiers' at State Security). Incidentally, this was not the first time that the Standing Committee I had investigated the activities of the intelligence services in relation to political representatives (STANDING COMMITTEE I, *Activiteitenverslag 1998* (Activity Report 1998), 67 et seq.; *Activiteitenverslag 1999* (Activity Report 1999), 12 et seq. In this regard, also see *Activity Report 2013*, 117 et seq. ('II.4. Monitoring of political representatives by the intelligence services').

105 The service memorandum was updated in June 2020 to improve reporting to management on disruptive activities.

106 These political representatives are the ministers of the various governments, the Belgian Commissioner in the European Commission and the members of the various parliaments, including the Belgian members of the European Parliament. It is not about other elected or appointed representatives (e.g. at municipal level, such as aldermen, or at provincial level, such as governors).

Justice also agreed with '*the principle of verification by the Standing Committee I that appears necessary under the Review Act of 18 July 1991* ' (free translation).[107] Implementing the principles stated in the above service memorandum, State Security effectively kept the Committee informed about both types of reports in 2019. Because of the municipal elections that took place in 2018 and the regional, federal and European elections in 2019, an increasing focus on politicians could be observed. After all, in the immediate period before or after elections, State Security sees a role for itself in monitoring the proper conduct of these elections, at least with regard to the threats that it is legally required to monitor (e.g. interference). A joint project was also set up with the military intelligence service and regular consultations were held with the Centre for Cyber Security Belgium (BCC) and the Federal Crisis Centre specifically concerning possible Russian online threats (cyber, disinformation) relating to the May 2019 elections.[108]

Despite repeated requests, the Committee received no information in that regard in 2019 from GISS, which, like State Security, had been urged to adopt a uniform directive with clear and unambiguous rules on collection, processing, consultation, storage and archiving relating to political representatives. GISS did not have a standing operating procedure (SOP) to deal with this information, nor was it determined how to inform the Standing Committee I.

Since there is no mention anywhere of what the Committee is supposed to do with the above information, it took it upon itself to produce a methodology on the '*problem of monitoring political representatives by the intelligence services and the role of the Standing Committee I*' (free translation). The Parliamentary Monitoring Committee approved this methodology in 2020.

IV.4. DAG HAMMARSKJÖLD AND THE BELGIAN INTELLIGENCE ARCHIVES

On the night of 17 to 18 September 1961, the then Secretary-General of the United Nations, Dag Hammarskjöld, died in a plane crash during a peace mission in Congo. Although there were suspicions that the plane was attacked, the cause of the crash was never clarified.

---

107 Letter from the Minister of Justice to the Standing Committee I dated 26 July 2018 on 'Collection of information by an intelligence service on a person holding a political office'.

108 During 2019, the Standing Committee I launched a '*Review investigation into how the intelligence services monitor possible interference by foreign services in Belgian elections, try to counter any threats, report on this to the authorities, and in particular on the danger of cyber interference or cyber attacks in this area*' (free translation) (see I.7.4).

Former UN secretary-general Ban Ki-Moon launched a new investigation in 2017, led by Eminent Person Mohamed Chande Othman,[109] calling on Member States with relevant information about the case to appoint an independent person to conduct research in their archives and submit their findings to the UN. On 16 April 2018, the Ministers of Justice and Defence appointed the then chair of the Standing Committee I, Guy Rapaille[110], and Professor Kris Quanten, a lieutenant-colonel and lecturer at the Royal Military School, as 'independent and high-ranking officials' to assist the UN with the investigation into the death of the Secretary-General. They submitted their report to the UN in late September 2018. In early November 2018, the United Nations General Assembly received a first interim report from Othman, followed by a final report in 2019.[111] [112]

At the end of January 2019, Judge Othman asked Belgium to expand the scope of the investigation. This request arose because of certain information that came to light in investigations in other countries.[113] More specifically, Belgium was asked to establish what information the Belgian intelligence services had on the presence and/or activities of intelligence and defence personnel from other countries in Katanga in September 1961. A report in this regard was sent to the UN in June 2019.[114] The Committee, together with Lieutenant-Colonel Quanten of the Royal Military Academy, concluded that '*"the research carried out […] within the framework of this investigation, did not reveal any information that sheds new light on the precise circumstances that led to the death of Mr. Dag Hammarskjöld and his company in September 1961'.* Additional clarifications could be made in early 2020 based on new intelligence.

---

109 UNITED NATIONS, General Assembly, *71/260 Investigation into the conditions and circumstances resulting in the tragic death of Dag Hammarskjöld and of the members of the party accompanying him*, Resolution adapted on 23 December 2016, 31 January 2017, A/RES/71/260 (and A/C.5/72/19).

110 Following Guy Rapaille's retirement, the Ministers for Justice and Foreign Affairs asked the Standing Committee I in mid-March 2019 to appoint one of its members to continue the investigation. The Committee decided to entrust the task to its chair, Serge Lipszyc.

111 The matter was again the subject of a film (*Cold Case Hammerskjöld* by M. BRÜGGER) and several publications (H. MELBER, *Dag Hammerskjöld, the United Nations and the decolonisation of Africa*, Hurst Publishers, London, 2019; M. PICARD, *Ils ont tué Monsieur H. Congo 1961. Le complot des mercenaires français contre l'ONU*, (They murdered Mr H in the Congo in 1961. The French mercenary plot against the UN) Seuil, 2019).

112 See: www.hammarskjoldinquiry.info/pdf/ham_263_UN_Final_Report_complete.pdf

113 The French, Swedish and German Independent Appointees requested a mutual exchange of the interim reports in that regard.

114 BELGIAN STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE, Review investigation of the information available to the intelligence services regarding the death of Dag Hammarskjôld. Final Report, June 2019, 29.

CHAPTER V.

THE STANDING COMMITTEE I AS THE COMPETENT SUPERVISORY AUTHORITY FOR THE PROCESSING OF PERSONAL DATA

V.1. INTRODUCTION

The General Data Protection Regulation 2016/679 (GDPR)[115] and Directive 2016/680 (the Directive)[116] regulate how public and private actors must act when collecting, storing, retaining and transferring personal data. Both European instruments resulted in some important legislative amendments at national level: in December 2017, the Data Protection Authority (DPA)[117] – the successor of the Privacy Commission – was established, and in July 2019, a new Data Protection Act (DP Act) was voted on.[118] This act, in turn, amended the Review Act of 18 July 1991, with the Standing Committee I being designated as the data protection authority for the processing of personal data in the context of 'national security'.

The Committee's role is described in the Act of 3 December 201 establishing the Data Protection Authority (DPA Act), the Data Protection Act (DP Act) and the Review Act.[119]

In 2019, the Committee developed various activities to be able to observe these additional duties and obligations. Already in 2018, a Data Protection Officer (DPO) was appointed to deal with all processing operations carried out by the Committee that fall outside 'national security' (for example, processing in the context of

---

115 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (GDPR), *Official Journal of the European Union* 2 May 2016.

116 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *Official Journal of the European Union* 4 May 2016, 119/89.

117 Act of 3 December 2017 establishing the Data Protection Authority (DPA Act), *Belgian Official Journal* 10 January 2018.

118 Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (DP Act), *Belgian Official Journal* 5 September 2018.

119 For more detailed information see: STANDING COMMITTEE I, *Activity Report 2018*, 71-82.

personnel management and logistics). In addition, various meetings were held with the three other competent supervisory authorities (*infra, V.2*). Arrangements were made with the Standing Committee P to draw up a proposed amendment of the Review Act, as various provisions are not adapted to the new competence of the two Committees. Finally, the Committee has developed a number of internal work processes for its advisory function and for the investigations of citizens' complaints.

This special role of the Committee is reported on below: first, the cooperation between the various competent supervisory authorities is discussed, and attention is then paid successively to BELPIU's monitoring of personal data processing, to the Committee's provision of legal advisory opinions and the handling of individual complaints. This all fits under Article 35 § 3 of the Review Act, which states that the Standing Committee I '*shall report annually to the Chamber of Representatives on the advisory opinions issued in its capacity as a data protection authority, on the investigations carried out and the measures taken in that same capacity, and on its cooperation with the other data protection authorities*' (free translation).

V.2. COOPERATION BETWEEN THE COMPETENT SUPERVISORY AUTHORITIES

Belgium has four competent supervisory authorities (CSAs) at federal level. As well as the Standing Committee I, there is the Data Protection Authority (DPA) which has a general and residual competence, the Supervisory Body for Police Information, which mainly controls processing activities that fall within the scope of Title 2 of the Data Protection Act, and the Standing Committee P, which, together with the Standing Committee I, controls the processing activities of CUTA (Art. 161 DP Act).

With the exception of this last case, the Standing Committee I therefore acts autonomously. This does not mean that there is no consultation or cooperation between the four bodies: on the contrary, the law states for example that in certain cases there must or may be cooperation or that information must be exchanged (Articles 98 and 131 DP Act).

More important is the obligation to cooperate closely, including with regard to the processing of complaints, opinions and recommendations affecting the powers of two or more CSAs, in order to ensure consistent application of national, European and international regulations on data protection (Art. 54/1 § 1 DPA Act). This provision also states that the joint handling of complaints, opinions and recommendations must take place by means of the 'one-stop shop mechanism'. This function is performed by the Data Protection Authority. The CSAs must also agree on a protocol to achieve the required cooperation; the various services prepared

and negotiated such a cooperation protocol in 2019.[120] The protocol was finalised in mid-2020.

V.3. BELPIU'S MONITORING OF PERSONAL DATA PROCESSING[121]

V.3.1. FRAMEWORK FOR BELPIU'S MONITORING

The Act of 25 December 2016 on the processing of passenger data (PNR Act) implements the European objectives of simultaneously preventing and combating terrorism and related serious crime.[122] For this purpose, a 'Passenger Information Unit' (PIU) was set up within the Home Affairs FPS. It keeps passenger data in a database for preventing and combating the crimes or threats specified in the PNR Act.

Under subtitle 5 of Title 3 of the DP Act, the Standing Committee I is the competent supervisory authority for '*any processing of personal data by the PIU for the purposes referred to in Article 8, § 1, 4 of the Act of 25 December 2016*' (Article 169 of the DP Act) or, in other words, processing operations that come under the scope of '*Articles 7, 1 and 3/1 and 11, § 1, 1 to 3 and 5 of the Act of 30 November 1998 regulating the intelligence and security service*' (free translation) (Article 8, § 1, 4 of the PNR Act). In other words, processing by State Security and GISS as part of their regular intelligence assignment. The Committee is competent to monitor the functioning of the PIU only to the extent that it cooperates with requests for information and intelligence from one of the two intelligence services, whether in the form of targeted searches, watch lists or profiles.

V.3.2. A SIMULTANEOUS (LIMITED) INSPECTION

Given their respective powers as competent supervisory authorities for data processing by the Passenger Information Unit, the Supervisory Body for Police Information (C.O.C) and the Standing Committee I decided, on their own initiative,

---

120 The legislators provide for an evaluation of the Data Protection Act three years after its entry into force (art. 283 DP Act). One of the aspects that will need to be addressed is the cooperation between the various CSAs.

121 BELPIU stands for Belgian Passenger Information Unit.

122 The PNR Act is the transposition of Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime (PNR Directive) and of Council Directive 2004/82/EC of 29 April 2004 on the obligation of carriers to communicate passenger data (API Directive).

to conduct a simultaneous (limited) inspection of this unit.[123] After all, the powers of both services with regard to the PIU may not be completely identical, but they at least overlap.[124] The inspection was not the result of an individual complaint or any specific indications of non-compliance with laws and regulations.

The approach to the inspection was designed with an emphasis on compliance: are passenger data processed in accordance with the law and with a high standard of security? The inspection focused more on information security than on legal aspects.[125]

The reason for a limited inspection was simple. First, the PIU had only been operational since the start of 2018. Second, not all envisaged passenger carriers and travel operators were technically connected to the PIU yet. The inspection was limited to two areas: first, ICT security and information safety; second, the proportionality of data processing. The inspection report was finalised in June 2020 and presented to the Parliamentary Monitoring Committee.

V.4. PROVIDING OPINIONS

The Committee may provide an opinion in two cases '*on a draft of a bill or a royal decree, circular or any other document setting out the policies of the competent ministers*' (free translation): if the law requires it to give an opinion or at the request of the Chamber of Representatives or the competent minister (Article 33, sixth paragraph of the Review Act). Such opinions relate specifically to the issue of data processing and must therefore be distinguished from the Committee's general advisory competence which may also relate, for example, to efficiency and coordination. This general advisory competence is broader in that sense, but it is also narrower since it is limited to the operation of the intelligence services and CUTA.

In this capacity, the Committee, working alone or once with the Standing Committee P, issued nine advisory opinions on bills or draft decrees in 2019. Preparing these opinions implied a considerable additional workload for the Committee. These opinions may be consulted in full on the Committee's website (http://www.comiteri.be/index.php/en/publications/advice). A list of the opinions issued is sufficient here:

123 The inspection took place on 27 November 2019.

124 This inspection did not cover how the two Belgian intelligence services use their powers in this context. This aspect was addressed by the Committee in a separate review investigation launched in 2019 (see I.7.2).

125 This approach did not prevent the Supervisory Body for Police Information or the Standing Committee I from taking appropriate action when obvious legal shortcomings were identified.

