ACTIVITY REPORT 2018

ACTIVITY REPORT 2018

Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee

INTERSENTIA

Cambridge – Antwerp – Chicago

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

Activity Report 2018
Belgian Standing Intelligence Agencies Review Committee

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

Cambridge – Antwerp – Chicago
www.intersentia.com

ISBN 978-1-83970-020-0
D/2020/7849/65
NUR 823

TABLE OF CONTENTS

APPENDICES

LIST OF ABBREVIATIONS

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
CDB	Common database
CDB HP	Common database Hate Propagandists
CDB TF	Common database Terrorist Fighters
CHOD	Chief of Defence
CHODOPORDER	Operational Order of the Chief of Defence
CI	Counterintelligence
Classification and Security Clearances Act	Act of 11 December 1998 on classification and security clearances, certificates and advice
CNCTR	*Commission nationale de contrôle des techniques de renseignement* (France)
C.O.C.	Supervisory Body for Police Information
C-Ops	Operation Centre
CSA	Competent Supervisory Authority
CT	Counterterrorism
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten* (the Netherlands)
CUTA	Coordination Unit for Threat Assessment
Data Protection Act	Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data
DCAF	Geneva Centre for the Democratic Control of Armed Forces
DGA/DAO	Directorate of administrative police operations
DGJ/DJO	Directorate of judicial police operations
DGPI	Directorate-General for Penal Institutions
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
FDPIC	Federal Data Protection and Information Commissioner (Switzerland)
FPS	Federal Public Service
FragO	Fragmentary orders
FTF	Foreign Terrorist Fighter
GCCR	Governmental Coordination and Crisis Centre
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
IMINT	Image intelligence
Intelligence Services Act	Act of 30 November 1998 governing the intelligence and security services
IPCO	Investigatory Powers Commissioner's Office (United Kingdom)
IR	Intelligence requirements
IS	Islamic State
ISIS	Islamic State of Iraq and Syria
ISP	Intelligence steering plan
ISTAR	Intelligence, Surveillance, Target Acquisition & Reconnaissance
IT	Information Technology
JIB	Joint Information Box
KPI	Key performance indicator
LIVC-R	Local Integrated Security Unit relating to radicalism, extremism and terrorism
LTF	Local Task Force
MoU	Memorandum of Understanding
NA	*Note aux autorités*
NATO	North Atlantic Treaty Organisation
NGO	Non governmental organization
NSA	National Security Authority
NSC	National Security Council
NTF	National Task Force

OPSEC	Operations security
OR	Operational report
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
RD	Royal Decree
RD Classification and Security Clearances	RD 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 Act
RD HP	Royal Decree of 23 April 2018 on the common database for Hate Propagandists and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the 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
RIR	Information report
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
SLA	Service Level Agreement
SOP	Standard Operating Procedures

SRP	United Nations Special Rapporteur for Privacy
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*
TESSOC	Terrorism, Espionage, Sabotage, Subversion and Organised Crime
TF	Terrorist Fighter
Threat Assessment Act	Act of 10 July 2006 on Threat Assessment
UN	United Nations

INTRODUCTION

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

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

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

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

Since 1 September 2010, the Standing Committee I has 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 and the SIM actualisation Act of 30 March 2017 have 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,

1 About the Standing Committee I: 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.

and the Committee can request any other text or document. The fact that many documents of the intelligence services are classified in accordance with the Classification Act, 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.

In the last few years the Standing Committee I has been confronted with the need to include existing assignments further (issuing opinions) and there are numerous statutory provisions under which the Committee has been given a new assignment: inspecting common databases (terrorist fighters, hate propagandists), monitoring certain assignments of the ISTAR battalion, monitoring how GISS makes images recordings and penetrate IT systems abroad, stricter monitoring of certain ordinary methods, monitoring how the intelligence services operate within the Passenger Information Unit and controlling how they use certain camera images.

Last but not least, under the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, the Standing Committee I has become the Data Protection Authority for almost all personal data related to national security. In that role, the Committee has to deal with individual requests but also to issue opinions and enter into protocols with other Data Protection Authorities.

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). Since 2006, with increased globalisation in mind, the Standing Committee I has strived to meet the expectations of a broader public by translating into English the sections of its activity reports that seemed most relevant to the international intelligence community (i.e. the review investigations, the control of special and certain ordinary intelligence methods and the recommendations). As a result seven books have been published in English so far (the *Activity Report 2006-2007,* the *Activity Report 2008-2009,* the *Activity Report 2010-2011, the Activity Report 2012-*

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

2013, Activity Report 2014-2015, the Activity Report 2016 and the Activity Report 2017 (also available on www.comiteri.be).

Given the new assignments that have been entrusted to the Standing Committee I, and of which report is made in its Activity Report 2018, 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 other new feature is the format in which the activity report is presented. The report will only be available in pdf format and can still be consulted on www.comiteri.be.

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

28 August 2019

CHAPTER I
REVIEW INVESTIGATIONS

In 2018, the Standing Committee I finalised five review investigations (I.1 to I.5). It also opened three new investigations in the course of the year. Two of the completed investigations had been started on its own initiative; in one investigation the Minister of Defence had made a referral to the Committee (under Article 32 of the Review Act)[4] and two investigations – including one in conjunction with the Standing Committee P – were carried out at the request of the Parliamentary Monitoring Committee. A brief description of the investigations still in progress and/or started in 2018 follows in I.6. The recommendations made following the review investigations have been collected together in Chapter XII.

The Committee received a total of 72 complaints or reports in 2018. Efforts to streamline, deformalise and standardise the 'complaints and reports' work process started in 2016.[5] If necessary after a brief preliminary investigation and after verifying some objective information, the Committee rejected 68 complaints or reports because they were evidently unfounded (Article 34 of the Review Act) or because the Committee did not have jurisdiction for the matter in question. In the latter cases, the complainants were referred, wherever possible, to the competent authorities (Standing Committee P, the Federal Police, the Public Prosecutor or other bodies). One complaint resulted in a review investigation (I.5), two complaints were added to an ongoing investigation (I.1), and, in view of the two committees' shared competence, notice of the complaint relating to the operations of CUTA was given at the end of 2018 to the Standing Committee P for joint consideration.

Besides review investigations, the Standing Committee I opens 'information dossiers', which must allow to provide a response to questions about how the

---

4 It is rather exceptional for the Committee to receive a referral from a member of the executive power. In this regard, see: VAN LAETHEM, W. and VANDERBORGHT, J., 'Torture numbers, and they'll confess to anything. Een analyse van twintig jaar toezichtonderzoeken, studies en adviezen' in VAN LAETHEM, W. and VANDERBORGHT, J. (eds.), *Inzicht in toezicht*, Antwerp, Intersentia, 2013, 266.

5 The admissibility of the complaint is first examined, after which it is processed by the Investigation Service I. For issues of a general nature, the Committee may decide to open a review investigation. Otherwise the inquiry remains limited to the complaint *per se* (a complaint inquiry).

intelligence services and CUTA operate.[6] Where such dossiers reveal indications of dysfunctions or aspects of the operations of the intelligence services that require 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. In 2017, an information dossier was opened on the deployment of GISS intelligence capacity in a conflict zone, which resulted in a review investigation being opened in 2018 (I.3).

Finally, briefings are also organised on a very regular basis at which members of the intelligence services inform the Committee about important topics within the intelligence community (e.g. the Belgian Passenger Information Unit (BELPIU), the use of special intelligence methods, etc.). Those briefings must promote informed discussion about the operations, powers and oversight of the intelligence and security services and CUTA. They can also lead to the opening of an investigation.

I.1. OPERATIONS OF THE COUNTERINTELLIGENCE (CI) DIRECTORATE OF GISS

I.1.1. 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 of mid-December 2016 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[7]; it was completed in February 2018. 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

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

7 The Committee conducted a similar audit on a previous occasion: STANDING COMMITTEE I, *Activity Report 2011*, 99–106 ('II.1. Audit of the military intelligence service') and 172–175 ('IX.2.1. Recommendations with regard to the audit of the GISS').

organisation and management that meets the standards of an effective and efficient public service. The investigation showed that these standards were not being met.

I.1.2. STATUTORY AND NON-STATUTORY DUTIES OF THE CI DIRECTORATE

I.1.2.1. Ambitions, mission and vision with regard to counterintelligence

In an internal document from 2012, the ambition of what was then called the CI Division was described as follows: '*In order to counteract any threat, the CI Division must be responsible for identifying, preventing and neutralising any activities that may be carried out by foreign intelligence services, by other organisations or by individuals in connection with terrorism, espionage, sabotage or subversion (TESS) and that could pose a threat to the interests of the Armed Forces in the broadest sense of the term – its personnel, its infrastructure, its plans and operations worldwide – or those of its military partners in Belgium*' (free translation).

The vision was also presented in the same document: '*Be able to prevent all threats to all Defence-related matters.' 'The CI Division must be capable of counteracting any realistic threat to which vital defence interests may be exposed. The CI Division must be able to operate in complete DISCRETION. This applies to knowledge of its structure, modus operandi, personnel and resources. The performance of operations and duties must be PROTECTED*' (free translation).

This ambition and vision were translated into strategic objectives in the 'Security Information Steering and Security Action Plan 2015–2018'[8]: '*The CI department must be capable, in the context of the duties and resources provided for in legislative texts, of realistically counteracting any threat to which vital defence interests may be exposed. In addition, the CI department must be capable of meeting existing commitments and agreements with partner agencies, in particular in the context of cooperation with the intelligence services, the police services and the judiciary. The CI department must also be capable of assisting its foreign military partners on Belgian territory in the field of counterespionage*' (free translation). Five priorities were also defined in the same plan.

This ambition, mission and vision derive from NATO doctrine and are based on Belgian legislation.

---

8 SGRS, Plan Directeur du renseignement de Sécurité et d'Actions Sécuritaires 2015–2018. Révision 2016 – Veiligheidsinlichtingen Stuur- en Veiligheid Actieplan 2015–2018. Revision 2016, SECRET (Act of 11 December 1998), 1 March, 2016, 11. This was a revision of a plan drawn up earlier in 2016. This passage was declassified by the service.

I.1.2.2. NATO doctrine

In 2014, NATO provided unambiguous definitions in a standardisation agreement (STANAG) of the terms used in the context of its activities.[9] From then on, counterintelligence was understood to mean:

- *'Counter Intelligence (CI organizations, military or civilian, of the member nations including Law Enforcement Organizations) of the Alliance are responsible for counteracting the threat to security posed by hostile intelligence services and subversive, criminal or terrorist groups or individuals.*
- *Counter-intelligence includes those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion or terrorism. […] (2) The main thrust of the CI effort is to protect personnel, information, plans and resources, both at home and when deployed. It aims to provide knowledge and understanding of the prevailing situation to keep privileged information secret, equipment secure and personnel safe. CI should be proactive and preventative in its approach. (3) CI is an intelligence function that provides commanders at all levels with a detailed understanding of threats, vulnerabilities and risks to enable them to make well-educated decisions on security measures. In reality, there are likely to be compromises between what is needed and what is feasible.'*

The same NATO document returns to the specific role of counterintelligence: '*to ensure successful military operations the commander should deny the adversary the opportunity to conduct terrorism, espionage, subversion, sabotage, organized crime or computer network attacks against friendly force. To achieve this requires identification of friendly force's vulnerability to an adversary's intelligence gathering operations. This information is used to inform OPSEC, counter surveillance and deception planning including Protective Security Policy*'.

In two other documents, from 2001 and 2016 respectively[10], a description was given of the mission of CI divisions within the national military intelligence services. Their mission consists of identifying and counteracting espionage, sabotage and threats of terrorism and subversion against NATO and the coalition partners. For some nations, it also includes protecting against threats from organised crime, fundamentalism, extremism and intelligence operations (of foreign countries).

---

9 NATO Standardization Office (NSO), STANAG 2190. Allied Joint Doctrine for intelligence, counter-intelligence and security, Edition 2, September 2014 (NSO(JOINT)1165(2014) JINT/2190, 7–2).

10 NATO's 'Allied Joint doctrine for Intelligence, Counterintelligence and Security (AJP 2(A) (February 2016)' and 'AJP 2.2 '(Restricted) Counter-intelligence and Security Procedures' (November 2001).

I.1.2.3. Belgian legislation

Counterintelligence is not explicitly mentioned in the Act of 30 November 1998. However, a number of tasks can be understood from Article 11 of the Intelligence Services Act as duties of a counterintelligence nature. Likewise, the Royal Decree of 21 December 2001[11], which determined the general structure of the Ministry of Defence and the powers of certain authorities, did not define the concept of counterintelligence nor mention a Counterintelligence Directorate. The same applies to the Royal Decree of 4 July 2014, which determines the status of part of the civilian personnel of GISS.[12]

I.1.3. CI DUTIES IN PRACTICE

I.1.3.1. CI in Belgium and abroad

Originally, the CI Directorate focused on detecting military espionage activities – both by members of the Belgian armed forces and by foreign services – and countering subversion within Belgium. The concept of counterintelligence has come to be interpreted more broadly over the years and now includes what is known as 'TESSOC': Terrorism, Espionage, Sabotage, Subversion and Organised Crime. The CI Directorate also considers its remit to include identifying TESSOC phenomena within its own service (GISS). There is a certain logic to this, as a national military intelligence service can be an important target for infiltration by other, foreign intelligence services.

As a result of the increasing deployment of Belgian troops abroad and in the context of NATO cooperation, the Directorate was entrusted from 2012 with a so-called 'CI in Ops Zone' role, involving the sending of CI personnel abroad in support of Belgian troops deployed there in order to counter local military espionage and forms of organised crime, such as prostitution and drug dealing, that can lead to infiltration or the subversion of individual military personnel. This role, which is usually referred to as 'force protection', also has a statutory basis in Article 11 of the Intelligence Services Act.

---

11 The Royal Decree of 21 December 2001 determining the general structure of the Ministry of Defence and the powers of certain authorities, *Belgian Official Journal*, 12 January 2002. This Royal Decree was superseded by the Royal Decree of 2 December 2018. There too, the concept of counterintelligence is not defined and there is no mention of a Counterintelligence Directorate.

12 The Royal Decree of 4 July 2014 determining the status of certain civilian officers of the staff department for intelligence and security of the Armed Forces, *Belgian Official Journal*, 18 July 2014.

I.1.3.2. Counterterrorism and the powers of GISS

The Standing Committee I has already previously noted that the rise of (mainly Islamist) terrorism was having a considerable influence on the functioning of the Belgian intelligence services, including GISS and the CI Directorate. The changed characteristics of terrorism (more cross-border networks and activities, etc.) led to a mixing of tasks and responsibilities, in terms of both territoriality (domestic versus foreign) and dimensions in need of monitoring (civilian versus military). The Standing Committee I argued in this context for a thorough assessment of the way in which the military intelligence service in general and the CI Directorate in particular were being led in a certain direction.[13]

The fact that terrorists started using heavy military-grade equipment[14] and were being run on military lines (with cells in Europe being controlled by the military leadership of IS from Syria/Iraq), and above all the attacks of March 2016 in Brussels and Zaventem, reinforced this development (the mixing of roles) even further. This was a pivotal period for GISS (and the CI Directorate). Its own powers, described as 'military' up to that point, were gradually being interpreted in broader – i.e. 'civilian' – terms by the service.

At a time when maximum cooperation was required from each service, the leadership did not, however, clearly examine whether GISS – and in particular the CI Directorate – actually felt called to provide such cooperation and, if it did, whether it could also offer clear added value, given the resources at its disposal.

This situation has therefore caused quite a few problems in recent years, including the taking up of resources, the fragmentation of powers within the service or the failure to take on certain roles or areas of competence, and the provision of technical assistance in judicial cases with limited added value.

In addition, in its role description the CI Directorate adhered to NATO rules, under which the fight against terrorism focuses on terrorism against military targets, primarily in an international context (e.g. in foreign operations zones). According to that view, terrorism that focused largely on civilian targets and that was historically mostly domestic in nature (e.g. the '*Cellules Communistes Combattantes*' and the '*Rote Armee Fraktion*') did not, in principle, fall within the scope of the military authorities, but within that of the civilian intelligence service (State Security).

---

13 GISS needs to retain its distinctive character (its 'military focus'). In this regard, see: STANDING COMMITTEE I, *Activity Report 2016*, 4 *et seq.* ('II.1. Issue of foreign terrorist fighters).

14 The fact that the terrorists who were in Europe had 'military' weapons at their disposal was an additional relevant point for consideration of the powers of GISS, given that Art. 11 §2, 1° of the Intelligence Services Act limits the competence of GISS to activities that threaten national territory or the population and are carried out '*with resources of a military nature*' (free translation).

The Committee therefore took the view that the counterterrorism mission needed to be clarified and that GISS, and in particular the CI Directorate, needed to explicitly establish, within the framework of existing policy, how far the military sphere extends, where the purely civilian sphere starts, and how the two relate to one another.

The Committee recommended that both internally (within GISS, within the CI Directorate and also vis-à-vis the I (Intelligence) Directorate) and externally (in relation to State Security, the Public Prosecutor's Office, CUTA and other agencies), GISS and the CI Directorate should work out an unequivocally supported position on what can and should be expected from the service, taking the available resources into account. Once the vision, ambition and strategy have been worked out, they must actually be adhered to, so that the service can show itself to be a valuable partner in Belgian anti-terrorism policy.

I.1.4. THE COUNTERINTELLIGENCE DIRECTORATE WITHIN GISS

GISS is managed by the Command (GISS/C), which is assisted by a staff and a secretariat. Until 2013, GISS – which employs both civilian and military personnel – was split into four divisions: A (Support), CI (Counterintelligence), S (Security) and I (Intelligence). CI and S were combined in 2013, and the A Division was closed down some time later. In 2017 a new reorganisation was then carried out: 'Divisions' became 'Directorates' and the S (Security) and CI (Counterintelligence) Directorates were separated again. Alongside the Intelligence Directorate, which had more of a foreign focus, a new Cyber Directorate was also established.

The Committee noted, however, that there was no uniform/single organisation chart of the CI Directorate: different versions were circulating in which clear terminology was not used (directorates, offices, departments, pillars, etc.). This made it impossible for CI personnel to gain a clear view of their own organisation and exactly who had responsibility for what.

I.1.5. THE INVESTIGATION'S FINDINGS

I.1.5.1. The (supposed) contrast between GISS and ACOS IS

The Committee found – again – that there was a great deal of uncertainty about the content and use of the names GISS and ACOS IS.[15] A large part of the personnel of the CI Directorate, including managers, believed that their

[15] ACOS IS is the acronym of 'Assistant Chief of Staff Intelligence and Security'.

directorate actually constituted 'GISS', while the other directorates (especially the I Directorate) were 'ACOS IS'. They also believed that the CI Directorate should be independent of the military structure of the Armed Forces. There was no legal or regulatory basis for this.

Much of the uncertainty and discussion about the role of the CI Directorate turned out to be due to the fact that the regulations refer to both the General Intelligence and Security Service (GISS) and the Staff Department for Intelligence and Security (ACOS IS). The duties of GISS are defined in the Intelligence Services Act (in particular Article 10), and the service falls directly under the authority of the Minister of Defence (Article 2 of the Intelligence Services Act). ACOS IS was mentioned in the Royal Decree of 21 December 2001 determining the general structure of the Ministry of Defence and the powers of certain authorities.[16] According to this decree, this service must provide intelligence support to defence operations (Art. 22–24), and is headed by the Assistant Chief of Staff Intelligence and Security, who reports to the CHOD (Chief of Defence). The decree also states the Assistant Chief of Staff and the head of GISS are one and the same person. However, the latter falls directly under the responsibility of the Minister of Defence, and GISS has a wider remit, defined in the Intelligence Services Act. The Committee expected the leadership of GISS and the CI Directorate to clear up this persistent terminological confusion.