- Opinion 001/VCI-BTA/2019 of 5 February 2019 on *'a draft bill amending the Act of 25 December 2016 on the processing of passenger data'*;
- Opinion 002/VCI-BTA/2019 of 9 April 2019 on the *'draft Royal Decree amending the Royal Decree of 12 October 2010 implementing various provisions of the Act of 30 November 1998 governing the intelligence and security services and the Royal Decree of 3 July 2016 implementing Article 21 of the Act of 30 November 1998 governing the intelligence and security services*';
- Opinion 003/VCI-BTA/2019 of 27 June 2019 on the '*draft bill amending the Act of 11 December 1998 on classification and security clearances, certificates and advice*';
- Opinion 004/VCI-VCP-BTA/2019 of 27 June 2019 relating to a request for an opinion from the Minister of the Interior on '*the draft bill on municipal administrative enforcement and establishing an Integrity Assessment Directorate for Public Administrations (CUTA)*';
- Opinion 005/VCI-BTA/2019 of 3 July 2019 relating to a request for an opinion from the Minister of the Interior on '*the draft bill on municipal administrative enforcement and establishing an Integrity Assessment Directorate for Public Administrations (State Security – GISS)*';
- Opinion 006/VCI-BTA/2019 of 23 August 2019 relating to a request for an opinion from the Minister of Foreign Affairs on '*the draft bill consenting to the Agreement between the Kingdom of Belgium and the Republic of Cyprus on the mutual protection of classified information, concluded in Brussels on 20 July 2015*';
- Opinion 007/VCI-VCP-BTA/2019 of 23 August 2019 relating to a request for an opinion from the Minister of Foreign Affairs on '*the draft bill consenting to the Agreement between the Kingdom of Belgium and Hungary on the mutual protection of classified information, concluded in Budapest on 21 September 2015*';
- Opinion 008/VCI-BTA/2019 of 23 August 2019 relating to a request for an opinion from the Minister of Foreign Affairs on '*the draft bill consenting to the Agreement between the Kingdom of Belgium and the Republic of Finland on the mutual protection of classified information, concluded in Helsinki on 20 July 2016*';
- Opinion 009/VCI-BTA/2019 of 23 August 2019 relating to a request for an opinion from the Minister of Foreign Affairs on '*the draft bill consenting to the Agreement between the Kingdom of Belgium and the Kingdom of Spain on the mutual protection of classified information, concluded in Brussels on 15 October 2015*' (free translations).

In February 2019, the chair of the Standing Committee I was invited to a hearing in the Commission for Justice to explain the opinion[126] formulated in 2018 on the bill containing various provisions on criminal matters and on religious services.[127]

V.5. INFORMATION FROM THE MONITORED SERVICES

The services monitored by the Committee must keep or make certain information available to the Standing Committee I[128] in the following circumstances:

- a security breach entailing a high risk to the rights and freedoms of natural persons, which must be reported as soon as possible, and preferably within 72 hours of the controller becoming aware of it (Articles 89, 122, 155 and 180 of the DP Act);
- a register with information about the databases or processing activities used (Articles 90, 123, 156 and 181 DP Act);
- the appointment of a Data Protection Officer (DPO) by the data controller or the processor (Articles 91, 124 and 127 DP Act).

No data breaches[129] were reported to the Committee in 2019. The Committee also did not receive registers containing information on databases or processing activities. The authorities for which the Committee is responsible were contacted for the purpose of compiling a list of the appointed data protection officers.
The Committee will continue to monitor the correct application of this complex legislation, given the monitored services' limited knowledge of it at present.

V.6. HANDLING OF INDIVIDUAL DPA COMPLAINTS

The Standing Committee I also handles individual requests with regard to the processing of personal data by the aforementioned persons and services and their processors (Art. 34 Review Act and Articles 79, 113, 145 and 173 DP Act). The requesting party has the right to ask for his or her inaccurate personal data to

126 Opinion 008/VCI-BTA/2018, available at www.comiteri.be/advies (New intelligence methods and protection and support measures (2018)).

127 *Parl. Doc.* Chamber of Representatives 2018-19, no. 54K3515/001.

128 Not every service has to keep or provide all of the data mentioned here. This is certainly true of the SIM Commission for example, which is not required to communicate any information to the Standing Committee I.

129 A personal data breach is defined as '*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*' (Article 4 GDPR) (free translation).

be rectified or erased and for a check to be conducted that the applicable data protection rules have been complied with. In order to be admissible, the request must be written, dated, signed and duly justified (Art. 51/2 Review Act).[130] If the request is manifestly unfounded, the Committee may decide not to comply with it. This decision must be duly justified and communicated to the requesting party in writing.[131]

In 2018 the Standing Committee I received five DPA complaints from citizens regarding potential processing of personal data by State Security and GISS, four of which were fully dealt with in 2019. In 2019, the Committee received fourteen complaints, three of which did not fall within its remit (but did fall within that of the Supervisory Body for Police Information) and one of which was judged admissible but manifestly unfounded. Eight of these new complaints have been dealt with in 2019.[132] The complainants were informed that the required verifications were carried out.[133] The managing officer of the intelligence service or the director of CUTA – and, subject to approval by the Committee, any other body or person – will receive '*the conclusions of the investigation*' (Art. 34, last paragraph of the Review Act – free translation). The three pending DPA complaints (one from 2018 and two from 2019) have been dealt with in 2020.

130 This provision also states that the request '*must justify the identity of the data subject*' (free translation). It is not immediately clear what this means. Probably it means that the data subject must provide proof of his or her identity, as this obligation is included in the relevant provisions of the Data Protection Act (see Articles 80, 114, 146 and 174 DP Act).

131 Such checks are conducted free of charge (Articles 80, 114, 146 and 174 DP Act).

132 One complaint was dealt with jointly with Standing Committee P.

133 *'The data subject has the right to ask for inaccurate personal data to be rectified or erased'* (Art. 79 DP Act). *'The Standing Committee I shall carry out the verification and merely inform the data subject that the necessary verifications have been made'* (Art. 80 DP Act), so no further explanation may be given (free translations).

CHAPTER VI.

MONITORING OF THE COMMON DATABASES

In 2016, the Ministers of Home Affairs and Justice set up the common database of foreign terrorist fighters (CDB FTF). Its purpose was to contribute to the analysis, evaluation and monitoring of individuals with links to this issue. In 2018, this common database (CDB) was redesigned: from now on it is known as the common database of terrorist fighters (CDB TF), and in addition to the (existing) general category of 'foreign terrorist fighters' also includes a new category of 'homegrown terrorist fighters'. In addition, a separate common database was set up in 2018 of 'hate propagandists' (CDB HP).[134]

Lastly, the Royal Decree of late 2019[135] included two additional categories of persons in the CDB TF, namely the 'potentially violent extremists' (PVE) and 'terrorism convicts' (TC).

VI.1. THE MAIN REGULATORY CHANGES

VI.1.1. THE DATA PROTECTION OFFICER

The Act of 22 May 2019[136] amended the Policing Act to bring it into line with the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Data Protection Act). The position of 'security and privacy adviser' was replaced by 'data protection officer' (Article 44/11/3*quinquies*/1 of the Policing Act). This officer is tasked with:

---

134 Article 44/6 of the Policing Act assigns the task of monitoring the processing of the information and personal data contained in the CDB to the Supervisory Body for Police Information and to the Standing Committee I (hereinafter 'the supervisory authorities').

135 Royal Decree of 20 December 2019 amending the Royal Decree of 21 July 2016 on the common database of terrorist fighters and the Royal Decree of 23 April 2018 on the common database of hate propagandists and implementing certain provisions of Section 1*bis* 'Information management' of Chapter IV of the Police Function Act, *Belgian Official Journal* 27 January 2020.

136 Act of 22 May 2019 amending various provisions relating to police information management, *Belgian Official Journal* 19 June 2019.

- providing expert advice on information security, data protection and data processing. In particular, the officer must ensure compliance with the general conditions governing the lawfulness of processing;
- implementing, updating and monitoring a data security and protection policy;
- performing other tasks relating to data protection and security determined by the King or entrusted to the officer by the Ministers of Home Affairs and Justice.

These tasks are performed in addition to those envisaged for data protection officers in the Data Protection Act.

VI.1.2. ROYAL DECREE OF 20 DECEMBER 2019

The Royal Decree of 20 December 2019 (above) has a threefold objective. First, new categories are added to the common database of terrorist fighters (CDB TF), namely 'potentially violent extremists' and 'terrorism convicts'. Second, several 'technical amendments' are made to the Royal Decrees TF and HP because of the amendment of the Act of 5 August 1992 by the Act of 22 May 2019. Lastly, the intention was to give FPS Finance's General Administration of the Treasury direct access to the TF and HP databases.

VI.1.2.1. Adding potentially violent extremists (PVE) to the CDB TF

A 'potentially violent extremist' is defined as any natural person who has a link with Belgium and meets these cumulative criteria:

a) they have extremist views that legitimise the use of violence or coercion as a method of action in Belgium;
b) there are reliable indications that they intend to use violence, in connection with the views mentioned in a);
c) the PVE must also meet at least one of these criteria that increase the risk of violence:
   - they have systematic social contacts within extremist circles;
   - they have a psychological problem, as determined by a qualified expert;
   - they have committed acts or have a record that may be regarded as a) a crime or an offence against the physical or mental integrity of third parties; or b) instruction or training in the manufacture or use of explosives, firearms, other weapons or noxious or hazardous substances, or in other specific methods or techniques useful for committing terrorist offences; or c) deliberate acts that constitute material support for a terrorist/extremist

organisation or network; or d) offences which by their nature point to a disturbing awareness of security by the person concerned.

VI.1.2.2. Adding terrorism convicts (TC) to the CDB TF

Terrorism convicts meet these cumulative conditions:
– they have a link with Belgium;
– they have been convicted or been the subject of a court decision for involuntary commitment, or in the case of minors, of a protection measure for terrorist offences as stipulated in Book 2, Part I*ter* of the Penal Code (in Belgium), or for similar offences abroad; and
– whose level of threat is classified by the CUTA as medium (level 2), serious (level 3) or very serious (level 4).

By introducing this new category in the CDB TF, all actors that must ensure monitoring of terrorism convicts (such as DGPI, law centres, police, closed asylum centres, State Security, the Local Task Forces, etc.) are proactively, promptly and fully informed about the persons concerned.

VI.1.2.3. Direct access to CDB TF and HP for a new service

Under the Royal Decree of 20 December 2019, the General Administration of the Treasury was also granted direct access to the CDB TF and HP.[137] In this case, it is the competent authority for imposing financial sanctions including freezing the funds and economic resources of persons or entities that commit or attempt to commit, facilitate or cooperate in terrorist offences.

VI.2. MONITORING ASSIGNMENT

VI.2.1. OBJECT OF MONITORING

For 2019, the Supervisory Body for Police Information and the Standing Committee I decided to focus their joint monitoring on two aspects: first, on following up certain recommendations formulated in the previous years' reports; second, on making inquiries at several basic and partner services about legitimacy

[137] It should be noted that access for the General Administration of the Treasury was not included in the draft Royal Decree or in the complementary prior report submitted to the Supervisory Body for Police Information and the Standing Committee I.

checks and the internal procedures to ensure the smooth processing of information in the CDB TF and HP.[138]

Coordinating the data processing of information in the CDB TF and HP, including the role of the Data Protection Officer (DPO), was also highlighted. The increasing number of services accessing the CDB TF and HP was also considered.

VI.2.2. FOLLOWING-UP THE RECOMMENDATIONS

VI.2.2.1. Appointment of the Data Protection Officer

The Ministers of Justice and Home Affairs jointly appointed a DPO for the CDB TF and HP in early September 2019.[139] This officer is the preferred discussion partner of the Supervisory Body for Police Information and the Standing Committee I.

VI.2.2.2. Implementation of a mechanism for reporting security incidents

A tab is available on the application screen to report a security incident.[140] The application user can thus report the identified problem and the DPO of the service(s) concerned can access a summary of all incidents saved in relation to the CDB TF and HP. The safety incident management rules are described on the screen to assist the user's understanding.

The procedure to be followed was defined in the manual. Although this had been addressed previously, the manual makes no mention of an external data breach that should be routinely reported to the Supervisory Body for Police Information and the Standing Committee I, even though this practice was a recommendation to the Federal Police within the meaning of Article 44/11/3quinquies/2, last paragraph, of the Policing Act.

VI.2.2.3. Development of an additional IT tool

It was previously established that CUTA did not have an IT tool for monitoring the retention periods and the deletion of data about persons who appear (or appeared)

---

138 The new PVE and TC categories were introduced by the Royal Decree of 20 December 2019, which appeared in the *Belgian Official Journal* on 27 January 2020. They were thus not subject to monitoring in 2019.

139 The Supervisory Body for Police Information and the Standing Committee I took note of the fact that this role is combined with both the role of DPO at CUTA and material activities at CUTA. It has not yet been possible to assess whether the material time commitment envisaged for this role is sufficient and what direction any risk of a conflict of interests will take.

140 These give access to the CDB TF and HP.

in one of the five FTF categories. This finding led the supervisory authorities to repeat their recommendation to develop an IT tool.

In 2019, 487 entities that had been in the CDB FTF for at least three years were monitored. For 485 of these entities, CUTA referred to *'the logical workflow where no anomalies were found'*. CUTA also provided a useful explanation. Even so, the recommendation to develop an IT tool that makes it possible to monitor the data retention periods referred to in Article 44/11/3bis § 5 of the Policing Act was repeated.

VI.2.2.4. Performance of spontaneous checking of logged information

According to information from the Federal Police in relation to spontaneous checking of logged information, a distinction must be made between a 'minor log'[141], a 'major log'[142] and a 'legitimacy check'. The logging request can be made using the user ID.

The Federal Police reported receiving 73 requests for logs within their own services in 2019, including 71 minor logs and two through the 'legitimacy check' tab. No 'major logs' were requested.

The Supervisory Body for Police Information and the Standing Committee I pointed out the importance of also checking major logs. Within the partner services, it was necessary to raise awareness of these legitimacy checks, which should be performed systematically.

VI.2.2.5. The exception to the obligation to include police information in the CDB

There are two exceptions to the obligation to feed the common databases (Article 44/11/3*ter* § 5 of the Policing Act). First, the obligation to feed may be postponed as long as the competent magistrate, with the consent of the Federal Prosecutor, believes feeding it may jeopardise the conduct of criminal proceedings or a person's safety. The managing officer of an intelligence service can also postpone the transfer of data, if and as long as they believe that feeding the database might endanger a person's safety or the third-party agency rule.

In a previous monitoring report, it was noted that police information from information reports (RIRs) with the code 00 or 01 is not included in the CDB TF and HP. These codes result from the Circular MFO3 and concern feeding the National General Database (BNG/ANG), but this exception has not been maintained in the regulations on the CDB TF and HP. De lege lata, the law and the implementing order do not allow to exclude these data from the common database.

---

141 A 'minor log' is a log about the processing performed on an entity of the common database and is accessible to all users with read and write rights.

142 A 'major log' is a log about the processing by the users of the common database and can be performed only by the Federal Police as administrator.

The Federal Police informed the supervisory authorities that a Local Task Force (LTF) working group decided to include only the RIR 01 in the common database. If necessary, the user concerned may request that they be notified of a RIR 01 referred to in the CDB TF and HP. This request is then assessed on a case-by-case basis.