I.1.5.2. Polarisation between civilian and military personnel

The Standing Committee I found that CI personnel felt that the CI Directorate occupies a 'special place' within GISS (see below) and has its own 'culture', as the nature of its duties requires the CI to conduct investigations which sometimes involve Armed Forces personnel (mainly soldiers); the personnel regard the directorate as an oversight body. This created the sense within CI that they were mistrusted by the other GISS directorates, as well as by other defence components, and that other entities did not understand the task and role of CI.

This mistrust, the lack of mutual understanding and the lack of information exchange between the CI and I Directorates led, among other things, to conflicts and undermined the possibilities for cooperation.[17] Moreover, there was an impression that the strong sense of solidarity among military personnel often put CI investigations in danger of being 'pulled' at an early stage. The Standing Committee I believed that this risk was not unreal, in view of a number of

16 This Royal Decree was superseded by the Royal Decree of 2 December 2018 determining the general structure of the Ministry of Defence and the powers of certain authorities, *Belgian Official Journal*, 18 January 2019. This decree changed nothing in the situation as regards the present investigation.

17 The Standing Committee I has raised this point for much longer: see STANDING COMMITTEE I, *Activity Report 2010*, 47–48 ('II.10 Information management by the military intelligence service').

incidents in very sensitive cases in which certain pieces of information or facts about the behaviour of GISS members were wrongly withheld from the CI Directorate. However, the reverse was also true: the CI Directorate kept certain information outside the military chain, with even the head of GISS not being informed at times.

The Committee believed that the CI closed itself off too much from the rest of GISS. An exaggerated tendency had arisen not to share certain information that was necessary for GISS to function properly. Significant in this respect is the fact that some CI personnel would rather see their Directorate operating outside GISS. The Committee felt that such a view might lead to standards and rules being applied within this directorate that differ from those in other parts of GISS. This would have the effect of jeopardising the coordination of the various intelligence activities.

I.1.5.3. Control and planning

As was the case in 2013[18], the Committee found that CI employees were not always aware of the precise intelligence goals on which they were supposed to focus. A number of essential management documents were lacking. As a result, there was a lack of clarity within the CI Directorate and in the workplace about their duties. The relationship between CI and other directorates was therefore somewhat problematic; there was a lack of consensus about the nature of its tasks.

I.1.5.4. Organisation and structure

The CI Directorate did not have an officially recognised and uniform/single organisation chart, the organisational table did not reflect the actual size of the workforce and various personnel members were performing duties that did not correspond with their position. Certain positions were found not even to be filled, and there was a lack of logistical support.

I.1.5.5. Nature of the output

The functioning of the various CI departments and offices was geared to operational intelligence work.[19] Work was mainly carried out in a reactive and *ad hoc* manner on specific cases, with little or no intelligence output being delivered at a strategic level. The Committee concluded that a redefining of the relationship

---

18 STANDING COMMITTEE I, *Activity Report 2013*, 101 ('II.1.3.3.5. Lack of clarity regarding the intelligence to be gathered'). The Committee I recommended that the '*GISS defines the connections that must be made between operational, tactical and strategic intelligence and the legal duties described in the Intelligence Services Act*' (*Ibid*., 169).

19 Operational analysis produces intelligence that is ready for use, i.e. immediately applicable in specific cases. Operational intelligence is usually also intended for internal use and has a tactical value. It contributes to the achievement of short-term objectives.

between collection and analysis (possibly accompanied by a restructuring within the CI Directorate and/or more broadly) was urgently required.

I.1.5.6. Provincial detachments

The provincial detachments – the local outposts of the CI Directorate – are responsible for collecting information (including through HUMINT), representing GISS at local level and maintaining relationships with local authorities and institutions and local units of the Armed Forces. Among the problems noted by the Standing Committee I were poor communication and feedback from headquarters, problems with direct access to the CI database, understaffing and lack of support. The nature of the relationship and interaction (in terms of coordination and division of tasks) between the provincial detachments and the national detachment was also unclear, with the two operating independently of each other. Finally, there was also a lack of consultation between the provincial detachments.

I.1.5.7. CI in Ops Zone

A special component of the CI Directorate is the CI in Ops Zone section.[20] Initially, GISS deployed combined teams to support operations: I Directorate and CI Directorate personnel worked together. Due to a shortage of personnel, the CI Directorate was unable to continue this arrangement. The I/Ops section took on the entire task and covered the aspects of 'force protection' in support of deployed troops. In 2012/2013, the CI Directorate again expressed the wish to be able to deploy personnel in operations zones. These personnel members were not integrated into the I/Ops structure, so as not to be assimilated with that detachment. However, the management of the CI Directorate did not initially permit personnel to be deployed permanently for these special duties. Eventually, two officers were released to permanently man this cell.

The Committee noted that the dual structure in operations was a source of tension.

I.1.5.8. Processes and methods: SOPs, workload measurement, KPIs and internal feedback

The Committee found that the Standing Operating Procedures (SOPs)[21] applicable to CI did not form a coherent whole and were not up to date: they did

20 NATO has developed guidelines on the deployment of national intelligence cells (such as BENIC). The guidelines state that these cells should, if possible, include national CI elements.

21 A standing (standard) operating procedure (SOP) is '*a set of instructions covering those features of operations which lend themselves to a definite or standardized procedure without the loss of effectiveness. The procedure is applicable unless ordered otherwise*' (NATO Glossary Terms and Definitions, AAP-6(V)).

not take account of the changed structure of CI or its changed statutory roles. CI attributed this to personnel shortages.

The Standing Committee I also found that the workload within the CI Directorate was not measured, analysed, managed or evaluated anywhere. The workload was not objectifiable either, due to a lack of the following: prioritisation, clear objectives, structure within the CI Directorate, job descriptions, procedures (or knowledge of them), management indicators and a benchmark to use as a reference point or gauge. In this regard, the Committee noted a lack of investment on the part of both the GISS command and the CI Directorate.

In addition, no standardised key performance indicators (KPIs)[22] had been developed within CI. However, analysis criteria had been determined, but they were almost exclusively qualitative and not quantitative.

Moreover, the Committee found that problems had arisen with internal communication management.

I.1.5.9. Processes and methods: managing tradecraft

Intelligence work requires the management of tradecraft.[23] This term covers 'the methods, techniques, technologies, procedures and basic principles established and used by the intelligence services in order to successfully carry out their duties and operations'.[24]

The Committee became aware of instances that indicated a lack of knowledge sharing about and understanding and joint implementation of tradecraft, and it was observed that there was a tension between the way in which CI looked at tradecraft and the way it was approached, for example, in the context of counterterrorism (CT): the need-to-know culture was in conflict with that of need-to-share.

I.1.5.10. Personnel management

Different employment statuses and workforce shrinkage

More than half of CI personnel are civilians, who can be divided into four different groups: permanent 'Auditors and Inspectors', who have a special career

---

22 A performance indicator is an indicator of efficiency or outcome (effectiveness) that constitutes a measurement tool supporting decision-making. A KPI focuses on a process of progress. It may be collective or personal and is necessarily tailored to the chosen strategy. KPIs are used in the presentation of management dashboards.

23 These rules are rarely formally defined, but are vital for maintaining trust between intelligence services that cooperate together.

24 For example, there is the need-to-know principle, the third-party rule, the observance of classification, surveillance and countersurveillance, cover stories and operational security, the management and protection of human resources, SIMs, the use of cryptography, and so on. Tradecraft also involves accepting a number of principles/concepts such as the intelligence cycle. However, care must be taken to ensure that these 'professional standards' remain consistent with the regulatory standards, and that tradecraft is sufficiently clearly documented and, where necessary, differentiated.

path that differs from that of ordinary state personnel (covered by the Royal Decree of 4 July 2014[25]), permanent 'Auditor-Analysts', also with a special career path (also covered by the Royal Decree of 4 July 2014), permanent state personnel with the so-called 'Camu status' (covered by the Royal Decree of 2 October 1937) and contractual personnel members (covered by the Employment Contract Act, 1978). The career path of personnel members covered by the Royal Decree of 4 July 2014 is closely linked to GISS: they can only be deployed in this service, whereas state personnel with Camu status and contractual workers can in principle also be employed in other areas of the Armed Forces.

The CI Directorate has fewer personnel than in the 1980s, whereas other services such as State Security, the police and CUTA have grown in size in the intervening period.[26] Even the planned recruitment wave (see below) would only bring the service back to its original strength. This has led to disillusionment and discouragement. CI management personnel therefore believed that the continuity of the service could be threatened. The Command acknowledged these problems and pointed out that they were due to the recruitment moratorium in the Federal Public Services between 1988 and 2009.

With regard to the various aspects of the personnel issue, the military intelligence service – like all other defence entities – is dependent on DG Human Resources and the options for GISS itself are very limited.

The taking over of civilian positions and duties by military personnel: a problem?

The CI Directorate was originally composed largely of civilians, but this ceased to be the case long ago. Historically, the purpose of creating a civilian component within the military intelligence service was to be able to rely on a civilian corps independent of the military apparatus to address potential threats within that apparatus (especially espionage, but also subversion or extremism). The civilian personnel believe that only civilians can ensure the necessary independence from the military hierarchy. The Committee did not share that opinion, arguing that independence does not necessarily have anything to do with status (civilian or military), but with people's mindset, structures and procedures. Due in part to the introduction of the recruitment moratorium from 1988 onwards, more military personnel gradually began to be deployed within the CI Directorate. There is no valid legal objection to this. This 'mix' was seen by many within CI as bringing added value.

---

25 The Royal Decree of 4 July 2014 determining the status of certain civilian officers of the staff department for intelligence and security of the Armed Forces, *Belgian Official Journal*, 18 July 2014. The Royal Decree of 7 July 2003 of the same name has been repealed.

26 The strategic plan of the Minister of Defence of 29 June 2016 stipulated that the overall workforce of GISS would grow by around a third by 2030. GISS expressed doubts about the feasibility of this objective, given that the reduction in personnel numbers in the Armed Forces (25,000 units in 2020) is happening much faster than expected.