The Supervisory Body for Police Information and the Standing Committee I noted that this practice is based purely on the (unpublished) Circular of 14 June 2002, which cannot conflict the statutory provisions on feeding the CDB TF and HP.

VI.2.2.6. Transfer of lists

In their previous monitoring report, the Supervisory Body for Police Information and the Standing Committee I listed the regulations and conditions for legitimately transferring lists. They recalled their earlier observation about the technical security needed for the transfer of lists if this is done by email. In addition, they considered it appropriate for the basic service performing the transfer to properly inform the recipient of the list.[143] Lastly, the supervisory authorities raised questions about the authority/authorities tasked with monitoring the recipients regarding the use of the list and how monitoring could be performed.

According to the monitoring performed in 2019, the practice consisted in a list of the personal data and information in the CDB TF and HP being emailed each month to the FPS Employment, the Federal Agency for Nuclear Control (FANC) and Brussels Prevention & Safety, among others. The Supervisory Body for Police Information and the Standing Committee I could not find any joint evaluation drawn up by the Federal Police, CUTA and the intelligence and security services.[144] The recommendation to notify the receiving services of the conditions under which the list may be communicated also proved to be a dead letter. In this context, the Supervisory Body for Police Information and the Standing Committee I asked questions particularly about how the institution Brussels Prevention & Safety could receive the lists, especially since it had not been added as a new partner service when the regulations were amended.[145]

The Supervisory Body for Police Information and the Standing Committee I emphasised that the communication of personal data and information from the common database to third-party bodies is subject to strict and cumulative statutory provisions. As for the technical security needed for transferring lists,

143 For example, by concluding a prior protocol between the services.

144 This is imposed by Article 44/11/3 quater of the Policing Act and referred to in Article 11 § 2 Royal Decree TF and HP.

145 A legal analysis of Brussels Prevention & Security and its access to the common database for terrorist fighters was presented to the Parliamentary Monitoring Committee in September 2020.

the monitoring in 2019 resulted in a repeat of the recommendation to conclude protocol agreements with the services that are the recipients of the lists.

VI.2.3. USE OF THE COMMON DATABASE TF AND HP BY THE PARTNER SERVICES

VI.2.3.1. Verifying access to the CDB TF and HP by the partner services and feeding the database

The number of active users in each partner service and the number of times this partner service accessed the database were checked. This showed that 17 out of a list of 47 partner services in December 2019 did not foresee any use for the CDB TF and HP.

As for the partner services that have indicated no user or logins for the CDB TF and HP for several years, the Supervisory Body for Police Information and the Standing Committee I pointed to a possible lack of the 'need to know' and the importance of monitoring the extent to which the conditions of Article 44/11/3ter § 2 of the Policing Act are, or are still being, fulfilled. Logically, the direct or indirect access of certain partner services should be reviewed in the context of that lack of necessity.

VI.2.3.2. Data security and protection policy

The Supervisory Body for Police Information and the Standing Committee I could establish that the role of data protection officer is seen as an advisory and coordinating function, and that the search for a common vision supported by all partner services involved is a priority. While the intention obviously cannot be for DPOs to take decisions instead of the controllers, the supervisory authorities emphasised that the initiative to provide an initial proposal can come from the DPO for the CDB TF and HP. After all, developing a common approach could be unnecessarily delayed if one were to wait for the initiative of the partner services to present (differing) proposals.

The Supervisory Body for Police Information and the Standing Committee I recommended they be given a copy of the policy notes that the Data Protection Officer of the CDB TF and HP will prepare in light of the data security and protection policy choices, more specifically in relation to accessing and feeding the CDB TF and HP. The DPO of the common database actually aims to establish a 'dynamic' register of processing operations during the first quarter of 2020. In general terms, it was explained that the dynamic nature refers to a solution integrated into each of the common databases that can both meet statutory requirements and be easily updated. An 'ordinary' register of processing operations, which will remain general,

will be provided in the meantime. In a first awareness-raising phase, the DPO will moreover provide a presentation module[146] covering the principles of processing, the obligations of the various actors involved in processing personal data and the role of the DPO.

VI.2.3.3. Two findings

A first finding concerns the General Administration of the Treasury, whose Financial Sanctions Unit is made up of four people with personal access to the common database. From the report to the King, it can be inferred that this General Administration is in a position to feed the CDB TF and HP with relevant information. But this access and the security measures applied need to be evaluated further.

The regulations also consider the independent status of the Public Prosecution Service, as there is no obligation (only an option) for that partner service to feed the CDB TF and HP, even though it has direct access to the TF database. The legislator has held that judicial data come mainly from the police forces. In this sense, the police forces' obligation to feed the common database suffices to ensure that the judicial police's relevant data are recorded.[147]

To ensure the TF database is fed properly, the judicial authorities have sent instructions. These stated that the Public Prosecutor's Offices will not feed the CDB TF and HP. But circular COL 10/2015 provides that magistrates on the closed list of reference magistrates for terrorism are to communicate the information relating to the case for which they are competent to CUTA, at its request, when the person concerned is the subject of a federal investigation by the Federal Public Prosecutor's Office. Changes to these judicial measures are also communicated to CUTA.

The Terrorism Expertise Network reviewed and updated the circulars to produce a single integrated and updated circular on the judicial approach to terrorist fighters and hate propagandists. The role of security magistrate will also be abolished and replaced by a magistrate-security officer. The Public Prosecution Service will therefore no longer depend on FPS Justice's security officer, but will have its own security officers.

It is envisaged that the magistrate-security officer's duties will include monitoring the CDB TF and HP's logs. At present, the security magistrate prepares the nominative lists of all magistrates and employees of the Public Prosecution Service who have access to the CDB TF, but after the various existing circulars are merged into a new circular, these lists will be available at one of the five competent magistrate-security officers (one for each Court of Appeal). In practice, the judicial

146 This module should be operational in the first half of 2020.

147 However, the Supervisory Body for Police Information and the Standing Committee I have noted that this reasoning does not apply to judgments and rulings of which police forces are unaware.

measures in the CDB TF and HP are included in a list that the public prosecutor's offices send to CUTA after an inquiry.

In their monitoring report, the Supervisory Body for Police Information and the Standing Committee I noted that CUTA's inquiry of the Public Prosecution Service regarding judicial measures is not systematic, which means that some of the information in the CDB TF and HP may be outdated or incomplete.

VI.2.3.4. The security clearances situation

There is currently no mechanism by which partner services are denied access to the CDB TF and HP on the basis that the user does not have a security clearance.[148] There is a separate arrangement for the Public Prosecution Service. Magistrates at the Public Prosecution Service do not need a security clearance. Only the employees of the Public Prosecution Service need a security clearance. COL 22/2016 states that once the request for that purpose has been made, employees will have access to the CDB TF. The Supervisory Body for Police Information and the Standing Committee I took the view that it was advisable not to grant access to the CDB TF until the clearance had been obtained. Consultation of the database in the meantime could be left to employees who already have such a clearance.

The question also arose of the need to continue providing access to the CDB TF and HP for services that have not requested the necessary security clearances or have not handed over a list of users to the Federal Police. From information that the Supervisory Body for Police Information and the Standing Committee I received from the DPO of the CDB TF and HP, it appeared several partner services did not envisage any use in practice and there were no logins associated with those services.

The Supervisory Body for Police Information and the Standing Committee I could moreover see that the vigilance regarding the correct application of Article 44/11/3*quater* of the Policing Act was very limited. The question arises whether access to non-personalised mailboxes is effectively limited to those with the necessary security clearance.

148 The obligation to have a security clearance stems from Article 7 § 2 Royal Decree TF and HP.

VI.3. ADVISORY ASSIGNMENT

VI.3.1. THE REQUEST NOT TO CARRY OUT PROCESSING OPERATIONS WITHOUT THE APPROPRIATE LEGAL BASIS

At the end of March 2019, the director of CUTA informed the chair of the Standing Committee I of a letter from CUTA addressed to the chair of the Data Protection Authority (DPA). This letter informed the DPA that a test period would be initiated, during which the processing of two new categories, namely the potentially violent extremists and the terrorism convicts, would be started in the CDB TF from the beginning of April 2019. According to the CUTA Director, including these two new categories responded to important needs in the field, especially in detention centres, and met the recommendations of the Parliamentary Inquiry Committee on Terrorist Attacks. The director of CUTA explained that the Local Task Forces' monitoring of entities would be unified thanks to the definition of clear criteria. Several texts, including the draft Royal Decree prepared at the technical level, but not yet validated at the political level, were attached to the letter. CUTA director therefore wished to inform the chair of the DPA '*in full democratic transparency*' and asked the chair for a preliminary opinion on the draft texts.

In a letter sent to the Ministers of Justice and of Security and Home Affairs in mid-June 2019, the Standing Committees I and P and the Supervisory Body for Police Information emphasised that the statutory procedure had to be followed, regardless of whether the processing was planned for a 'test period' or on a permanent basis. The letter stressed that personal data could be processed in a common database only after the approval of a Royal Decree submitted to the Council of Ministers (adopted after an opinion from the supervisory authorities and the Council of State) and after a prior report to the Supervisory Body for Police Information and the Standing Committee I. In doing so, the Standing Committees I and P and the Supervisory Body for Police Information supported the view of the Board of Procurators General. As a result, the Ministers, in their capacity as controllers, were asked to stop processing the data relating to the two categories concerned. In a letter sent in mid-July 2019, the Ministers confirmed that they had instructed the Federal Police to make it technically impossible to use the two new categories.

VI.3.2. OPINION ON A DRAFT ROYAL DECREE TO INCLUDE THE PVE AND THE TC

In early 2019, the Supervisory Body for Police Information and the Standing Committee I issued a joint advisory opinion[149] on the draft Royal Decree amending the Royal Decree TF. They first noted the significant expansion of the existing CDB TF to include potentially violent extremists. Referring to the risks, especially in the context of transfer to (foreign) authorities, the supervisory authorities felt that the draft should be amended so that individuals subject to 'preliminary investigation' for six months should only be known to the basic services, which should use their existing statutory options to obtain information and intelligence that would allow them to confirm or cancel the inclusion in the database.

The Supervisory Body for Police Information and the Standing Committee I have thoroughly examined the various criteria and subcriteria that describe the PVEs in the draft Royal Decree.

The supervisory authorities stated that they clearly understand the difficult task of the police intelligence and security services in (proactively) combating terrorism and extremism that may lead to terrorism. In this sense, creating the common databases meets the recommendations of the Parliamentary Inquiry Committee on Terrorist Attacks to allow information to circulate more efficiently among the actors in the criminal justice and security chain. But this Parliamentary Inquiry Committee does not recommend that the target group should be expanded to such an extent that the link with terrorist violence disappears. For this reason, it was requested, firstly, that their recommendations be taken into account and, secondly, that the predefined criteria be applied seriously.

The Supervisory Body for Police Information and the Standing Committee I pointed out that if their recommendations are not followed, there is a risk that the basis for registration in the CDB will be lowered to the level that corresponds to the processing conditions for the administrative police, on the one hand, and the processing conditions for the intelligence services on the other. As a result, highly privacy-sensitive data are increasingly being passed on to (more and more) services and institutions outside the criminal justice or security chain. However, these (administrative) services often have no or limited experience in managing such sensitive and sometimes uncertain data, with possible consequences for the data subjects' lives.

As for expanding the CDB TF by including terrorism convicts (TC), the Supervisory Body for Police Information and the Standing Committee I asked the authors of the draft to consider questions about persons convicted abroad, minors imposed a protection measure for terrorist offences, and persons not yet finally convicted.

---

149 Opinion 001/VCI-COC/2019 of 1 August 2019 on a draft Royal Decree amending the Royal Decree of 21 July 2016 on the common database of terrorist fighters (www.comiteri.be).

Lastly, the supervisory authorities also considered the new indirect access provided for in the draft Royal Decree for the institution Brussels Prevention & Safety (BPS). Specific emphasis was placed on the lack of clarity of the context in which this institution was designated a partner service, with reference to Article 44/11/3*ter*, § 3 of the Policing Act. Given that the draft left many questions unanswered (about the use and sharing of data by BPS, the rules on retention and on envisaged security measures), the Supervisory Body for Police Information and the Standing Committee I considered it unacceptable for a new institution to be added to the already extensive list of recipients without demonstrating its relevance and social added value.

VI.3.3. OPINION ON THE 'COMPLEMENTARY PRIOR REPORTS'

In mid-July 2019, the Ministers of Justice and of Security and Home Affairs submitted a request for an advisory opinion to the Supervisory Body for Police Information and the Standing Committee I on the complementary prior report of the CDB TF and HP. This (third) complementary prior report set out the practical data processing arrangements for the Law Centres of the Communities and the Flemish Youth Welfare Agency (*Vlaams Agentschap Jongerenwelzijn*).[150]

In their joint opinion at the end of November 2019[151], the Supervisory Body for Police Information and the Standing Committee I pointed out that the failure to appoint a DPO had now been resolved and that the contact details – or changes in the contact details – of DPOs of the existing and new services with existing or new access must be reported. Their opinion on this complementary report was favourable, subject to the comments made.

150 The Supervisory Body for Police Information and the Standing Committee I were able to ascertain from the contents of the letter of 24 July 2019 from the Ministers responsible for processing that the National Security Authority had still not been granted access.

151 www.comiteri.be.

CHAPTER VII.

CRIMINAL INVESTIGATIONS AND JUDICIAL INQUIRIES

As well as contributing to review investigations, the Investigation Service I also conducts investigations into members of the intelligence services suspected of a crime or offence. Such investigations are carried out by the Investigation Service on behalf of the judicial authorities. This competence is described in Article 40, third paragraph, of the Act of 18 July 1991 on the supervision of the police and intelligence services and of the Coordination Unit for Threat Assessment. The Threat Assessment Act of 10 July 2006 extended this competence to crimes or offences committed by members of the Coordination Unit for Threat Assessment (CUTA).[152]

When they perform a judicial police assignment, the members and director of the Investigation Service I for the intelligence services are under the supervision of the prosecutor-general at the Court of Appeal or the federal prosecutor (Article 39 of the Review Act), and the Standing Committee I has no authority over them. However, the chair of the Standing Committee I must also ensure that the performance of judicial police assignments does not impede the performance of review investigations. The reason for this is obvious: the supervisory body has many other statutory duties, which could be compromised if too much time is spent on judicial cases. In such cases, the chair may consult with the judicial authorities about the use of members of the Investigation Service I in criminal investigations (Art. 61*bis* of the Review Act).

In the cases in which the Investigation Service I conducts criminal investigations, the director must report to the Standing Committee I after the investigation is completed. In this case, however, '*the report shall be limited to the information necessary for the Standing Committee I to perform its assignments*' (free translation) (Art. 43, third paragraph Review Act).

In 2019 the Investigation Service I carried out investigative actions in the context of its judicial role, in two criminal investigations.

In 2019, the Investigation Service I completed an investigation that had started in 2017. This investigation was being conducted at the request of the Federal

[152] With regard to the members of the other 'supporting services' of CUTA, this provision only applies with respect to the obligation to pass on relevant information to CUTA (Articles 6 and 14 of the Threat Assessment Act).

Prosecutor's Office and concerned the possible involvement of a member of an intelligence service in a crime or offence against the internal and external security of the State. In connection with this, it was investigated whether another member of the same intelligence service had violated their professional secrecy in relation to this person.[153]

At the request of an examining magistrate and headed by the Federal Public Prosecutor's Office, the Investigation Service I also carried out several investigative acts as part of an investigation into crimes committed by a criminal gang and into the question of whether the intelligence services had any information on them.
In addition, Article 50 of the Review Act states that '*any member of a police service who observes a crime or offence committed by a member of an intelligence service must draw up an information report and send it to the Head of the Investigation Service I within fifteen days*' (free translation). In 2019, the investigation service received no notifications to this effect.

153 STANDING COMMITTEE I, *Activity Report 2015*, 139 ('II.9. Complaint regarding the disclosure of personal information by an intelligence agent to a third party').

CHAPTER VIII.
EXPERTISE AND EXTERNAL CONTACTS

VIII.1. EXPERT AT VARIOUS FORUMS

Members of the Standing Committee I and its personnel were consulted as experts by public and private institutions in Belgium and elsewhere several times in 2019:

- In March 2019, at State Security's invitation, the chair of the Committee participated in the founding meeting of Intelligence Network Europe (INE).[154] The project aims to establish a training platform for intelligence service members, but also to focus on informing policymakers who come into contact with intelligence. It is intergovernmental and wants to focus on connections and networking rather than acquiring a physical infrastructure.
- In May 2019, the chair and registrar were invited to Berlin to participate in a European Intelligence Oversight Network (EION) workshop with topics including '*How can oversight bodies better assess and demonstrate the effectiveness of their control instruments?*' and '*What insights can be distilled from other systems, such as banking supervisory authorities or antitrust compliance programs, to identify innovations for intelligence oversight?*'
- In November 2019, at the request of the German think tank *Stiftung Neue Verantwortung*, the registrar made a contribution ('*A simple yet existential demand: let oversight bodies work together*') towards a new online communication platform (www.aboutintel.eu) whose aims include serving as an inspiration for intelligence, technology and democracy, making specialised contributions on these items accessible to a wide audience, and promoting mutual understanding between the different actors of the intelligence community.
- The Standing Committee I registrar was invited to explain the Committee's work for the Intelligence course of the Master's programme in International Relations and Diplomacy (University of Antwerp).

---

154 Initially, the project was called the European Intelligence Academy (*Académie européenne de Renseignement*, AeR) but the name INE (with the motto 'Enhancing a common strategic culture') was ultimately chosen to underline its networking character. It is the response to a call that French President Macron made in September 2017, wanting to build a European intelligence culture.

VIII.2. COOPERATION PROTOCOL ON HUMAN RIGHTS INSTITUTES

The 'Human Rights Institute' – whose full name is the Federal Institute for the Protection and Promotion of Human Rights – was established under the Act of 12 May 2019 after many years of insistence.[155] The creation of a national Human Rights Institute, a commitment made when the Protocol to the UN Convention against Torture was signed, was a long time coming. Belgium was reproached several times for this, including by the United Nations.

Pending the actual creation of the institute, meetings with various institutions with a human rights mandate[156] resulted in a cooperation protocol signed in January 2015,[157] in which the participating bodies agreed to exchange practices and methods, to investigate common issues and to promote mutual cooperation.

The newly created institute ('Federal Institute for the Protection and Promotion of Human Rights') was given various tasks: it provides opinions and recommendations on matters relating to the promotion and protection of fundamental rights, either on request or of its own accord; it monitors the implementation of international commitments entered into by the Belgian authorities; and it encourages the ratification of new international human rights instruments. One year after the founding Act was published, the Chamber of Representatives formed a board of directors by appointing twelve independent persons from academic and legal circles, from civil society and from the social partners.

VIII.3. A MULTINATIONAL INITIATIVE ON INTERNATIONAL INFORMATION EXCHANGE

The increased international data exchange between intelligence and security services entails a number of challenges for national oversight bodies. The oversight bodies of (initially) five European countries (Belgium, Denmark, the Netherlands, Norway and Switzerland)[158] are therefore working together to meet these challenges by finding ways to reduce the risk of a supervisory gap. After some time, a new partner became involved in this project, i.e. the Investigatory Powers Commissioner's Office (IPCO) from the United Kingdom. The group was renamed the Intelligence Oversight Working Group (IOWG) and expanded in

155 Act of 12 May 2019 establishing a Federal Institute for the Protection and Promotion of Human Rights, *Belgian Official Journal* 21 June 2019.

156 Such as Unia (the former Interfederal Equal Opportunities Centre), the Federal Migration Centre, the Institute for Gender Equality, the Data Protection Authority, the Federal Ombudsman, the High Council of Justice, and the Standing Committees I and P.

157 Cooperation protocol of 13 January 2015 between institutions with a full or partial mandate to safeguard respect for human rights.

158 See STANDING COMMITTEE I, *Activiteitenverslag 2015* (*Activity report 2015)*, 80-81.

2019 to include three observers, i.e. the Swedish Foreign Intelligence Inspectorate (*Statens inspektion av försvarunderättelse-verksamhet*, SUIN), the Swedish Board of Inventions (*Statens uppfinnarnämnd,* SUN) and the German G10 Commission.

The partners believe the established oversight needs more intense cooperation between the national oversight bodies. This purely national mandate and the national classification rules present challenges for oversight, which can only look for the time being at one end of the spectrum when exchanging data. The increasing volumes of data transfers, multilateral exchange and common databases also pose a challenge for oversight bodies, all the more so since the regulations on them are rather scanty and vary from country to country. Lastly, technological developments make the task of oversight bodies even more difficult.

In recent years, various expert meetings have been held during which methods, best practices and legal and practical problems have been discussed and experiences exchanged. A 'joint' review investigation was also conducted (see I.3). At the beginning of November 2018 a joint statement and press release were prepared by the participating oversight bodies.[159]

In March 2019, the Committee organised a meeting in Brussels as part of a new project to jointly study two topics with these institutions: first, the implications of introducing the new PNR system for the functioning of the intelligence services and for their oversight; second, the innovation of oversight, in particular through using a common investigative methodology coupled with ICT resources.

In mid-December 2019, on the initiative of the Dutch Intelligence and Security Services Review Committee (CTIVD), the 'Charter of the Intelligence Oversight Working Group'[160] was signed.

VIII.4. CONTACTS WITH FOREIGN REVIEW BODIES

The Standing Committee I also maintained close contacts with various foreign oversight bodies in 2019.

With a view to creating a normative framework for international cooperation between intelligence services and oversight bodies, initial contacts were made with various Benelux authorities. However, the topic could not be put on the agenda of the Benelux Ministerial Committee.

During a colloquium held at the French Military Academy (*Ecole Militaire*) in early February 2019, ties were strengthened with the chairs of the National Commission for the Review of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement,* CNCTR) and the Parliamentary Delegation on Intelligence (*Délégation parlementaire au renseignement*, DPR),

159 See STANDING COMMITTEE I, *Activity Report* 2018, Appendix D. 'Strengthening the oversight of international data exchange between intelligence and security services'.

160 See Appendices of this activity report.

which participated as part of the panel 'The right to intelligence – a strongly controlled right that deviates from the general law' (*Le droit du renseignement - un droit exorbitant du droit commun fortement contrôlé*).

As usual, there were also bilateral contacts with the Dutch oversight body. In April 2019, the Dutch 'system-based oversight' concept was explained during a working meeting in Brussels and the strategy to be followed for foreign partnerships was also discussed. In May 2019, a two-day meeting was held with representatives of the Special Commission to Authorize Telecommunications Surveillance and Monitoring Measures and Traffic Data Tracking (*Commission spéciale chargée d'autoriser les mesures de surveillance et de contrôle des télécommunications ainsi que le repérage des données relatives au trafic*) and with the full delegation of the Review Commission of the State Intelligence Service (*Commission de contrôle du Service de renseignement de l'État*). A consultation also took place between the chairs of the Committee and the French National Commission for the Review of Intelligence Techniques (*Commission nationale de contrôle des techniques de renseignement,* CNCTR) in Paris in June 2019. Arrangements were made with the new Investigatory Powers Commissioner (UK) for a mutual introduction. Following the entry into force in July 2019 of the National Security and Intelligence Review Agency Act, a new Canadian supervisory body was established, i.e. the National Security and Intelligence Review Agency (NSIRA), with a broader mandate than its predecessor. Both chairs agreed to organise a working visit. Lastly, privileged contacts were maintained with the Swiss Independent Intelligence Review Authority (*Autorité de surveillance indépendante des activités de renseignement*, AS-Rens) with a view to implementing an internship/exchange project during 2020.

In October 2019, the third edition of the International Intelligence Oversight Forum on the topic of 'Intelligence oversight at a crossroads' was organised in London by the Special Rapporteur for Privacy (SRP), Professor Cannataci. Representatives of oversight bodies, intelligence services, universities and NGOs took part. The purpose of the forum was to improve understanding of the challenges faced by democratic oversight bodies (among others) in a confidential environment.[161]

VIII.5. MEMORANDUM

In the wake of the May 2019 federal parliamentary elections, the Standing Committee I submitted a Memorandum to the *informateurs* (those appointed to

[161] With themes such as '*Relationship between overseers and overseen (outreach, transparency, personnel selection)*', '*Oversight across the intelligence cycle*', *'Making oversight affordable and accessible for the citizen*'.

identify a likely coalition) at the time. [162] [163] The Committee did not doubt the necessary interest reserved for the proper functioning of the country's intelligence services and the need to maintain democratic and effective control over them. The Memorandum drafted with this in mind wanted to draw the informateurs' attention to the importance of certain legislative initiatives in this regard. The proposals included amending the Review Act, paying attention to the strengthened functioning of the Committee, the requirements for the protection of personal data (and the installation of a secured network), the need to set up an internal control and audit service within the intelligence services, and the computerisation and simplification of the procedures for the Appeal Body on security clearances, certificates and advice.

[162] Both intelligence services, the Ministers of Defence and Justice, and the President of the Chamber of Representatives also received the Memorandum.

[163] The Committee had already taken a similar initiative at the request of the King's then *informateur* after the federal parliamentary elections of June 2007 (STANDING COMMITTEE I, *Activiteitenverslag 2007* (Activity Report 2007), 52-54).

CHAPTER IX.

THE APPEAL BODY FOR SECURITY CLEARANCES, CERTIFICATES AND ADVICE[164]

IX.1. INTRODUCTION

The Appeal Body is the administrative jurisdictional body which deals with disputes relating to administrative decisions in four domains: security clearances, security certificates granting access to places where classified documents are stored, security certificates granting access to specific places where there is a threat, and finally, security advice. In addition, the Appeal Body can also hear proceedings for annulment against decisions by public or administrative authorities to request security certificates or advice in a specific sector or for a specific location or a specific event.[165]

The Appeal Body is composed of the chairs of the Standing Committee I, of the Standing Committee P and of the Dispute Chamber of the Data Protection Authority. The chair of the Standing Committee I chairs the Appeal Body. The registrar of the Committee I performs the registry role. The registry's personnel are appointed by the Committee I. For more than 20 years, the Appeal Body's activities have been a perfect example of synergy within certain satellite institutions of the Parliament.

This is because the Standing Committee I fully supports its operation. On the one hand, this not only includes providing the chair, their deputies and the registrar, but also the lawyers and the administrative personnel who form the registry of this administrative tribunal. On the other hand, the Committee I also includes the costs of the offices as operating costs of the Appeal Body in its budget.

The registrar, assisted by lawyers and Committee I employees, keeps the registry running, receives the appeal files for the hearings and prepares them.

---

164 This chapter implements Article 13 of the Act of 11 December 1998 establishing an appeal body for security clearances, certificates and advice, which stipulates that the appeal body must draw up an annual report.

165 For more information, see STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 91-124 and STANDING COMMITTEE I, *Activity Report 2018*, 107-120.

IX.2. A SOMETIMES CUMBERSOME AND COMPLEX PROCEDURE

The increase in the number of cases in 2019 (see below) is accompanied by an increased workload. The administrative management of cases, hearings and decisions remains complex. The quality of the compiled case file is certainly one of the causes, but the increasingly frequent involvement of lawyers also has a major impact. Indeed, this rightly entails the obligation for the Appeal Body to give reasons for its decisions by responding to all the arguments that a lawyer puts forward in defence of their client's interests.

Many cases do not meet the requirements set out in Articles 2 and 3 of the Royal Decree on the Appeal Body, which state that '*all procedural documents are to be sent to the Appeal Body by registered letter*' and that '*the notice of appeal is to be signed and dated by the appellant or by a lawyer*' (free translations). The future law (*lege ferenda*) must take better account of the capacity and even the vulnerability of many appellants and create statutory provisions that do not entail nullity by operation of law.