It is true that the deployment of military personnel is not without problems: during the 2011 Audit, the Committee already noted that rapid rotation of military personnel was posing serious challenges in terms of introduction, training and knowledge management. However, there are also advantages (transfer of best practices, an influx of new ideas, etc.). The Committee did realise that the deployment of military personnel for CI duties was not necessarily a straightforward matter.

Another important issue was the recognition and appreciation of civilian personnel. Many civilians felt undervalued. It was already clear during the 2011 Audit that of all personnel categories this was most pronounced among the auditors (level A of CI). In that audit, the Committee stated that it was therefore better to '*not think in terms of "staff categories" (military personnel and civilians, contractual and statutory personnel, level X and level Y, etc.), but rather in terms of "positions"*'.[27] As this had no positive effect, the Committee feels that more far-reaching structural measures need to be taken. The possibility of a complete restructuring of GISS should not be ruled out, without losing sight of the specific nature of the various duties.

The contractual personnel issue

The CI Directorate has a small number of contractual analysts who have been employed for a long time. Their career prospects and remuneration are not very attractive. The Command acknowledged the problem and indicated that efforts were made in 2016 and 2017 to improve their status. The Command also referred to the initiatives of the Minister for the Civil Service in this area.

Job description and job content

The problems identified by the Committee are usually related to a lack of procedures and uncertainty about who does what and who bears what responsibility. Despite the recommendations of the Standing Committee I in the 2011 Audit, it had to be concluded that many job descriptions were still missing or lacked transparency.

On the other hand, many personnel members were found to be very satisfied with their job content. The work was described as 'varied, adventurous and exciting', with a high degree of autonomy and a mutually supportive atmosphere.

Recruitment, selection, mobility and outflow

As part of the armed forces, GISS and hence the CI Directorate have no autonomy with regard to personnel management in any of its facets (recruitment,

27 STANDING COMMITTEE I, *Activity Report 2011*, 103.

training, etc.). The CI Directorate is largely dependent for recruitment on the DGHR (for military personnel) and SELOR, the Federal recruitment and selection agency (for civilians). However, the Committee stated that some responsibility also lies with GISS itself: the service needs to provide properly detailed job descriptions so that recruitment can be more targeted.

Another problem is the rotation of military personnel. The rule for the career development of officers within the Armed Forces is that they are deployed within different units in the course of their career. This means that officers change unit every three years and non-commissioned officers every five years.[28] This was sometimes seen as a problem, because the military personnel who arrive at GISS from another unit cannot always be deployed in an efficient and effective manner, especially in view of the specific nature of an intelligence service and intelligence work. On the other hand, this system does create an opportunity for the influx of new ideas.

The career paths of civilian personnel contain fewer twists and turns. They can change units, but it is not common. An outflow was noted among contract personnel who were able to find a permanent position elsewhere (the Federal Police, the FPS Justice, State Security).

Education, training and knowledge management

In contrast to civilians who enter as inspectors or auditors and who will develop their careers in intelligence work from the outset (and have therefore been selected and trained for the purpose), military personnel who come to GISS following a change of position often arrive without specific knowledge. This is a serious problem.

There is a cell within GISS that is responsible for training. Its most important task is to organise and monitor a career path for civilian personnel.

In order to train new personnel members, a 'Basic Inspector Counter Intelligence Course 2018–2019' has been developed in which the candidates have to complete modules, followed by a one-year internship.

Despite previous recommendations,[29] the Committee again found that there was no formal knowledge management within CI.[30] A lot of knowledge was found to be held by individual personnel members and was not shared. Finally,

---

28 However, there are exceptions to this rule.

29 In the 2011 Audit, the Standing Committee I urgently recommended that actions be taken to mitigate the risks of discontinuity in the performance of a function and the consequent loss of knowledge. '*It is recommended that explicit attention is paid to knowledge management within GISS. Clear instructions should be developed to inventory existing knowledge, assess its relevance and take measures to save, store and disseminate this knowledge. It is recommended that a knowledge manager be appointed within each division to support the knowledge management process*', in STANDING COMMITTEE I, *Activity Report 2011*, 175.

30 This is the process of creating, documenting in an inventory (who knows what), sharing, using and managing the knowledge and expertise within an organisation.

the Committee noted that the risk of loss of knowledge and expertise within the organisation was increased by the personnel turnover (especially among analysts), and that there were no specific procedures to make up for loss of knowledge and expertise.

Individual assessment

The Committee found that there were three evaluation systems being employed independently within GISS: two for civilians (Camu/contractual status versus 2014 status) and a third for military personnel; this leads to unequal treatment. It is an established principle that military personnel do not have final authority over the evaluation of civilians or *vice versa*. This cuts across hierarchical lines and can be problematic.

I.1.5.11. Working conditions and infrastructure

The Standing Committee I was forced to conclude (again) that working conditions were appalling and unacceptable in various areas.

Material working conditions were the top priority for personnel. The Committee identified various shortcomings in terms of safety, hygiene and health, accommodation, etc., which were sufficient to seriously compromise the integrity of the buildings and the well-being of personnel.[31] For improvements to material conditions, GISS is dependent on the General Directorate for Material Resources (DGMR), and has very little autonomy in this area.

The accommodation problem of GISS and hence the CI Directorate must be seen in the broader context of the new infrastructure which is to be built for defence personnel. The Standing Committee I nevertheless considered that urgent work needed to be done to provide better working conditions.

I.1.5.12. Support and logistics

The personnel of the support services within GISS (personnel and budget management, IT, logistics, etc.) did not appear to have got the message about the intelligence culture or the distinctive nature of the service. There was a lack of knowledge about intelligence work, and they therefore had trouble communicating the needs of the service to the other General Directorates and departments. It was found that communication between the CI Directorate and the support services was inefficient, and indeed poorly developed.

The Standing Committee I also concluded that the CI Directorate rarely communicated with the sections of the General Staff. The Committee

[31] The Minister of Defence pointed out that maintenance work was being carried out pending a structural solution.

emphasised that these sections of the General Staff form the interface for communicating with other actors outside GISS. CI staff members indicated that their administrative, logistical and technical support had largely eroded away. There were complaints about a lack of autonomy and burdensome bureaucracy.

I.1.5.13. Information management[32]

From previous investigations, the Standing Committee I had learnt that information management at GISS was particularly problematic.[33] The investigation again confirmed these findings with regard to the CI Directorate. For example, this could be deduced from the personnel survey, which indicated that, among other things, there was a problem with access to external databases. CI was also rated poorly with regard to the speed, structure, completeness, user-friendliness and accessibility of information and documentation. With regard to CI's own database, there were three major problems: a backlog in the processing of data, faulty links with the source documents and the creation of individual folder structures.

I.1.5.14. Partnerships

The CI Directorate has numerous national and international partners (Belgian government agencies, foreign partner services, private partners, etc.). However, few synergies could be identified. The Committee referred to the findings and recommendations of the Parliamentary Inquiry Committee on Terrorist Attacks.[34] Naturally, when creating synergies, care must be taken to ensure that they do not jeopardise the distinctive nature of the CI Directorate's duties.

I.1.5.15. Feedback

As long ago as 2010[35], the Committee recommended that a feedback mechanism should be included in all GISS deliverables. On the one hand, the services had to

---

32 The issue of information management is far broader than is discussed here. Following the Committee's discovery of problems with information storage and management in 2005, a work and investment programme was set up in 2007. Due to budgetary constraints, the investments could not start until 2013. An Information Management Cell was also set up in 2013 to improve information management. This cell devised a meta-data management model, but lacked the resources to make the model work. In this regard, see: Senate 2017–18, 29 November 2017, Q no. 6–1674.

33 See, for example, STANDING COMMITTEE I, *Activity Report 2016*, 42 ('Investigation into the information position of the two intelligence services before the Paris attacks').

34 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, third interim report, *Parl. Doc.* Chamber of Representatives 2016–17, no. 54K 1752/007.

35 For example, see: STANDING COMMITTEE I, *Activity Report 2011*, 172–173 ('IX.2.2.1. Recommendations regarding organisational conditions required for a proper deployment of resources').

make clear under which conditions, how and to whom they wish to or may distribute intelligence and what 'ambition' may be expected of the service in that regard (descriptive, explanatory or predictive intelligence). The Committee also emphasised the role of the customers here. They must state what they expect and what their (intelligence) needs are. During this investigation, the Committee again found that there was little or no feedback.

I.2. THE ACTIVITIES OF GISS IN A FOREIGN OPERATIONS ZONE

An important part of GISS's work focuses on the production of intelligence about the political and military situation in other parts of the world. This is why the Committee has already previously expressed an interest in the role of this service in foreign operations zones such as Afghanistan and Lebanon.[36] In 2018, the Committee re-examined the deployment of GISS – and by extension the ISTAR battalion (see below) – in a specific[37] operations zone.[38] GISS was providing support to the Belgian military commanders on the ground there and, in accordance with the recommendations of the Rwanda Parliamentary Inquiry Committee[39], was responsible for providing force protection for Belgian military personnel. GISS was also carrying out support duties for the Belgian embassy and helping ensure the safety of expats. Finally, through its analysis offices in Belgium, GISS was contributing to the development of the Belgian strategic vision with regard to the conflict zone.

For its investigation, the Committee relied on sources including numerous documents[40], briefings from GISS and contacts with military intelligence service personnel. It also considered the cooperation among the various departments of GISS and the cooperation with foreign partners on the ground. As the information that came from the investigation is classified, the Committee cannot comment further on it here. In what follows, we focus on three points: the legal context of the deployment of GISS, the functioning and control of the ISTAR battalion, and some general conclusions.

---

36 STANDING COMMITTEE I, *Activity Report 2013*, (II.1. 'The role of the General Intelligence and Security Service in monitoring the conflict in Afghanistan'), 89–105 and *Activity Report 2007* ('II.2. Monitoring of radical Islamism by the GISS'), 93–97.