Another factor that sometimes adds to the workload and delays the processing of cases is the way in which the different security and other authorities concerned handle the administration of these cases. It is evident that such a delay may be contrary to the appellant's interests. To remedy this, the Appeal Body has regularly drawn the attention of these authorities to the following problems:

- The statutory deadline within which the administrative file must be sent to the Appeal Body is often exceeded. This makes it difficult for the Appeal Body to adhere to the period within which it must make a decision.
- As the administrative files sent by the various security authorities are not always complete, the registry has to take additional actions. Sometimes the file turns out only to have been compiled after an appeal has been lodged.
- The application of Article 5 § 3 of the Appeal Body Act is often problematic. This provision allows the Appeal Body to decide, at the request of an intelligence or police service, to remove some documents from the file made available for examination by the appellant or their lawyer. This is the case if distribution of these documents could jeopardise the protection of sources, the privacy of third parties, the performance of the intelligence services' statutory duties, or the secrecy of an ongoing criminal investigation or judicial inquiry. However, such requests are rarely (properly) substantiated, or they come from an authority that is not legally competent to make them, which again sometimes makes it necessary for the registry to obtain additional information. Often these authorities also mistakenly cling to the idea that the appellant and their lawyer will be barred from inspecting classified data without any further explanation being required, and despite the settled case

law of the Appeal Body showing that the Appeal Body Act is a *lex specialis* in terms of the Classification Act. Finally, there are also cases in which the chair of the Appeal Body has to remove information from the file on his or her own initiative, in order to protect the privacy of third parties, because the service in question has obviously neglected to invoke Article 5 § 3 of the Appeal Body Act.

- The decisions of the security authorities are insufficiently substantiated and – contrary to the statutory requirements – a duly justified decision is not drawn up in the cases in which Article 22, paragraph 5 of the Classification and Security Clearances Act allows certain information to be omitted from the decision notified to the person concerned. The security authority must also clarify in its justification which specific facts constitute a contra-indication to disclosure, given the regulatory purpose of a specific security verification. Only in this way can the Appeal Body determine whether a decision is proportional or not.
- Furthermore, the decisions of various security authorities have shown a lack of care and respect for the formal principles of administrative law (decisions without the details and identity of the official taking the decision; the person concerned has never been heard; language use in administrative matters).
- The security authorities do not follow the established case law of the Appeal Body (for example, on the issue of investigations into or verifications of non-Belgian nationals).

It should also be noted that the hearings take much longer than they used to a few years ago. There are various reasons for this. More and more appellants are being assisted by one or two lawyers. The complexity means that certain cases take a long time. The Appeal Body therefore has to make more decisions before passing judgment or granting adjournments.

As a result, the number of hearings is also increasing. After all, these are necessary to obtain the additional information that the tribunal requires to make a decision.

The decision-making process itself also takes more time than a few years ago. There are two reasons for this. First, there are the many procedural issues (e.g. admissibility, use of language, rights of defence or delegation of power of the body making the decision). Second, the Appeal Body is more often confronted with extremely sensitive cases. These cases obviously require extremely careful handling and appropriate motivation because of the delicate balance between the need for the legal subject to understand the decision and the need to keep secret information that could endanger the security of the state or its institutions.
It is sometimes also necessary to take specific security measures.

IX.3. CHANGES OF THE STATUTORY FRAMEWORK: TWO LEGISLATIVE AMENDMENTS

In 2018, the legislative framework was significantly changed, both as regards the Classification and Security Clearances Act and the Appeal Body Act.

In 2019, the legislator made only two amendments (of relative importance for the work of the Appeal Body). The first concerned the definition of protected witnesses as provided for in Article 3 of the Classification and Security Clearances Act.[166] The purpose of the second was to exempt accredited professional journalists from paying the fee referred to in Section 22*septies* of this Act.[167]

IX.4. DETAILED STATISTICS

This section gives a statistical picture of the nature of the contested decisions, the capacity of the competent authorities and of the appellants and the nature of the decisions of the Appeal Body within the various appeal procedures. To make some comparison possible, the figures for the past four years have also been included.

The general trend in the figures of the past few years shows an increase in the number of appeals submitted to the Appeal Body. This increase is occurring around three major axes: first, an increase in the number of appeals relating to security clearances (from 36 in 2018 to 51 in 2019). Second, after a year of decline, disputes over security advice have also increased sharply (from 92 in 2018 to 115 in 2019). And third, there were also many more appeals relating to the refusal of security certificates for the nuclear sector (from 11 in 2018 to 17 in 2019).

For the first time, the Appeal Body has dealt with the issue of granting a security certificate to an imam to work in Belgian prisons under the provisions of the Royal Decree of 17 May 2019.[168]

A case was also brought before the tribunal on the issue of granting security advice to customs officers required to carry a weapon in the course of their duties, in accordance with the provisions of the Royal Decree of 15 December 2013.[169]

As far as the Appeal Body knows, the new security advice procedure described in the 2018 Activity Report has not yet been used. There are some suggestions of a desire to step up checks in future on the integrity and morality of the personnel of

166 Act of 5 May 2019 containing various provisions on criminal matters and religious services, and amending the Act of 28 May 2002 on euthanasia and the Social Penal Code (*Belgian Official Journal* 24 May 2019).

167 Act of 2 May 2019 amending the Act of 11 December 1998 on classification and security clearances, certificates and advice (*Belgian Official Journal* 27 May 2019).

168 Royal Decree of 17 May 2019 concerning chaplains, religious service consultants and moral counsellors at prisons (Article 3 § 3, 1).

169 Royal Decree of 15 December 2013 identifying the services at the General Customs and Excise Administration where performing roles is subject to security verification.

the European institutions and ports. The new security advice procedure might be applied for this purpose.

Lastly, there were 21 hearings of the Appeal Body in 2019.

Table 1. Security authority concerned

	2015	**2016**	**2017**	**2018**	**2019**
National Security Authority	68	92	129	113	114
State Security	1	0	0	0	0
General Intelligence and Security Service	47	68	53	32	61
Federal Agency for Nuclear Control	10	8	7	10	17
Federal Police	3	1	3	3	3
Local Police	1	0	0	0	1
TOTAL	**130**	**169**	**192**	**158**	**196**

Table 2. Nature of the disputed decision

	2015	**2016**	**2017**	**2018**	**2019**
Security clearances (Article 12 *et seq*. Classification and Security Clearances Act)					
Confidential	9	5	1	2	5
Secret	35	38	33	31	39
Top secret	4	7	6	3	7
Refusal	36	28	30	26	39
Withdrawal	7	9	7	4	16
Refusal and withdrawal	0	0	0	0	0
Clearance for a limited duration	3	4	1	1	3
Clearance for a lower level	0	1	0	0	0
No decision within the time limit	2	7	2	5	0
No decision within the extended time limit	0	1	0	0	0
SECURITY CLEARANCES SUBTOTAL	48	50	40	36	51

	2015	2016	2017	2018	2019
Security certificates for classified zone (Art. 22*bis*, para. 1 Classification and Security Clearances Act).					
Refusal	6	1	3	3	1
Withdrawal	0	0	0	0	0
No decision within the time limit	0	0	0	0	0
Security certificates for a place or event (Art. 22*bis*, para. 2 Classification and Security Clearances Act).					
Refusal	12	9	20	15	12
Withdrawal	1	0	0	0	0
No decision within the time limit	0	0	0	0	0
Security certificates for the nuclear sector (Art. 8 *bis* Classification and Security Clearances Act)					
Refusal	-	7	7	11	17
Withdrawal	-	1	0	0	0
No decision within the time limit	-	0	0	1	0
Security advice (Art. 22*quinquies* Classification and Security Clearances Act)					
Negative advice	63	101	122	92	115
No advice	0	0	0	0	0
Retraction of positive advice	0	0	0	0	0
Normative legal acts of an administrative authority (Art. 12 of the Appeal Body Act)					
Decision by a public authority to request security certificates	0	0	0	0	0
Refusal by the NSA to carry out verifications for security certificates	0	0	0	0	0
Decision by administrative authority to request security advice	0	0	0	0	0

	2015	2016	2017	2018	2019
Refusal by the NSA to carry out verifications for security advice	0	0	0	0	0
CERTIFICATES AND ADVICE SUBTOTAL	82	119	152	122	145
TOTAL DISPUTED DECISIONS	130	169	192	158	196

Table 3. Capacity of requesting party

	2015	2016	2017	2018	2019
Official	4	2	4	5	4
Military personnel	29	23	20	8	27
Private individual	93	139	164	140	163
Legal entity	4	5	4	5	2

Table 4. Appellant's language

	2015	2016	2017	2018	2019
French	75	99	115	83	101
Dutch	54	70	77	75	95
German	0	0	0	0	0
Other	1	0	0	0	0

Table 5. Registry acts

	2015	2016	2017	2018	2019
Complete file requested (1)	130	167	191	154	191
Supplementary information requested (2)	7	23	36	12	18
Reminders sent to the security authorities (3)	/	/	/	/	21[170]

170 These are reminders that the registry sends to the security authorities by letter (eleven reminders related to investigation files, two related to security verification files for security certificates and eight related to security verification files for security advice). There were also numerous telephone reminders, but these cannot be considered or included in these statistics for practical reasons.

(1) The Appeal Body has the option to request the entire file from the security authorities. As this file contains more information than the investigation report alone, this request is made by the registry as a matter of course.
(2) The Appeal Body has the option to make a request during the procedure for supplementary information that it deems useful. In practice, the registry asks the authorities to complete the files.
(3) Article 6 of the Royal Decree on the Appeal Body sets the periods for the security authorities to deliver the files. Those periods start when the registrar sends a copy of the appeal to the security authority concerned. These vary according to the nature of the disputed act. For example, the security authority must submit its file within fifteen days for security clearances, within five days for security certificates and within ten days if the appeal relates to a security advice. If these deadlines are not met, the registry makes the necessary contacts. These data have been recorded since 2019.

Table 6. Preparatory judicial acts of the Appeal Body[171]

	2015	2016	2017	2018	2019
Hearing a member of a government agency (1)	7	10	0	1	6
Decision by the chair (2)	0	0	0	0	0
Removal of information from the file by the Appeal Body (3)	50	54	80	72	77
Decisions before passing judgment (4)	/	/	/	/	9[172]

(1) The Appeal Body may decide to hear the members of the intelligence and police services or of the security authorities who have cooperated in the security investigation or security verification.
(2) The chair of the Appeal Body may decide that the member of the intelligence service must keep certain information secret during his or her questioning.
(3) If the intelligence or police department concerned so requests, the chair of the Appeal Body may decide that certain information is to be removed from the file presented to the appellant for examination.

171 The figure for 'preparatory judicial acts' (Table 6), 'how the appellant exercises their rights of defence' (Table 7) or the 'nature of the decisions of the Appeal Body' (Table 8) are not necessarily the same as the number of applications submitted (see Tables 1 to 4). Some applications were started in 2019, for example, but the decision was not made until 2020.

172 Of these interlocutory decisions, five were taken with regard to security clearances, one with regard to a security certificate and three with regard to security advice.

(4) For example, this could involve a decision to merge two files or to ask for further information on the context of a judicial file. These data have been recorded since 2019.

Table 7. How the appellant exercises their rights of defence

	2015	2016	2017	2018	2019
Access to file by the appellant and/or their lawyer	84	87	105	69	96
Hearing the appellant (whether or not assisted by a lawyer)[173]	107	127	158	111	143

Table 8. Nature of the Appeal Body's decisions

	2015	2016	2017	2018	2019
Security clearance (Art. 12 ff. Classification and Security Clearances Act)					
Appeal inadmissible	4	0	3	0	1
Appeal devoid of purpose	3	7	0	4	3
Appeal unfounded	19	18	13	12	12
Appeal well-founded (full or partial adjudication)	24	24	24	12	25
Additional investigative actions by the authority	0	2	0	1	1
Additional time for the authority	1	2	1	1	0
Waiver of appeal granted	1	0	0	3	2
Security certificates for classified zone (Art. 22*bis*, para. 1 Classification and Security Clearances Act).					
Appeal inadmissible	0	0	1	0	0
Appeal devoid of purpose	0	0	1	0	0
Appeal unfounded	4	1	0	1	1
Appeal well-founded (adjudication)	2	1	1	0	3
Waiver of appeal granted	-	-	-	-	1

173 The Appeal Body Act regulates the assistance of a lawyer during the hearing, but not the representation by this lawyer. In certain cases, the appellant (whether or not assisted by a lawyer) is heard more than once.

	2015	2016	2017	2018	2019
Security certificates for a place or event (Art. 22*bis*, para. 2 Classification and Security Clearances Act).					
Appeal inadmissible	0	0	1	2	4
Appeal devoid of purpose	0	0	1	0	0
Appeal unfounded	8	2	12	2	4
Appeal well-founded (adjudication)	10	4	7	3	4
Waiver of appeal granted	2	0	1	2	0
Security certificates for the nuclear sector (Art. 8*bis* § 2 Classification and Security Clearances Act)					
Appeal inadmissible	-	1	1	0	1
Appeal devoid of purpose	-	1	0	1	0
Appeal unfounded	-	0	1	1	5
Appeal well-founded (adjudication)	-	7	5	6	7
Waiver of appeal granted	-	-	-	2	0
Security advice (Art. 22*quinquies* Classification and Security Clearances Act)					
Appeal Body did not have jurisdiction	0	0	20[174]	12	0
Appeal inadmissible	6	15	10	3	7
Appeal devoid of purpose	0	0	1	3	1
Confirmation of negative advice	28	42	49	46	40
Conversion to positive advice	23	46	41	27	43
Waiver of appeal granted	0	0	1	0	1
Appeal against normative legal acts of an administrative authority (Art. 12 of the Appeal Body Act)	0	0	0	0	0
TOTAL	135[175]	173	195	144	166

174 The appeals in question had been lodged against (negative) security advice from the National Security Authority (NSA) with regard to the personnel of subcontractors active at European institutions. The Appeal Body had ruled that there was no statutory basis for the advice of the National Security Authority. The Appeal Body therefore ruled it lacked jurisdiction to judge whether the security advice provided by the National Security Authority was well-founded.

175 There were two more specific decisions of granting a waiver of appeal, bringing the total in 2015 to 137.

IX.5. PROSPECTS

At the direction of the chair, extensive reflections and steps have been taken to modernise the functioning of the Appeal Body. Several important objectives have been set: simplifying and standardising the procedure, improving access to the tribunal for citizens, and digitalised processing of files by the registry.

Like other tribunals, the Appeal Body has committed itself to simplifying its legal language.

To transform the Appeal Body into a more accessible, efficient and modern tribunal, the Organic Law and the Royal Decree governing the administration of justice for the Appeal Body must be amended. The Appeal Body hired an external expert to review the basic texts: Ivan Verougstraete, former president of the Court of Cassation. Several meetings were held with him.

A simpler procedure with uniform time limits for appeals must be developed. This procedure must also enable the legal subject to lodge their application electronically and to obtain letters and other notifications of decisions from the registry by the same means.

Lastly, the project aims to create the conditions for consulting files remotely, considering the possible classification of certain documents making up the file.

Secure electronic communication of both the file and its documents and of the decisions should become the norm with the various security authorities in future.

This desire to simplify goes hand in hand with developing an IT platform to enable the registry to fully process appeals digitally.

A specific website for the tribunal is also being developed. Legal subjects, the bar associations and the administrative authorities will be able to find all the information they need there. In view of the development of legislation, the website will be designed so appeals can be made electronically. The parties will also be able to contact the registry about their case through this platform.

It should also be noted that publishing the decisions on that website is under consideration. It is important that everyone has access to the case law of the Appeal Body. This guarantees an institution's transparency for its citizens. The published decisions will be anonymised, taking into account that the information must not be of such a nature as to endanger a fundamental state interest, the confidentiality of information or the confidentiality of an ongoing criminal investigation, the protection of sources or the protection of privacy of third parties.

CHAPTER X.

INTERNAL FUNCTIONING OF THE STANDING COMMITTEE I

X.1. COMPOSITION OF THE STANDING COMMITTEE I

In 2019, the composition of the Committee did not change: Serge Lipszyc, first substitute labour prosecutor at the Labour Court in Liège (F), who was sworn in during September 2018[176], fulfilled his role as chair. Counsellor Laurent Van Doren (F), former chief police commissioner[177] and counsellor Pieter-Alexander De Brock (N) remained in office. Although Mr De Brock's mandate expired in May 2019, he was not reappointed until mid-January 2020.[178]

In the Investigation Service I, however, there was a change with the recruitment of an additional commissioner-auditor, specialised in ICT. After a few months of employment, this person left the service; their replacement was appointed in September 2019. The investigation service thus comprises six commissioner-auditors, including the director Frank Franceus (N).

The administrative staff of the Standing Committee I, headed by registrar Wouter De Ridder (N), remained unchanged in 2019 with 18 administrative personnel members. However, vacancies were published for the recruitment of a French-speaking and a Dutch-speaking statutory lawyer and a French-speaking statutory secretary.[179] The Committee could continue to rely on the Data Protection Officer (DPO), appointed to deal with all processing operations that fall outside 'national security' (for example, processing in the context of personnel management and logistics).

176 On 28 February 2019, Vanessa Samain and Didier Maréchal were appointed as first and second deputy chair respectively.

177 Several calls had to be issued in 2018 for the positions of first and second successor of French-speaking member of the Committee. On 22 November 2018, Thibaut Vandamme and Michel Croquet were designated as first and second substitute respectively.

178 *Proceedings* Chamber of Representatives 2019-20, CRIV55PLEN020, 52.

179 *Belgian Official Journal* 13 June 2019 and *Belgian Official Journal* 22 October 2019.

X.2. MEETINGS WITH THE MONITORING COMMITTEE

The Chamber of Representatives amended the Chamber Rules at its plenary session on 17 October 2019. This altered the composition of the Special Committee Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee. In the future, as many members as necessary will be appointed so that each political group represented on the standing commission has at least one member on the Monitoring Committee. Each political group not represented on the Monitoring Committee will appoint one non-voting member from among its members to participate in its work.[180] The voting members of the Monitoring Committee are[181]: Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Marco Van Hees (PVDA-PTB), Egbert Lachaert (Open Vld) and Meryame Kitir (sp.a). As from June 2019, the Committee met under the chairmanship of the President of the Chamber of Representatives, Patrick Dewael (Open Vld). Georges Dallemagne (cdH) participated as a non-voting member.

Only two meetings were held in the course of 2019. During these Monitoring Committee meetings, various review investigations handled by the Standing Committee I were discussed in closed sessions. Time was also reserved to discuss the annual report on the use of specific and exceptional methods by the intelligence services and their monitoring by the Standing Committee I (Art. 35 of the Review Act) and the report drawn up within the framework of its supervisory powers – together with the Supervisory Body for Police Information – regarding the common databases (Art. 44/6 of the Policing Act). The general *Activity Report 2018* was discussed during the meeting of 17 December 2019.[182] The Standing Committee I was thanked for '*its accurate report, which is a very useful tool for the commission*' (free translation). Several topics attracted the special attention of the MPs, such as the functioning of GISS, the oversight of the monitoring of political representatives and the follow-up of the recommendations. As its final conclusion, the Monitoring Committee '*took note of the activity report 2018 of the Committee I*'

---

180 *Belgian Official Journal* 25 October 2019. '*The change in the rules allows for a smaller composition of the monitoring commission in the current composition of Parliament, which will hopefully improve efficiency*' (free translation), in *Proceedings* Chamber of Representatives 2019-20, 17 October 2019, CRIV55PLEN009, 33.

181 *Proceedings* Chamber of Representatives 2019-20, 24 October 2019, CRIV55PLEN010, 2.

182 The Commission refers for this purpose to Article 66 bis, § 2, of the Review Act, as amended by the Act of 6 January 2014 amending various laws for the reform of institutions (*Belgian Official Journal* 31 January 2014).

(free translation). In contrast to previous years, '*the approval of the Committee's recommendations*' (free translation) was not made explicit.[183]

In December 2019 the 'Charter of the Intelligence Oversight Working Group' – signed as part of developing the international relationship of six review bodies[184] – and the '2019-2022 Management Plan of the Standing Committee I' were provided to the President of the Chamber of Representatives.[185] On the one hand, this plan contains a mission statement intended to define the Committee's institutional role, the purpose of the assignments, and the values it wishes to promote. On the other hand, it lists the strategic and operational objectives.

X.3. JOINT MEETINGS WITH THE STANDING COMMITTEE P

As well as informal contacts in the workplace, five joint meetings took place in 2019. Articles 52 to 55 of the Review Act determine the circumstances and manner in which the Standing Committee I and the Standing Committee P are supposed to organise joint meetings. These joint meetings are chaired alternately by the Chairmen of the Standing Committees (Article 54 of the Review Act). The purpose of the meetings is twofold: to exchange information and to initiate and discuss ongoing joint review investigations.

In 2019, one joint review investigation was under discussion: the previously launched investigation into CUTA's supporting services (see I.7.1). It was decided not to launch additional joint investigations (e.g. into right-wing extremism).

Various points were also put on the agenda: the joint status of administrative staff, drafting an ethics charter and amending the internal regulations, the adversarial aspect to review investigations, and the search for possible synergies between both institutions. In relation to the latter point, a protocol on the use of the 'audio and video' interrogation room was concluded, the joint shooting training of the commissioner-auditors was studied, and a training course for a judicial site visit was organised.

---

183 *Parl. Doc.* Chamber of Representatives 2019-20, no. 55K0888/001, 20 January 2020 (Activity report 2018 of the Standing Committee on the Intelligence and Security Services, Report on behalf of the Special Committee Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee).

184 See Appendices of this activity report.

185 The plan was approved on 18 October 2019 and delivered to the President of the Chamber of Representatives on 9 December 2019.

X.4. FINANCIAL RESOURCES AND ADMINISTRATIVE ACTIVITIES

The Standing Committee I's 2019 budget was set at 4.211 million euros, up 12.02% on the 2018 budget.[186] This significant increase was prompted by the Committee's involvement in implementing the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (*Belgian Official Journal* 5 September 2018), which stems directly from Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. After all, Part III of this Act designates the Standing Committee I as the 'data protection authority tasked with monitoring the processing of personal data by the intelligence and security services and their processors' (free translation). This new assignment required additional employees: two lawyers and a commissioner-auditor.

The sources of financing for the budget were allocated by the Chamber of Representatives[187] as follows: 89.76% appropriation budget and 10.24% surplus from 2017.

Because of the government's resignation on 21 December 2018, it was not possible to vote on the bill containing the general expenditure budget for the 2019 financial year. Even so, the chronology of the parliamentary proceedings allowed for the 2019 budget to be formally adopted and the provisions of Article 2 of the Act of 25 December 2016[188] to be implemented, thus avoiding the application of the provisions on the provisional twelfths.

The implementation of the 2019 budget produced a budget surplus of 475,019 euros, consisting of the difference between income and combined expenses.

The budget is traditionally based on various sources of financing and the only new contribution for management purposes is entered against the appropriation from the State's general expenditure budget. Until 2017 this appropriation was insufficient to cover the Committee's actual expenses, resulting in a systematic loss. The tendency to apply Article 57, paragraph 1 of the Review Act as far as possible, which states that the funds required for functioning should be imputed to the appropriations budget, allows the Committee to finance its activities nowadays.

The significant accounting surplus is mainly due to the passage of time between approving the budget and, in particular, employees actually taking up their employment because of the lengthy recruitment procedures and obtaining the required security clearances. But once these employees are recruited – all other things being equal – a natural balance is expected between income and expenditure.

---

186 *Proceedings* Chamber of Representatives 2019-20, CRIV55PLEN020, 52.

187 *Parl. Doc.* 2017-2018 Chamber of Representatives, 54K3418/001, 57-58 and *Proceedings* Chamber of Representatives 2019-20, 20 December 2018, CRIV54PLEN264.

188 Act of 25 December 2016 amending the Act of 22 May 2003 on organising the budget and accounts for the Federal State, *Belgian Official Journal* 29 December 2019, 3rd ed.

In parallel with receiving the new tasks assigned to it, the Standing Committee ensured that it continued to seek and implement synergies between the various institutions entitled to appropriations.

X.5. IMPLEMENTATION OF THE AUDIT RECOMMENDATIONS OF THE COURT OF AUDIT

In December 2017, at the request of the Accounts Committee of the Chamber of Representatives, the Court of Audit, together with Ernst and Young, launched an investigation into the institutions entitled to appropriations, including the Standing Committee I. The Court of Audit focused primarily on budgetary aspects (an analysis of income and expenditure) and on delineating the tasks of the various institutions. Ernst and Young's main assignment was to further analyse the processes, systems and organisational structure in each of these institutions. The audit report[189] was delivered at the end of March 2018. It formulated recommendations for the 'assignments' of nine of the institutions entitled to appropriations that were involved in the audit. The common feature in the assignments of these institutions *'lies in the aim of achieving better legal protection for citizens by exercising various forms of oversight in specific policy areas*' (free translation).

2019 was dominated by implementing the numerous audit recommendations. This created a lot of extra work for the Standing Committee I in addition to the already increased workload (*supra*).[190]

X.6. TRAINING

Because of its importance for the organisation, the Standing Committee I encourages its members and employees to attend general (IT, management, etc.) or sector-specific training courses and conferences.[191] In April 2019 a cooperation protocol for this purpose was concluded between the Committee and the Institute for Judicial Training.[192] The following study days were attended by one or more personnel or other members of the Standing Committee I:

---

189 *Institutions entitled to appropriations. Duties – Income – Expenditure.* Audit at the request of the Accounts Committee of the Chamber of Representatives, Report approved on 28 March 2018 by the general meeting of the Court of Audit.

190 It resulted in a 'follow-up report' in 2020: COUR DES COMPTES, *Institutions à dotation - Suivi des recommandations formulées en 2018*, (COURT OF AUDIT, Institutions entitled to appropriations. Follow-up of recommendations made in 2018), 57 p.

191 Internal training courses were also held, including a number of safety briefings (compulsory for employees) as well as intelligence-related training courses.

192 Cooperation Protocol between the Standing Intelligence Agencies Review Committee and the Institute for Judicial Training, 4 April 2019.

DATE	TITLE	ORGANISATION	LOCATION
2019-2020	*Hautes études de sécurité et défense/ Hogere studies Veiligheid en Defensie* (Advanced Studies in Security and Defence)	Royal Higher Institute for Defence	Brussels
24-25 January 2019	Oversight	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)	The Hague
31 January 2019	*'Radicalisering, burgerschapszin en onderwijs'* (Radicalisation, Citizenship and Education)	Belgian Intelligence Studies Centre (BISC)	Willebroek
08 February 2019	*Le droit du renseignement* (Intelligence Law)	Intelligence Academy	Paris
05 March 2019	Inaugural meeting of Intelligence Network Europe (INE)	French Government	Paris
7-8 March 2019	Oversight on intelligence services		Brussels
29-30 March 2019	Good governance in the area of security	Democratic Centre for Armed Forces (DCAF) / MinInt Tunisia	Tunis
02 April 2019	22nd Public Sector Congress: 'The Digital Official'	4Instance	Brussels
25 April 2019	European Defence – The Capability Issue	Royal Higher Institute for Defence	Brussels
14 June 2019	Terrorism data and studies in Belgium – exchange of ideas between practice and research	Egmont Institute and the Coordination Unit for Threat Assessment (CUTA)	Brussels
31 July 2019	Working visit	*Coordination nationale du renseignement et de la lutte contre le terrorisme, Unité de coordination de la lutte anti-terroriste, Service national du renseignement pénitentiaire* (National Intelligence and Counter-Terrorism Coordination, Counter-Terrorism Coordination Unit, National Prison Intelligence Service)	Paris
13 September 2019	*De politionele omgang met geesteszieken en suïcidalen* (The police treatment of mentally ill and suicidal persons)	Standing Committee P	Brussels
8-9 October 2019	International Intelligence Oversight Forum (IIOF 2019)	UN High Commissioner for Human Rights	London
2-3 December 2019	Working Visit	MI5	London
12-13 December 2019	European Intelligence Oversight Conference 2019	Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten (CTIVD)	The Hague

Very regular briefings are also organised during which various experts inform the Committee about current and important topics within the intelligence community (e.g. the relationship between the intelligence services and the Directorate of judicial police operations (Director-General Eric Snoeck), about the strategic vision for Belgian Defence (CHOD Marc Compernol), about the establishment of the Joint Intelligence Centres and Joint Decision Centres[193] (Prosecutor-General Johan Delmulle)). These briefings are meant to promote an informed discussion about the functioning, powers and oversight of the intelligence and security services, CUTA on the one hand and the intelligence work on the other hand.

[193] A Joint Intelligence Centre (JIC) must allow the services involved (both intelligence services, CUTA and the Federal Judicial Police) to hold weekly meetings on new operational information, priorities and the division of tasks. The Joint Decision Centre (consists of the services mentioned supplemented by the Federal Public Prosecutor's Office) decides, based on the JIC's common perception, which service will be entrusted with further investigation. The strict separation between the police, intelligence services and justice is thus abandoned and replaced by a circular and collegial approach. See *Parl. Doc.* Chamber of Representatives, 2017-18, no. 54K1752/008, p. 58.