37 For security reasons, the Standing Committee I decided not to mention the location.

38 The investigation was opened in early March 2018 and completed in early July 2018.

39 *Parl. Doc.* Senate 1997–1998, 6 December 1996, no. 1–611/7.

40 The Chief of Defence Operations Order (CHODOPORDER), briefings from the various departments, reports produced by deployed units, etc.

I.2.1. THE LEGAL CONTEXT OF THE DEPLOYMENT AND ACTIVITIES IN THE ZONE

The military units were deployed in the zone as part of a non-international armed conflict. This meant that the law governing armed conflicts was applicable. The deployment of Belgian troops took place in accordance with a resolution of the United Nations Security Council and was approved by the Council of Ministers.

The authority of GISS to provide support to operations is described in Article 11 §1, 1°, d) of the Intelligence Services Act: '*§. 1. The duties of the General Intelligence and Security Service are: 1° 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, as well as the intelligence relating to any activity that […]: d) the fulfilment of the assignments of the Armed Forces; […] and immediately informing the competent Ministers thereof and advising the government, at its request, on the description of its internal and foreign policy in relation to security and defence*' (free translation).

As the service cannot perform every possible role in this context, priorities are defined in the so-called 'Intelligence Steering Plan' (ISP). The country in which the conflict zone was located, was given the highest priority in the 2015–2018 ISP.

The concrete activities of GISS in foreign operations are further specified in so-called operations orders from the CHOD (CHODOPORDER). Finally, there are also Fragmentary Orders (FragO), which determine the deployment of specific GISS units, such as Contact Teams which are temporarily sent in. All these documents determine the framework and limits within which the various detachments (including those from GISS) can perform their roles. For the sake of completeness, it should be noted that the National Security Council is also able to issue special directives in the context of the deployment of GISS resources abroad. This has not yet occurred up to now.

I.2.2. THE ISTAR BATTALION

As early as 2013, 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.[41] The Committee emphasised that the battalion had been formed

41 The Senate Monitoring Committee was informed of the Committee's legal standpoint on this subject in 2013 (STANDING Committee I, *Activiteitenverslag 2013* (Activity Report 2013), 92).

to meet a growing need for battlefield intelligence, in view of the increasing number of foreign missions. It reiterated that the Act of 30 November 1998 governing the intelligence and security services only recognises two intelligence services, 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, a provisional solution was worked out by means of a protocol agreement between GISS and the CHOD[42], defining 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. This role lies with GISS. The Standing Committee I was assigned the task of monitoring the battalion's activities, albeit indirectly, through reports made by GISS.

The Committee found that, in line with the recommendations of the Parliamentary Inquiry Committee on Terrorist Attacks and its own recommendations, the elements of the ISTAR battalion that were present in the operations zone were seconded to GISS for the duration of their deployment, and in administrative terms were therefore regarded as organic elements of GISS.

I.2.3. CONCLUSIONS

Apart from the fact that GISS had not complied with a particular formal condition for the use of a collection method, the Committee found no illegality. All deployed personnel demonstrated professionalism and commitment. The activities of GISS made it possible to gather essential information relating to events or incidents in which Belgian nationals or Belgian or European interests were involved. The Standing Committee I also found that cooperation between the directorates of GISS was based on intensive informal dialogue.

The working and security conditions were analysed. The Committee detected several vulnerabilities that could present a potential risk to the security of operations or personnel. With regard to the level of control, the Standing Committee I found that during the first rotation of elements of the ISTAR battalion, GISS had failed to carry out an inspection stipulated in the regulations.

---

42 Protocol agreement of 24 May 2018 between the CHOD and GISS regarding the HUMINT and analysis capabilities of the ISTAR Bn.

I.3. INFORMATION POSITION OF THE INTELLIGENCE SERVICES BEFORE THE ATTACK PERPETRATED IN LIÈGE

I.3.1. CONTEXTUALISATION

On 29 May 2018, Benjamin Herman killed two female police officers in Liège. Both were attacked with a knife and then shot. The perpetrator subsequently stopped a car and killed the passenger. Herman then sought refuge in a school, where he took a hostage. In the firefight that ensued, several officers were wounded and he himself was killed.

The perpetrator had been known to the Ministry of Justice since his youth. At the time of the attack, he was serving a long-term prison sentence for criminal offences. He had been held at various prisons and was due to be released in the course of 2018. The day before the attack, he had been granted leave in preparation for his final release and gone to the house of an acquaintance to stay the night. This person was afterwards found also to have been murdered.

The Parliamentary Monitoring Committee asked the Standing Committees I and P to start a review investigation in early June 2018,[43] as there were indications that Benjamin Herman had shown signs of radicalisation in Lantin prison in the course of 2017. The Monitoring Committee specified the part of its request that related to the Standing Committee I in mid-June 2018, asking for a review investigation '*into the information position of State Security and the exchange of information between State Security and its partners regarding the perpetrator and any co-perpetrators or accomplices in the incidents in Liège*' (free translation).[44]

The following questions were raised for the intelligence and security services[45]:

---

43 The Monitoring Committee also asked the two Committees to start a joint investigation into the role of CUTA in monitoring the perpetrator. In this regard, see: 'II.4. Information position of CUTA before the attack perpetrated in Liège'.

44 The Standing Committee P conducted an investigation into the exchange of information in the police services. The two Committees' joint final report was approved on 16 July 2018.

45 The review competence of the two Standing Committees does not extend to services other than the police, intelligence and security services, although they may invite people from other services (such as the DGPI) to hearings if they consider it necessary (Art. 24 and 48 of the Review Act). The investigation services were in contact with the administrative unit of the Office of the Minister of Justice (ATS/SAT Justice) in order to gain insight into the way in which information about prisoners is made available. Meetings were also held with the Extremism Unit (CelEx Department) of the DGPI and with a representative of the Directorate-General, with the aim of obtaining background information on how extremist prisoners are monitored.

- Was the perpetrator known to State Security and/or GISS prior to the attack, what information was available about him and which service was the source of this information?
- With which services were there exchanges of information or consultations?
- Was the perpetrator discussed at local or national meetings (of the Local Task Force (LTF), National Task Force (NTF)[46], or even the Local Integrated Security Unit (LIVC-R)[47])?
- Were State Security and/or GISS contacted by the partner services regarding the perpetrator before 29 May 2018?
- For State Security in particular: how did cooperation with the Directorate-General for Penal Institutions (DGPI) proceed in the implementation of the Protocol Agreement?

I.3.2. MONITORING OF EXTREMIST PRISONERS

I.3.2.1. A variety of actors

Various services have roles assigned in the monitoring of prisoners who have extremist ideas or have been convicted for terrorism offences. They cooperate by exchanging information and/or conferring together on the current situation or on actions to be taken.

The DGPI has an important role to play in this context. Prisoners come into daily contact with prison officers and local management teams. A personal file is kept on every prisoner, and updated if any incidents occur. In the DGPI's central management, the Extremism Unit ('CelEx Department') is charged with the special monitoring of prisoners with a radical profile.

State Security is also interested in these individuals, both during their imprisonment and after their release. A Prisons Unit was established within State Security in 2015 and is in close contact with the DGPI.[48] The field services (provincial posts) of State Security also play a role in this respect, by gathering information through their contacts with the prison authorities about prisoners of interest to the service.

---

46 A Local Task Force is a consultation platform, set up at a decentralised level, in which police and intelligence services exchange information and intelligence about violent radicalisation and make coordination arrangements about information-gathering (from: Ministerial Circular GPI 78 of 31 January 2014 on the processing of information to ensure an integrated police approach to terrorism and violent radicalisation, *Belgian Official Journal*, 17 February 2014.) The LTFs operate under the coordination of the National Task Force.

47 The LIVC-R is a multidisciplinary, municipal consultation platform for socio-preventive actors in the fight against violent radicalisation, detecting at an early stage individuals who are undergoing radicalisation and developing individualised monitoring processes for them.

48 Since the creation of the Prisons Unit, the size of this office has quadrupled from three people (including one analyst) in 2015 to twelve employees (including three analysts).

Police forces that have a prison in their territory are required as part of their administrative policing role to cooperate with the prison authorities. They are responsible for assessing the risk of transferring prisoners (e.g. temporary releases) as well as for basic policing, including at local level. Article 20 of the Policing Act provides for the monitoring by the police of convicted offenders who are sentenced to an alternative to imprisonment.[49]

The Coordination Unit for Threat Assessment (CUTA) only intervenes when a prisoner is either listed in a common database[50] (as a foreign terrorist fighter, home-grown terrorist or hate preacher) or when there are indications – provided by its support services – that point to a terrorist or extremist threat.

Finally, the judicial authorities – in particular the public prosecutors – can also play a role when they receive information from the various services about prisoner activities of a criminal nature, when they are involved in such activities, or when there are judicial actions to be undertaken.

I.3.2.2. A variety of databases

The SIDIS Suite database, which is managed by the DGPI, processes 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 secure unit within a prison (for involuntary commitment) or a community institution for minors. Its purpose is to facilitate appropriate management of the detention and of the institutions. The database makes the necessary information exchange and data flows possible between the police, the public prosecutor's office, the intelligence services, the courts and other parties. SIDIS Suite contains information about the duration of the detention, fingerprints, the subject's prison process and regime, visitors, periods of leave and other matters. State Security, the Federal Judicial Police, DGA/DAO, DGJ/DJO, the District Communication and Information Service (SICAD) and the police zones with a prison or court building in their territory have access to the data.[51, 52] However, the police services do not have access to all the data.

---

49 Joint circular letter COL 11/2013 from the Ministers of Justice and Home Affairs and the Board of Procurators General clarifies that the police monitoring tasks described in it do not necessarily have to be performed in cases of temporary release and prison leave. In the latter cases, the role of the police services is confined to general police monitoring.

50 See Art. 44/11/3*bis* of the Policing Act providing for the establishment of common databases. See the detailed discussion of this in: 'Chapter VI. Monitoring of the common databases'.

51 Judicial alerts regarding freed or conditionally released persons are the subject of COL 11/2013 and of the FTF Circular of 2015. With regard to prison leave granted by the Minister of Justice, COL 11/2013 does not state that the prison must actively send information to the police zones.