CHAPTER XI.
RECOMMENDATIONS

On the basis of the review investigations, controls and inspections concluded in 2019, the Standing Committee I – in some cases with the Supervisory Body for Police Information – has formulated the following recommendations. These relate to the protection of the rights conferred on individuals by the Constitution and the law, the coordination and efficiency of the intelligence services, CUTA and the supporting services, as well as the optimisation of the review capabilities of the Standing Committee I.

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

XI.1.1. ANNOUNCEMENT OF A ROYAL DECREE ON INTERCEPTIONS

Article 44/4 of the Intelligence Services Act states that the Committee, '*irrespective of the other powers conferred on it on the basis of the Act of 18 July 1991, has the right to stop ongoing interceptions, intrusions or image recordings if they are found to breach the legal provisions or the [ministerial] permission. It shall order that the data obtained unlawfully may not be used and must be destroyed in accordance with the more detailed rules to be determined by the King.*' (free translation). Article 44/5 of the Intelligence Services Act (mandatory cooperation of an operator) also requires an implementing decree. However, the Royal Decrees referred to here have not yet been issued. The Standing Committee I urges (again) that this be done as soon as possible.

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

XI.2.1. VARIOUS RECOMMENDATIONS FOLLOWING THE REVIEW INVESTIGATION INTO SECURITY SCREENINGS[194]

XI.2.1.1. Coherent and simplified screening legislation

Screening legislation is complex and diverse. The Standing Committee I recommends that the legislator should make this legislation more coherent and simple. The content and purpose of each screening must also be clearly stated. The legislator must also determine in which cases an additional intelligence investigation should be allowed. It is also appropriate to clarify the circumstances in which intelligence services may obtain additional information about the person who is the subject of a verification. This could be necessary, for example, to update or contextualise existing data.

XI.2.1.2. Agreements with public services that receive decisions by the Appeal body

The Standing Committee I recommends that both intelligence services make the necessary arrangements with public services that receive Appeal body decisions on security screenings, so they can also take note of these decisions. In this way, both services can analyse the case law and consider it when carrying out future screenings.

XI.2.1.3. Consulting on the purpose of screening

The Standing Committee I recommends that State Security and GISS consult regularly with the various authorities/clients that receive their security advice or intelligence. This is to ensure that the intelligence provided satisfies the purpose of the requested screening.[195]

---

194 See Chapter I.1. ('Security screenings conducted by the intelligence services').

195 Which information is useful and should be communicated to the requesting authority in relation to which type of verification or screening (e.g. the interpretation of the concept of '*obstacle due to important facts, specifically related to the person*' in the context of a naturalisation procedure).

XI.2.1.4. Systematic inquiries at foreign partner services

The Committee recommends that the necessary human and other resources and procedures be provided, particularly to allow for systematic inquiries at foreign partner services if the security screening concerns a person who has resided abroad for a long time.[196]

XI.2.1.5. Setting up a registration and consultation system

The Standing Committee I recommends that State Security and GISS set up a case registration and consultation system. It is a consultation list that mentions which cases the services have investigated. This must allow for a systematic, central registration of all internal movements in a case file. It is also particularly important that there is centralised management of all responses transmitted by the service (e.g. also by the analytical services) to the authority/client concerned. This is necessary to ensure that any response times are respected and to ensure coherence in how communication with partners is conducted. It is also appropriate to retain and file all the documents of an original case file for the purpose of a screening. This is useful for conducting quality or other audits.

XI.2.1.6. Striving for uniform composition of case files

The way in which State Security and GISS process case files in the context of screenings also depends on external factors. One of these factors is how the case files to be processed are communicated to the services by the authorities/clients. The diverse (digital) composition of these files and any inaccuracies may influence/complicate how they are processed. The Committee recommends striving for uniform composition of files, and even integrating the various actors' ICT systems for the purpose of requesting and processing screenings. It also recommends creating a common platform, by analogy with requests for security clearances.

XI.2.1.7. Setting up an internal control system

The Standing Committee I recommends that State Security and GISS set up an internal control system, including determining performance and management indicators and implementing a sufficiently large and systematic sample to check and maintain the quality of the verifications.

---

196 The alternative is that State Security and GISS make clear arrangements on this with the National Security Authority (NSA) to leave making inquiries at foreign services up to the NSA.

XI.2.1.8. Greater automation of the requests

Greater automation of verification requests is also recommended. The ideal would be to develop an IT tool that allows automatic checking of names in a database.

XI.2.1.9. Creating a handbook

The Standing Committee I recommends that both State Security and GISS develop a handbook describing the internal procedure – including the information flow – and methodology for security verifications and screenings.

XI.2.1.10. Improved integration of the Security Verifications Service in State Security's information management system

The Standing Committee I recommends improved integration of the Security Verifications Service in State Security's information management system. The documents prepared by this service must be available for consultation by other departments. A mechanism should also be set up that involves reporting and correcting inaccuracies that the Security Verifications Service detects in State Security's database. It is crucial to develop a flagging system in the database by which all persons known in the database who are or have been the subject of a security verification are identified as such. In this way, all departments can be aware of these persons, and new, relevant information relating to them can be brought to the departments' attention. If necessary, a new security advice can then be communicated to the authority concerned.

XI.2.1.11. Framework of the security screenings assignment at GISS

The Standing Committee I believes that GISS handles the security verifications and screenings assignment poorly and that it is not properly framed by the hierarchy. A clear hierarchical line, including a clearly defined person with ultimate responsibility, must be established for this purpose.[197]

XI.2.1.12. Verifications in all GISS databases

The Committee recommends that the Screening Unit at GISS must be allowed to conduct verifications in all GISS databases. GISS must also take the necessary

[197] GISS's proposed solution is to integrate the Screenings Unit within the DISCC coordinating body. The question is whether this adequately resolves the existing ambiguity relating to hierarchical responsibility. In the Committee's opinion, it is problematic that the Screening Unit operates independently of the S Directorate.

measures to ensure that all databases used in the service are adequately 'fed' with relevant information and that this also happens promptly.

XI.2.1.13. Keeping figures on completed security screenings

The Committee recommends that GISS should soon start keeping figures on the number of security verifications completed and yet to be carried out. The purpose of this exercise is to be able to regularly assess the workload and the feasibility of response times. In this way, trends can be recognised, an increase in the number of queries can be anticipated and, if necessary, additional human and other resources can be arranged. These figures are best grouped by type of verification (statutory basis).

XI.2.2. RECOMMENDATIONS FOLLOWING THE REVIEW INVESTIGATION INTO CARLES PUIGDEMONT[198]

XI.2.2.1. Adapting the Directive on international cooperation

As for cooperation with foreign intelligence services, the Standing Committee I recommends that the National Security Council's directive be adapted and updated. This Directive should specify the content of the intelligence exchanged with foreign services and consider Part III of the Act of 30 July 2018 on the protection of individuals with regard to the processing of personal data, which has specific provisions for processing of personal data by intelligence and security services, in particular specific terms depending on whether the service concerned is a European service.

XI.2.2.2. Concluding a cooperation agreement between GISS and State Security

As for the division of tasks regarding the collection, analysis and processing of intelligence relating to the activities of foreign intelligence services on Belgian territory, the Standing Committee I recommends that the National Security Council should adopt guidelines, and that a cooperation agreement should be concluded between State Security and GISS under Article 20, § 4 of the Intelligence Services Act.

198 See Chapter I.5. ('Puigdemont and possible activities by foreign intelligence services in Belgium').

XI.2.2.3. Preparing a list of foreign intelligence and security services

As for the nature of the foreign services, the Standing Committee I recommends that State Security and GISS draw up a list of foreign services that could be classified as 'an intelligence and security service', by analogy with its recommendation relating to the investigation into the international contacts of CUTA.[199]

XI.2.2.4. Developing a common methodology on threat assessment

As for the threat assessment, the Standing Committee I recommends that State Security and GISS adopt a common methodology, inspired by State Security's methodology, which allows measures to be taken in relation to credibility, possible actions and proportionality after a risk analysis. Among other things, such methodology must also allow for:

- guaranteeing the traceability of documents and decisions with a view to *a posteriori* review by the Standing Committee I;
- ascertaining that the intelligence service informs the competent minister of its decisions and adopted measures.

XI.2.3. RECOMMENDATIONS FOLLOWING THE REVIEW INVESTIGATION ON THE FUNCTIONING OF GISS'S HUMINT DEPARTMENT[200]

XI.2.3.1. Recommendations for managing and planning intelligence activities

The Standing Committee I recommends:

- that GISS shows in the different plans why countries or themes are assigned a certain priority level, by explicitly referring to national or international interests;
- standardising the use of the various management documents, the Intelligence Steering Plan, IntelFocus and the Intelligence Collection Plans. Where necessary, any differences in these management documents must be explicitly justified (for example, why countries in one plan are considered priorities but not in another plan);
- that the Intelligence Collection Plans within GISS's Intelligence Directorate have a fixed and uniform structure for all collection services (including I/H) and are continuously updated;

199 STANDING COMMITTEE I, *Activity Report 2015*, 175-177.

200 See Chapter I.2. ('Examining the functioning of the HUMINT Department at the Military Intelligence Service').

– assessing the use of resources of GISS's various collection services to identify any gaps and determine which threats or priorities require attention and resources. This overview would make it possible to ultimately optimise and complement the collection services;
– that GISS evaluates the sources (specific, permanent or periodic, depending on the situation), to check whether they are being used in line with the priorities;
– ensuring that the human intelligence of its various collection bodies, including I/H, are jointly coordinated and managed. The Standing Committee I also recommends filtering existing sources to free up capacities and recruiting new sources, thus ensuring a certain evolution/renewal;
– ensuring the monitoring, evaluation and updating of the various management documents, the Intelligence Steering Plan, IntelFocus and the Intelligence Collection Plans.

XI.2.3.2. Recommendations for the resources of the I/H Department

Once managing and planning the I/H Department's intelligence activities are defined (in addition to GISS's other collection services), resources need to be allocated. As for the organisation chart and allocation of personnel, the Standing Committee I has identified several problems that GISS should inform the Minister of Defence about so investments can be made. The Committee therefore recommends:
– analysing personnel requirements[201], drawing up a forward-looking organisation chart, and updating the staffing level of the service based on the needs of a service that manages human intelligence in the context of assignments such as those of GISS;
– limiting the staff turnover within the I/H Department;
– it also reiterates that developing a new 'intelligence' branch in Defence or detailing alternative solutions might help attract staff specialised in intelligence and develop their careers. The Committee refers to its earlier recommendations.[202]

XI.2.3.3. Recommendations for source management and procedures

Once managing and planning the intelligence activities are done and the resources are released to put everything into practice, processes and work procedures

[201] This includes considering the number of sources a Case Officer can manage and the support they need. This requires cooperating with the Defence HR specialists and benchmarking with other services that are given the same assignments.
[202] See STANDING COMMITTEE I, *2011 Activity Report*, p. 104 and 174, *Activity Report 2018*, p.132-133, Recommendations on personnel management and on careers, education and training.

need to be developed. The Standing Committee I emphasised that using human intelligence for data collection (see Article 18 of the Intelligence Services Act) requires directives from the National Security Council.
The Standing Committee I noted that despite the absence of such a directive from the National Security Council at the time, most internal directives (standard operating procedures or SOPs) of the I/H Department were updated in 2018. Even so, the Committee recommends:

- that the I/H Department continue its efforts in evaluating sources and the intelligence bulletins they provide. As for the latter, I/H and the analytical services must establish a joint schedule to achieve the objective together;[203]
- implementing an internal control process, specifically to continuously monitor compliance with procedures, especially those implemented at I/H;[204]
- that the various directives/standard operating procedures (SOPs) be included in a classified handbook for personnel.

XI.2.4. RECOMMENDATIONS CONCERNING THE COMMON DATABASES

XI.2.4.1. Assessing conflicts of interest and time spent by the Data Protection Officer

Given the different roles that the DPO in the CDB TF and HP combines, and in view of a forthcoming review by the Oversight Body for Police Information and the Standing Committee I, it is important to clearly assess any conflicts of interest and the time spent on the tasks that the common database's DPO is supposed to fulfil.

XI.2.4.2. Monitoring the 'need to know' principle

Given the imminent expansion of the number of partner services that will have direct access to the CDB TF and HP, it is important that the CDB TF and HP's DPO closely monitors the extent to which feeding the database by the various partner services could overlap, and the extent to which such overlap violates the 'need to know' principle. Services with direct or indirect access to the CDB TF and HP must have a 'need' to access it when making decisions that fall within their remit.

---

[203] The responsibility for evaluating the source lies with I/H itself, knowing that it depends on the evaluation of the intelligence bulletins and feedback from the analysis services for which the information is ultimately intended. Reorganising the GISS at the beginning of 2020 would have resulted in all its collection services being brought together in one pillar and all analysis services in another, as opposed to the current situation in which these services are mixed. This reorganisation could be used to achieve the aforementioned objective. But the approach must be realistic in the sense that it must consider the available resources.

[204] The Standing Committee I recognises that this recommendation may seem unrealistic for lack of measurability.

In that context, it should be noted that a partner service (with the exception of the Public Prosecution Service) must make the necessary effort to feed the database, and the aim should not be to provide direct write access to ensure in practice that one service with write access would enter the relevant information in the CDB TF and HP.

XI.2.4.3. Taking action in response to security incidents

The standard procedure for security incidents must be adequately communicated to the services concerned so they are not only aware of its existence but also of how it works. In addition, the Oversight Body for Police Information and the Standing Committee I should be (more quickly) informed and (more closely) involved in such incidents. Both 'minor' and 'major' log checks should be carried out more systematically by all services involved. The operational manager holds a key position in this regard.

XI.2.4.4. Protocols on the transfer of mailing lists

The operational manager of the common database and the data protection officer must ensure that protocols are available under Article 44/11/3*quater* of the Policing Act that regulate the conditions for transferring mailing lists to third-party bodies. Due attention needs to be paid to prohibiting the further dissemination of these data. The preparation of these protocols will be followed up in a subsequent report.

XI.2.4.5. Evaluating direct access for partner services

As for partner services that have specified no user or logins for the CDB TF and HP for several years, the Oversight Body for Police Information and the Standing Committee I point to a possible lack of the 'need to know' and the need to evaluate to what extent the conditions of Article 44/11/3*ter* §2 of the Policing Act are still fulfilled in future. Direct access of certain partner services might need to be reviewed after this evaluation.