52 On SIDIS Suite and the way in which services outside the DGPI have access to it, see also the answer of the Minister of Justice in the Parliamentary Committee on Justice on 20 June 2018, *Parl. Doc.* Chamber of Representatives, CRABV, 54, COM 930. It should be noted that access to SIDIS Suite is not identical for all services. In its capacity as competent supervisory

In addition, the DGPI also maintains a 'CelEx' list.[53, 54] This list – based on DGPI's 'Specific instructions on extremism' – has been drawn up for the attention of prison management teams but also for all personnel members so that they are constantly on the look-out for signs of radicalisation and extremism. Inclusion in this list results in closer monitoring of the prisoner. The CelEx list includes four categories of prisoners.[55] Once a person is put on the list, a message is sent to the partner services (State Security, DJSOC/Terro, CUTA) in order to share this information, but also to find out if that person is already known to the intelligence and police services. In certain cases, a message is also sent to different services when a prisoner makes a trip outside prison. Benjamin Herman was not on the CelEx list.

Twice a month a meeting is organised at federal level of the Radicalism Plan Prisons Working Group, at which the DGPI (CelEx), State Security, CUTA and the Federal Police (DJSOC/Terro) confer together on various subjects, including the composition of the CelEx list. State Security noted that there is no formal procedure for placing individuals on this list (and removing them from it), and that the advisory role of the DGPI's partner services is rather informal and has developed from the daily practice of cooperation. State Security argued in favour of formalising procedures and broadening ownership, which at the time of the investigation still lay completely with the DGPI.

Finally, it should be noted that State Security does not confine itself to monitoring the prisoners on the CelEx list. The Prisons Unit also works with 'target lists' of prisoners for each prison. At the time of the investigation, around 500 prisoners were subjects of interest from State Security because of a potential connection with terrorism (access to weapons, financing of terrorism with drug money, etc.). The fact that two lists are used is partly due to the fact that State Security does not wish to share the names of certain prisoners because it would endanger a source, because of the third-party agency rule, or to prevent ongoing

---

authority, the Standing Committee I, together with the Standing Committee P, issued an opinion in October 2018 on a draft bill on access to SIDIS Suite for CUTA (www.comiteri.be, Opinion 007/2018 – Leesrecht SIDIS SUITE/OCAD). The Standing Committee I also issued an opinion on access rights to SIDIS Suite for State Security, GISS and the security services (www.comiteri.be, Opinion 006/2018, Leesrecht Sidis Suite).

53 CelEx is short for 'Cellule/Cel Extremisme' (the Extremism Unit), which compiles and maintains the list. The list contained 234 names at the beginning of July 2018 (see answer from the Minister of Justice, *Parl. Doc*. Chamber of Representatives, CRABV, 54, COM 910, 4 June 2018, p. 34: *'There are around 250 radicalised individuals in our prisons*' (free translation)).

54 The DGPI tends to refer to the 'CelEx report' rather than the CelEx list.

55 (a) those convicted of or charged with terrorist offences; (b) those whose actions are equated with terrorist offences; (c) the (foreign) terrorist fighters and home-grown terrorists from the CUTA list, whether or not the reason for their detention is their FTF character (many ordinary criminal offences); and finally (d) a fourth residual category D. With the support of its partners, the central Extremism Unit evaluates whether prisoners should be placed in this category. The unit's privileged partners are CUTA, DJSOC/Terro and State Security.

intelligence or judicial investigations from being placed at risk. In addition, account must be taken of the fact that State Security and the DGPI have different purposes; State Security can go ahead with obtaining information about certain prisoners at an early stage, without there being sufficient reason for the DGPI to put them on the CelEx list. Benjamin Herman was not on these target lists either.

I.3.3. INFORMATION THAT WAS AVAILABLE TO THE INTELLIGENCE SERVICES[56]

Benjamin Herman was not known in the GISS databases. It was found that GISS had attended and received a report on an LTF meeting in Marche-en-Famenne on 22 February 2015, at which Benjamin Herman was mentioned. However, there was no military link, so it was not unusual for the name of the person concerned not to be entered in the GISS database.

Benjamin Herman appeared in seven documents at State Security.[57] The available notes show that the information that the service had about Benjamin Herman was rather vague and limited in content. The latest information it had collected itself dated from 1 February 2017: this stated that, according to a source, Benjamin Herman was radicalising and increasingly seeking contact with a person who engaged in proselytising activities in prison. The analysis notes that followed reiterated this and earlier information. For example, in May 2017 an analysis note was distributed to the Federal Police, CUTA and the DGPI.

I.3.4. MUTUAL INFORMATION FLOWS

Consultation meetings took place between different services (LTF, the Prisons Working Group) at various times, during which the name of the perpetrator came up.

I.3.4.1. The Local Task Force (LTF)

Benjamin Herman was named in two reports on the Luxembourg LTF meetings (February 2015 and March 2017).

Various police services and GISS were present at the 2015 meeting; CUTA, State Security and the public prosecutor were not present. The minutes were sent

56 The information that was available to the police services is reported by the Standing Committee P (www.comitep.be).

57 These were five operational reports (ORs) from the collection services, which were not directly distributed externally but processed by the analysis services, one summary sheet (FS) and two 'Notes aux autorités' (NAs) in which the authorities were informed.

to those that attended and State Security, but not to CUTA.[58] The report contains a reference to Benjamin Herman, who along with two others was said to pray intensively, but also mentions that no fellow prisoners were pressured to participate in the prayers.[59]

At the March 2017 LTF meeting, a list of more than 50 people was gone through. Various police services, State Security and CUTA were present, as well as the public prosecutor; GISS was not. The report, in which Benjamin Herman appears, was sent to all services. In the 'Person' column, Herman's name is not explicitly mentioned; rather, another prisoner in Marche-en-Famenne is listed, who was behaving threateningly and arrogantly and trying to pass himself off as a tough jihadist. It is stated that this person was imprisoned for criminal offences that he had committed with – among others – Benjamin Herman.[60] This information came from an information report (RIR) from the Famenne-Ardenne local police zone. Benjamin Herman himself was not the subject of the RIR. During such meetings, according to the respondents it is customary for a person only to be mentioned when the services concerned have something useful to say or add about him. Benjamin Herman had not attracted any attention in that regard. The State Security inspector present at the meeting prepared an internal report for the benefit of his superiors. Benjamin Herman's name is not mentioned in this internal report. When asked about this, State Security stated that the interpretation was that these offences fell within the scope of ordinary criminal law, which is not of relevance to the service. There was therefore no reason for the service to specifically include Benjamin Herman's name in an internal report based on the LTF list.

I.3.4.2. The Radicalism Plan Prisons Working Group

Benjamin Herman was not on the CelEx list. His name was never mentioned during the biweekly discussions of the Radicalism Plan Prisons Working Group between State Security, DGPI (CelEx), CUTA and the Federal Police (DJSOC/Terro). State Security only produced a report on these meetings for internal use.[61]

In early August 2017 emails were exchanged between a number of services – State Security, the DGPI, DJSOC/Terro and CUTA – about a person X who was

58 The reports of the Local Task Forces did not have to be sent to CUTA at that time. CUTA was only a recipient of relevant information regarding foreign terrorist fighters.

59 This information is the same as that contained in a police information report (RIR) a month earlier.

60 Benjamin Herman was still in Lantin prison on 13 March 2017, and was only transferred to Marche-en-Famenne a few days later.

61 State Security stated that the results of the discussions had in the past been sufficiently covered by the very frequent email exchanges between the services, but that further formalisation – in the form of an official report – has recently become normal.

in Leuze prison (Hainaut). State Security followed up by compiling an analysis note about this person X. Benjamin Herman was also mentioned, and it was stated in the note that radicalisation and other issues had been (briefly) discussed with respect to him too.[62] On the day the note was sent, there was contact between State Security and the Extremism Unit, but with regard to person X rather than Benjamin Herman. In the subsequent email correspondence between State Security and the DGPI, Benjamin Herman was discussed, however. The DGPI asked whether, along with others, he 'should be placed on the CelEx list', while noting that apparently no further radicalisation had been noticed since 2017.[63] State Security replied that the DGPI 'should take the administrative decision itself, based on the intelligence provided by State Security'. It added that people were still being monitored by State Security even if they were not on the CelEx list.

The subject of Benjamin Herman was apparently not returned to in subsequent consultations. The police and intelligence services heard nothing further until the time of the attack at the end of May 2018.

I.3.5. EVALUATION OF THE DGPI/STATE SECURITY PROTOCOL

As early as 2014, an investigation was initiated by the Standing Committee I into how State Security implements the 'Protocol Agreement governing cooperation between State Security and the (then) Directorate-General for the Execution of Penalties and Disciplinary Measures'.[64] The Standing Committee I was unable at that time to provide precise figures on the exchange of data. The present investigation was able to provide quantitative evidence of the intense contacts between the two services.[65]

The earlier investigation found no serious shortcomings or expressions of dissatisfaction with the reality of the cooperation. This finding was confirmed.

In its recommendations, the Committee stressed the need to use these lists carefully in order to ensure that the purpose of the various lists was clearly established and respected. One important point concerning the interaction

---

62 The analysis note was sent to the DGPI, DJSOC/Terro and CUTA. The CelEx list was not mentioned in the note.

63 The inclusion of a prisoner on the CelEx list has certain consequences for the person concerned. The DGPI must therefore give detailed reasons for putting someone on the list. In addition, a problem may arise when the DGPI acts on the basis of soft information or information that is classified and therefore cannot simply be used to justify a decision.

64 STANDING COMMITTEE I, *Activity Report 2016*, 63–68 ('State Security and the cooperation protocol with penal institutions').

65 The number of outgoing emails from State Security to the CelEx fluctuated between 100 and 270 between January 2017 and June 2018; the number of incoming emails for the same period fluctuated between 200 and 450. An upward trend was noticeable for both flows over time.

between the lists of the DGPI and State Security was the observation that inclusion on the CelEx list often led to a prisoner becoming aware of the fact, as he experienced the consequences on a daily basis. This made discreet monitoring by State Security harder.

The exchange of information was also the subject of investigation in the evaluation of the protocol (in particular the distribution of raw information). State Security did not distribute the internal operational reports in which Benjamin Herman was mentioned. The police services did so with the RIRs they drew up, although these also contained raw information.[66]

I.3.6. CONCLUSIONS OF THE STANDING COMMITTEES I AND P

I.3.6.1. Information position of the services

It has to be concluded that the information about Benjamin Herman that was available to the police, intelligence and security services, as well as CUTA, was sparse, brief and not very alarming. The term 'radicalisation' appears for the first (and last) time in relation to Herman in an operational report from State Security of February 2017. The information is very brief, as the target was not Herman, but someone else. Herman exhibited certain religious behaviours that were not considered extremist; proselytism was not observed. It was not possible to deduce that he would constitute an extremist or terrorist threat separately from his record of ordinary criminal offences.

If Herman was already planning to carry out an attack during his prison leave, this was not apparent from the monitoring of him by the services or from his behaviour in prison. His name did not come up in the period prior to the attack.

There is little variation in the information held by the police and State Security, and hence too in the information that CUTA obtained from them both. This can be explained by the fact that the services have a limited direct view of prisoners.

The different lists – the CUTA list, the CelEx list, the target lists of prisoners of State Security – are not completely consistent with each other. However, it was shown that the information was shared. The Minister of Justice stated that he

66 State Security only distributes analysed information ('intelligence') based on the information it collects itself or obtains from other sources/partners. Not every collection report automatically and immediately leads to an analysis note that is sent to the authorities; the way in which the collected information is processed in analysis notes and the time when an analysis note is drawn up depends, among other things, on the quality and quantity of the raw information. In the present case, the information from the collection notes was in fact processed in analysis notes and hence distributed.

was developing plans to transform the CelEx list and to include it in the CUTA common database in order to eliminate the differences between the lists.[67]

I.3.6.2. Exchange of information

The different services each had separate information about Benjamin Herman and shared this with CUTA. There was a noticeable difference in this respect in the way of working of the police services and of State Security. The Federal Police's DJSOC provided CUTA with the information reports (RIRs) prepared by Federal or Local Police services after an internal quality check, but without adding any analysis. State Security does not transfer the collection services' internal operational reports (ORs) directly, but analyses them and sends the processed information (analysis notes) to CUTA. The difference is related, among other things, to the different underlying approach and the intended purpose of the documents: the police approach in which the basic information must remain unaltered, versus the intelligence approach in which analysis and the piecing together of information from multiple sources play a major role. State Security also sent these analysis notes to the Federal Police.

The information obtained by CUTA was stored in the internal database, which is not accessible to other services. Such information is accessible in relation to persons who are included in the common database 'terrorist fighters'[68] or hate preachers, but since Benjamin Herman could not be linked to any extremist or terrorist threat, the information was not processed in this database and was not generally consultable.

The very important position and possible role of the DGPI in the whole process of gathering information about prisoners are also apparent.[69]

I.3.6.3. Roles of the services

The Standing Committees I and P believe that the various services acted properly. The information available to them was sparse and not particularly significant, but it was exchanged. It could not be deduced from it that Benjamin Herman had extreme/radical or terrorist plans or presented a threat of that nature. There was no reason for CUTA to draw up an individual threat analysis

---

67 On this subject see the answer from the Minister of Justice in the Parliamentary Committee on Justice, 20 June 2018, in which he states that '*a Royal Decree is being drafted that will include the CelEx list in the CUTA common database*' (free translation), in *Parl. Doc.* Chamber of Representatives, CRABV, 54, COM 930, 5. State Security suggested that the revision of the Action Plan on Radicalisation in Prisons of March 2015 could be the starting point for this.

68 See 'Chapter VI. Monitoring of the common databases'.

69 State Security stated that the importance of CelEx could not be sufficiently emphasised. It had been calling for some time for a reinforcement of CelEx, linked to the recruitment of 'local radicalism coordinators'.

for him. Based on what it knew, none of the services could foresee that Herman would commit an attack.

The management of the CelEx list by the DGPI falls outside the competence of the Standing Committees P and I, which therefore cannot comment on it.

Although it was not the subject of the review investigations, the Standing Committees P and I became aware of the internal note that was drawn up within the prison administration three days before the attack (25 May 2018). The content of this note confirmed what had been previously stated. Again, Benjamin Herman was not the direct subject, but (various) other people. Herman did not play a leading role, and there was no indication of an extremist or terrorist threat or plan. The note was simply intended for information purposes for the prison management. It was clear that even if this note had been known to the other services in advance, it could not in any case have led to the conclusion that Herman was a threat or had plans to commit an attack.[70]

I.4. INFORMATION POSITION OF CUTA BEFORE THE ATTACK PERPETRATED IN LIÈGE

I.4.1. OPENING OF A JOINT REVIEW INVESTIGATION

In the wake of the attack perpetrated by Benjamin Herman in Liège in late May 2018[71], the Parliamentary Monitoring Committee also asked the Standing Committees I and P to conduct a joint investigation into the information position of the Coordination Unit for Threat Assessment.[72] The service was asked the following questions:

- What information did CUTA have about the perpetrator before 29 May 2018 (the time of the attack)? Was the perpetrator known to be radicalised? What information did CUTA receive from its partners/supporting services?
- Did CUTA exchange information with its partners/supporting services? Was information about the perpetrator made available via a database? Did consultation take place about the perpetrator?
- Did CUTA prepare a threat assessment or risk analysis about the perpetrator?

The two investigation services jointly contacted CUTA to find out what information the service had, and also held a meeting with the director and the members of the coordination unit.

---

70 It is clear that if the attack had not taken place, there would have been no reason, in principle and in view of the content, to specifically inform State Security of its content.

71 See 'I.3. Information position of the intelligence services before the attack perpetrated in Liège'.

72 Under Article 53, first paragraph, 6° of the Review Act of 18 July 1991, the Standing Committees I and P fulfil their review roles as regards CUTA and its support services jointly.

I.4.2. INFORMATION SOURCES

CUTA is only supposed to intervene when a prisoner is either listed in the common database (as a foreign terrorist fighter, home-grown terrorist or hate preacher) or when there are indications – provided by its supporting services – that point to a terrorist or extremist threat that falls within the competence of CUTA.

CUTA had only limited information about Benjamin Herman. This consisted of:

- three information reports (RIRs) from the Luxembourg Federal Judicial Police (2015), the Liège Federal Judicial Police (2016) and a final one prepared by the Famenne-Ardenne Police Zone (2017);
- two analysis notes from State Security (2017);
- the report of the Neufchâteau Local Task Force of March 2017.[73]

Information from the prison system can reach CUTA through several channels: directly from the prisons – for example during meetings about CelEx prisoners – or via other messages[74], but also indirectly, for example via the police services (in RIRs), State Security (in analysis notes), or a Local Task Force (LTF).[75] At the time of the investigation, the DGPI was not yet a supporting service of CUTA.[76, 77]

I.4.3. INFORMATION AVAILABLE TO CUTA

The Committees were able to establish that the information available to CUTA was identical to that of the police and intelligence services. Benjamin Herman never appeared 'directly' in it, but always in relation to and on the margins of other people who had caught the services' attention more directly. Nothing was known about the perpetrator's views, other than the fact that he was a practising Muslim (in the sense that he participated in prayers). CUTA could not deduce from the available data that he was or might be a threat.

---

73 An earlier LTF report from 2015 was not sent to CUTA, which at that time only received relevant information with regard to foreign terrorist fighters.

74 For example, email messages specifically concerning prisoners on the CelEx list.

75 CUTA points out that, just like the DJSOC/Terro and State Security, it received information and questions directly from the DGPI, in accordance with the arrangements made between these services in the Prisons Working Group. However, CUTA does not intervene in matters that affect the operational powers of the services concerned.

76 This was changed by the Royal Decree of 17 August 2018 implementing Article 2, first paragraph, 2°, g) of the Act of 10 July 2006 on threat analysis (*Belgian Official Journal* 12 September 2018).

77 There is no guaranteed feedback to the DGPI: if the police or State Security report internally or externally (for example to CUTA) about a prisoner, the DGPI does not necessarily know; nor does it know whether the information it has provided has had any consequences.

Benjamin Herman was recorded as an entity in the internal database of CUTA, in which the aforementioned documents were included. However, this database is not accessible to other services.[78] As noted (I.3), the different lists (the CUTA list, the CelEx list and the target lists of prisoners of State Security) are not completely consistent with each other.

The available information did not contain conclusive elements that met established criteria for the inclusion of the person concerned in the common database of which CUTA is the operational administrator (the consolidated terrorist fighters and hate preachers database). For the same reason, CUTA did not prepare internal documents relating to Benjamin Herman or produce a threat analysis. The two Committees accepted this and concluded that the information was not of such a nature that a threat analysis was required. The 2017 data on the radicalisation of the person concerned[79] was too slight to work with, and Benjamin Herman had not attracted attention since then.

I.5. ALLEGED COMMITMENT MADE BY AN INTELLIGENCE SERVICE TO A THIRD PARTY

In 2018, the Standing Committee I received a complaint in which the person concerned claimed that he had been made a certain commitment as an informant. The Committee then carried out the required checks with the relevant intelligence service. The Committee concluded that no evidence of such a commitment could be found.

I.6. REVIEW INVESTIGATIONS IN WHICH INVESTIGATIVE STEPS WERE TAKEN DURING 2018 AND INVESTIGATIONS OPENED IN 2018

I.6.1. INTERNATIONAL EXCHANGE OF INFORMATION ON FOREIGN TERRORIST FIGHTERS

As early as 2016, during an international meeting with various European review bodies[80], it was decided to start a similar review investigation in all participating

78 If the common database were expanded and also included individuals who radicalise in prison and individuals who leave prison after a terrorism sentence, as is apparently the plan of the Ministers of Justice and of Home Affairs (see reply from the Minister of Justice, *Parl. Doc.* Chamber of Representatives, 54, CRABV, COM 910, 4 June, 2018, 34), this problem would be remedied and services outside CUTA would also be able to consult this information.