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

XI.3.1. ACCURATE INFORMATION ON THE FUNCTIONING OF THE COMMON DATABASES

The Supervisory Body for Police Information and the Standing Committee I must be kept more closely informed of policy decisions, consultations between the services involved, annual and other periodic reports, as well as meeting reports concerning the CDB TF and HP and its functioning.

APPENDICES

18 JULY 1991
ACT GOVERNING REVIEW OF THE POLICE AND INTELLIGENCE SERVICES AND OF THE COORDINATION UNIT FOR THREAT ASSESSMENT
(*extract updated in April 2020*)

CHAPTER I – GENERAL PROVISIONS

Article 1
Both a Standing Police Services Review Committee and a Standing Intelligence Agencies Review Committee shall be established. In particular, review shall relate to:

1° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the police services on the one hand and the intelligence and security services on the other;
2° The protection of the rights conferred on individuals by the Constitution and the law, as well as the coordination and effectiveness of the Coordination Unit for Threat Assessment;
3° The way in which the other supporting services satisfy the obligation laid down in Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

An Investigation Service shall be established for each of these committees.

Art. 2
The review governed by this Act does not relate to judicial authorities nor to the actions taken by them in the exercise of the prosecution function. The review does not relate to the administrative police authorities either.

The review referred to in this Act is governed without prejudice to the review or inspection governed by or by virtue of other legislation. In the event of review or inspection governed by or by virtue of other legislation, the review referred to in this Act relating to the activities, methods, documents and directives of the police services and of the intelligence and security services, shall only be undertaken to ensure fulfilment of the assignments provided for in this Act.

Art. 3
For the purposes of this Act, the following definitions shall apply:

1° "Police services": in addition to the local police and the federal police, the services that come under the authority of the public authorities and public interest institutions, whose members have been invested with the capacity of judicial police officer or judicial police agent;
2° "Intelligence and security services": State Security and the General Intelligence and Security Service of the Armed Forces;
3° "Coordination Unit for Threat Assessment": the service referred to in the Act of 10 July 2006 on threat assessment;
4° "Other supporting services": the services other than the police services and the intelligence and security services referred to in this Act, that are required, in accordance with the Act of 10 July 2006 on threat assessment, to pass on information to the Coordination Unit for Threat Assessment;
5° "Threat Assessment Act": Act of 10 July 2006 on threat assessment;
6° "Data Protection Act": Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data;
7° "Data Protection Authority": a supervisory authority for the processing of personal data.

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 supporting service, nor another data protection authority, nor the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services.

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 supporting services.

In this chapter, "the competent authority" shall mean the director of the Coordination Unit for Threat Assessment.

Subsection 3 – Assignments

Art. 32
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, or at the request of another data protection authority.

When the Standing Committee I acts on its own initiative as part of the activities and methods referred to in article 33, first paragraph, it shall forthwith inform the Chamber of Representatives thereof.

Art. 33
Within the framework of the objectives laid down in Article 1, the Standing Committee I shall investigate the activities and methods of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services, their internal rules and directives, as well as all documents regulating the conduct of the members of these services.

The Standing Committee I also controls the processing of personal data by the intelligence services and their processors.

The intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services shall, on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services. The Standing Committee I and the Investigation Service for the intelligence services shall have the right to be provided with all texts that they consider necessary for the performance of their assignment. The Standing Committee I may, based on a reasoned request of its Chairman, request the administrative authorities to provide it with the regulations, guidelines and documents issued by these authorities which the Committee considers essential for the performance of its assignment. The concerned administrative authority has the right to assess whether it is relevant to communicate the requested regulations, guidelines and documents to the Standing Committee I.

The Standing Committee I shall provide the competent minister or the competent authority, as well as the Chamber of Representatives with a report on each investigation assignment. This report shall be confidential until its communication to the Chamber of Representatives in accordance with Article 35.

This report shall include the conclusions relating to the texts, activities or methods that could jeopardise the objectives laid down in Article 1.

The competent minister or the competent authority may, with regard to the investigation reports, hold an exchange of views with the Standing Committee I. The Standing Committee I may itself propose that such an exchange of views be held.

The competent minister or the competent authority shall inform the Standing Committee I within a reasonable period of time of his/its response to its conclusions.

Unless required by law, the Standing Committee I may only advise on a Bill, Royal Decree, Circular Letter, or any documents expressing the political orientations of the competent ministers, at the request of the Chamber of Representatives, or the competent minister.

When the Standing Committee I acts at the request of the competent minister, the report shall only be submitted to the Chamber of Representatives at the end of the term laid down in accordance with Article 35, § 1, 3°. The Chairman of the Monitoring Committee concerned referred to in Article 66bis shall be informed of the request of the minister to the Standing Committee I and of the content of the report before the end of the term laid down in Article 35, § 1, 3°.

Art. 34

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

The Standing Committee I also processes requests relating to personal data by the intelligence services and their processors.

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, the denunciation or lodged the request.

When the investigation is closed, the results shall be communicated in general terms, except in the case of investigations relating to the processing of personal data by the intelligence services and their processors. The Standing Committee

I shall merely inform the complainant that the necessary verifications have been made.

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

Art. 35

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

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the Chamber of Representatives and the Senate, and to the competent ministers by 1 June at the latest. In this report, the Standing Committee I shall pay special attention to the specific and exceptional methods for gathering information, as referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, as also to the application of Chapter IV/2 of the same Act and to the implementation of the Act of 10 July 2006 on threat assessment.

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

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

§ 2. The Standing Committee I shall present a report 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.

§ 3. The Standing Committee I shall present an annual report annually to the Chamber of Representatives regarding the advice provided as a data protection authority on the investigations conducted and the measures taken in this quality

and regarding its collaboration with other data protection authorities. A copy of this report will also be provided to the competent ministers as well as State Security, the General and Security Service which are entitled to draw the attention of the Standing Committee I on their remarks.

Art. 36
In order to prepare its conclusions of a general nature, the Chamber of Representatives may request the Standing Committee I to provide each and every investigation dossier, according to the terms and conditions that they determine and which in particular aim to safeguard the confidential nature of these dossiers and to protect the privacy of individuals. If the investigation was initiated at the request of a competent minister, his consent shall be required before handover of the investigation dossier, unless the term laid down in Article 35, § 1, 3° has expired.

Art. 37
After acquiring the advisory opinion of the competent ministers or the competent authority, the Standing Committee I shall decide, within a period of one month from the request for advice, to make public all or part of its reports and conclusions, according to the terms and conditions it stipulates.

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

Art. 38
The prosecutor-general and the auditor-general shall ex-officio send to the Chairman of the Standing Committee I a copy of the judgments and judicial decisions relating to the crimes or offences committed by the members of the intelligence services and the Coordination Unit for Threat Assessment.

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

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

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

The copies shall be delivered without charge.

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

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

SECTION 2 – THE INVESTIGATION SERVICE FOR THE INTELLIGENCE SERVICES

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

It shall examine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another supporting service. Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

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

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

Art. 41
A person may not be appointed Head of the Investigation Service I if he has not been a magistrate or a member of an intelligence or police service for a period of

five years, or if he cannot demonstrate at least five years' relevant experience as a public servant in positions relating to the activities of the intelligence or police services. At the time of his appointment he must have attained the age of 35 years.

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

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

He must have knowledge of the French and Dutch languages.

He shall retain his right to advancement and salary increase.

He may be dismissed by the Standing Committee I.

Art. 42

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

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

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

Art. 43

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

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

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

Art. 44

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

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

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 apart from the cases referred to in article 13/1 of the Act of 30 November 1998 governing the intelligence and security services and those referred to in articles 226, 227 and 230 of the Data Protection Act, 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.

When a member of the Investigation Service I learns of an offense referred to in articles 226, 227 and 230, he shall inform the Standing Committee I as soon as possible. The latter shall follow it up within the procedures established.

Art. 47

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

SECTION 3 – INVESTIGATION PROCEDURES

Art. 48

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

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

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

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

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

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

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

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

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

Art. 49

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

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

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

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

SECTION 4 – POWERS OF THE STANDING COMMITTEE I AS DATA PROTECTION AUTHORITY

Art. 51/1
As data protection authority, the Standing Committee I acts either on its own initiative, or at the request of another data protection authority, or at the request of any data subjects.

Art. 51/2
To be admissible, the request is written, dated, signed and reasoned, and justify the identity of the person concerned.

Art. 51/3
In the follow-up of the cases, the Standing Committee I has the authority to:

1° conclude that the processing is carried out in accordance with the provisions of the regulations relating to the processing of personal data;
2° warn the service concerned or its processors that an intended processing of personal data is likely to violate the regulations relating to the processing of personal data;
3° call to order the service concerned or its processors when processing has resulted in a violation of a provision of the regulations relating to the processing of personal data;
4° order the service concerned or its processors to bring processing in accordance with the provisions of the regulations relating to the processing of personal data, where appropriate, in a specific manner and within a specified period;
5° impose a temporary or permanent limitation, including a ban, on processing;
6° order the rectification or erasure of personal data;
7° forward the case to the Brussels public prosecutor's office, who informs him of the actios taken on the case.

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

Art. 52
The Standing Committees shall exchange information on their activities and send each other the reports and conclusions referred to in Articles 9, 11, 33 and 35.
At least twice a year, they shall hold joint meetings, during which additional information may be exchanged.

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

1° With regard to the public services that perform both police and intelligence assignments;
2° With regard to the division of the assignments and the coordination of the operation between the police services on the one hand, and the intelligence services on the other;
3° With regard to any question put to them, either by a joint request from the ministers responsible for the Interior, Justice and National Defence, or at the request of the Chamber of Representatives;

4° With regard to any question that each Standing Committee believes does not fall within its exclusive competence;
5° With regard to any question considered by a Standing Committee to be sufficiently important to warrant a joint meeting;
6° With regard to the Coordination Unit for Threat Assessment or another supporting service.

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

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

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

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

CHAPTER V – COMMON PROVISIONS

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

The following are excluded from this allowance:

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

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.]

(…)

CHARTER OF THE INTELLIGENCE OVERSIGHT WORKING GROUP

1. MEMBERS OF THE EUROPEAN INTELLIGENCE OVERSIGHT GROUP

This Charter establishes the Intelligence Oversight Working Group, an informal cooperation between the following oversight bodies:

Belgian Standing Intelligence Agencies Review Committee, *Comité permanent de contrôle des services de renseignement et de sécurité /Vast Comité van Toezichtop de inlichtingen- en veiligheidsdiensten* (Belgium);

Danish Intelligence Oversight Board, *Tilsynet med Efterretningstjenesterne* (Denmark);

Review Committee on the Intelligence and Security Services, *Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten* (The Netherlands);

EOS Committee - The Norwegian Parliamentary Intelligence Oversight Committee, *EOS-utvalget* (Norway);

Independent Oversight Authority for Intelligence Activities (OA-IA), *Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND* (Switzerland);

Investigatory Powers Commissioner's Office, (United Kingdom).

2. PURPOSES OF THE INTELLIGENCE OVERSIGHT WORKING GROUP

The Intelligence Oversight Working Group aims to:

- strengthen cooperation between the participating oversight bodies;
- increase transparency between oversight bodies within the limits and according to the standards set by national legislators, in order to support effective oversight of international cooperation between intelligence and security services;
- exchange knowledge, experiences and best practices of oversight;
- provide a platform for developing new and/or more effective oversight methods;
- maintain contact, share information and provide each other with mutual assistance as appropriate, in accordance with the boundaries set by national laws and regulations.

3. MEETINGS

a) Chair meetings

The Intelligence Oversight Working Group shall annually hold at least one meeting between the chairs of the oversight bodies, or a member of the oversight body representing the chair. In principle, each chair will be supported by their head of secretariat and/or another senior staff member.

b) Staff meetings

The intelligence Oversight Working Group shall regularly, when appropriate, hold staff meetings. The staff meetings are aimed at practically substantiating the purposes referred to in Section 2 of this Charter and carrying out the cooperation projects referred to in Section 4 of this Charter.

c) Preparation of meetings

Chair meetings shall be prepared by the oversight body hosting the meeting in cooperation with the informal secretariat referred to in Section 5 of this Charter. Staff meetings shall be prepared by the oversight body hosting the meeting. All Members voluntarily contribute to hosting meetings on a rotation basis.

4. COOPERATION PROJECTS

The Intelligence Oversight Working Group may decide to enter into cooperation projects. Cooperation projects relate to a specific interest of the Group. The decision to enter into a cooperation project will be taken during a Chair meeting on the basis of a project proposal. Project proposals are prepared at staff level and shall include at a minimum:

- the intended goals for the project;
- the proposed methods to reach those goals;
- the timeframe in which the project is to be carried out.

5. INFORMAL SECRETARIAT

The informal secretariat will be responsible for:

- reporting conclusions of the chair meetings;
- reporting conclusions of the staff meetings in cooperation with the oversight body that organised the respective meeting;
- monitoring progress on the cooperation projects;
- communication with regard to outside interest in the Group. The secretariat will rotate every two years.

6. INFORMATION EXCHANGE

The participating oversight bodies commit to facilitating information sharing within the Group to further the purposes referred to in Section 2 of this Charter, where appropriate and in accordance with the boundaries set by national laws and regulations. The nature and extent of information sharing within the Group may also be defined by or dependent upon bilateral and/or multilateral agreements between the intelligence and security services overseen by the participating oversight bodies.

7. MEMBERSHIP

Extending membership of the Intelligence Oversight Working Group to other European oversight bodies on their request, shall take place on the basis of a decision by consensus taken during a Chair meeting.

8. STATUS, IMPLEMENTATION AND AMENDMENT OF THE CHARTER

This Charter reflects the intent of the participating oversight bodies within the Intelligence Oversight Working Group. Each participating oversight body commits to implementing this Charter. Amendment of this Charter shall take place on the basis of a decision by consensus taken during a Chair meeting. This Charter is not legally binding.

Signed in The Hague on 12 December 2019,

Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board

Mr. Nico van Eijk, Chair of the Dutch Review Committee on the Intelligence and Security Services

Mr. Svein Grønnern, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

Mr. Thomas Fritschi, Director of the Swiss Independent Oversight Authority for Intelligence Activities

Sir Brian Leveson, Investigatory Powers Commissioner, United Kingdom