79 See 'I.3. Information position of the intelligence services before the attack perpetrated in Liège'.

80 The Belgian Standing Intelligence Agencies Review Committee, the Dutch Intelligence and Security Services Review Committee (CTIVD), the Swiss Strategic Intelligence Service

countries into the international cooperation between the various intelligence services with regard to the fight against foreign terrorist fighters (FTFs). This initiative subsequently received the express support of the chairperson of the Monitoring Committee (Chamber of Representatives). The intention is 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 section of the investigation[81] is 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 the FTF issue.

The ultimate aim of the investigation is 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 undermining the fundamental rights of citizens.

Regular meetings have been held over the past three years to discuss methods, best practices and legal and practical issues and to exchange experiences from the national investigations. No classified information was shared at these meetings. At the beginning of November 2018, a joint statement and press release were prepared by the participating oversight bodies.[82] The Belgian part of the investigation was completed in early 2019.

I.6.2. SECURITY SCREENINGS CONDUCTED BY THE INTELLIGENCE SERVICES

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

The role that intelligence services play in the context of trustworthiness investigations is not always the same. Sometimes it is limited to passing on personal data in their possession to other authorities. Sometimes they actively 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 authorisation.

Supervision and delegations from Sweden (Commission on Security and Integrity Protection), Norway (Parliamentary Oversight Committee) and Denmark (Intelligence Oversight Board). In this regard, see STANDING COMMITTEE I, *Activity Report 2015*, 80–81.

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

82 See Appendix 'Strengthening the oversight of international data exchange between intelligence and security services'.

In this case, a complaint resulted in a review investigation. An employee at Brussels National Airport had his access badge revoked after a negative decision[83] from the National Security Authority (NSA). He lodged an appeal with the Appeal Body on security clearances, certificates and advice and brought an action for annulment and suspension before the Council of State. The Appeal Body ruled that the complaint was inadmissible because it was lodged against the decision of the FPS Mobility and Transport and not against the NSA's decision. The Council of State also rejected the complaint. The complainant then turned to the Standing Committee I, however without defining the subject of the complaint. He stated he did not understand why a negative decision had been made, as a result of which he lost his job and had his pilot licence suspended.

Based on this individual complaint, the Committee considered it legitimate to open a wider investigation into how intelligence services perform security screenings.[84]

Due to other priorities, the first investigative acts could only be carried out towards the end of 2017. From January to May 2018, interviews were organised with those in charge of the sections that handle security screenings at the two intelligence services, as well as with some of their employees. The interviews took place in several sessions, with additional clarifications and details being provided. A detailed legal analysis of the legislation relevant to this investigation was also carried out, and figures and documents were requested from the services.

A draft report was sent to both State Security and GISS in November 2018; in December the Committee received comments from the services and adjusted its report accordingly where necessary. The review investigation was finalised in March 2019.

I.6.3. 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.[85]

---

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

84 '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 on 13 February 2017.

85 W. VAN LAETHEM, 'Het coördinatieorgaan voor de dreigingsanalyse: een punctuele analyse', *Vigiles*, 2007, Vol. 4, 109–127. Also see: Belgian Standing Committee I, *All Source Threat Assessments in the Fight against Terrorism – Fusion Centres throughout Europe*, Antwerp, Intersentia, 2010, 220 p.

Its core task is to make ad hoc or strategic assessments. This task is entrusted to analysts and experts (seconded from the 'supporting services'). Those supporting services, which are CUTA's most important source of information, include State Security, GISS, the integrated police, the Customs and Excise Administration of the FPS Finance, the Immigration Service of the FPS Home Affairs, the FPS Mobility and Transport and the FPS Foreign Affairs (Article 2, 2° of the Threat Assessment Act). They are very diverse services, each with their own culture and size.

In 2010, the Standing Committees I and P carried out a joint review investigation into the information flows between CUTA and the supporting services, paying particular attention to the two intelligence services and the Federal and Local police.[86]

At the joint plenary meeting in December 2017, it was decided to open a review investigation into the 'other' supporting services.[87] 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 four[88] other supporting services, based on an extensive survey.

In the course of 2018, various investigative actions were carried out. For example, interviews were conducted on the basis of a structured, detailed questionnaire with representatives from the Immigration Service (FPS Home Affairs), the FPS Mobility, the FPS Foreign Affairs and the Customs and Excise Administration (FPS Finance). The points of contact at the various supporting services themselves were also questioned. Consultations with the investigation team of the Standing Committee P took place at various times.

The joint review investigation was to be finalised during the second half of 2019.

I.6.4. EXAMINATION OF THE FUNCTIONING OF THE I/H DEPARTMENT OF GISS

A judicial investigation by the Federal Public Prosecutor's Office, conducted on the ground by the Investigation Service of the Standing Committee I, revealed a

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

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

88 Motivated by the need to establish an arrangement as soon as possible for the information flows from the services concerned to CUTA and vice versa, the Governmental Coordination and Crisis Centre (FPS Home Affairs), the Directorate-General of Penal Institutions (FPS Justice), the Department of Worship and Secularism (FPS Justice) and the General Administration of the Treasury (FPS Finance) were added as 'supporting services' (Royal Decree of 17 August 2018 implementing Article 2, first paragraph, 2°, g) of the Act of 10 July 2006 on threat analysis, *Belgian Official Journal*, 12 September 2018. These supporting services fell outside the scope of the investigation.

number of structural dysfunctions in the functioning of the I/H (Human Intelligence) Department of GISS. This department, which forms part of the Directorate I (Intelligence) of the military intelligence service, is tasked with establishing networks of sources and informants that enable GISS to gather intelligence on foreign phenomena. A number of those dysfunctions had already been raised in the course of a previous review investigation.[89] They included the description of assignments, strategic management, the skills and quality of personnel and tradecraft. The I/H Department was also mentioned in the investigation into the functioning of the Counterintelligence Directorate (I.1): it was clear that there was at least a risk that the two services could hamper one another's work due to a lack of clear agreements and guidelines.

At the beginning of May 2018, the Chair of the Monitoring Committee, the Minister of Defence and GISS were all informed of the opening of a '*review investigation into the functioning of the I/H Department of GISS*' (free translation).

There was a first general briefing soon afterwards, followed by numerous investigative actions. The investigation will be continued in 2019.

I.6.5. INFORMATION POSITION OF THE INTELLIGENCE SERVICES CONCERNING THE PAKISTANI NUCLEAR SCIENTIST KHAN

In mid-January 2018, an article appeared in the press[90] about the North Korean nuclear programme. Reference was made, among other things, to the Pakistani nuclear weapons programme and the late Professor Martin Brabers (University 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. On 12 June 2018, on the initiative of a member of Parliament, the Monitoring Committee of the Chamber of Representatives tasked the Standing Committee I with investigating the matter. On 2 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 knowledge he acquired of weapons of mass destruction which were*

89 See STANDING COMMITTEE I, *Activity Report 2017*, 12–19 ('II.1. A complaint about three GISS operations').

90 M. RABAEY, *De Morgen*, 13 January 2018 ('De Belgische bommen van Kim Jong-un'). Frequent reference is made in the article to Luc BARBÉ (L. BARBÉ, *België en de bom. De rol van België in de proliferatie van kernwapens*, June 2012), which calls for a wide-ranging independent scientific inquiry within academic circles and at State Security concerning the nuclear sector in Belgium.

ultimately used to develop nuclear weapons in Pakistan' (free translation) was initiated.

Various investigative tasks were carried out in the second half of 2018. The investigation was completed at the beginning of 2019.

I.6.6. PUIGDEMONT AND POSSIBLE ACTIVITIES BY FOREIGN INTELLIGENCE SERVICES IN BELGIUM

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.[91] 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.

Various investigative tasks were carried out in the second half of 2018. This investigation was also completed at the beginning of 2019.

[91] 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).*

CHAPTER II
CONTROL OF SPECIAL AND CERTAIN ORDINARY INTELLIGENCE METHODS

This chapter includes further statistics on the use by State Security and the General Intelligence and Security Service (GISS) of the special and the ordinary methods with regard to which the Standing Committee I has been assigned a specific role. It also describes the manner in which the Committee performed its jurisdictional monitoring of these methods.

II.1. STATISTICS RELATING TO SPECIAL METHODS AND CERTAIN ORDINARY METHODS

Between 1 January and 31 December 2018, a combined total of 2445 authorisations were granted by the two intelligence services for the use of special intelligence methods: 2315 by State Security (of which 1971 were for specific methods and 344 were for exceptional methods) and 130 by GISS (of which 102 were for specific methods and 28 were 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	1102	122	1378
2014	114	36	976	156	1282
2015	87	34	1143	128	1392
2016	88	33	1558	189	1868
2017	79	22	1612	210	1923
2018	102	28	1971	344	2445

The total number methods used increased by more than 25% in 2018 (from 1923 to 2445). The observed increase is mainly due to the sharply increased use of

special methods by State Security. The increase in exceptional methods is particularly striking in this context. GISS also made more use of special intelligence methods in 2018, thus returning to the same level as a number of years before.

A similar situation can be observed for the regular methods of requests made to operators to identify certain means of communication. State Security Service made 6482 requests, which represents a substantial increase. At GISS, the figure nearly doubled.

	Requests by GISS	Requests by State Security
2016	216	2203
2017	257	4327
2018	502	6482

In its previous annual report, the Committee commented as follows on this: '*Apart from the fact that it is almost impossible to compare the statistics on identifications over the years, the Committee cannot ignore the finding that the number of identifications has increased considerably since the introduction of the streamlined procedure under Article 16/2 of the Intelligence Services Act. Based on its general powers of review, the Committee will request State Security to internally investigate the extent to which this high number of requests is caused, or partly caused, by the streamlining of the procedure. Attention must also be paid to the nature of the threats that justify the requests and to whether and to what extent such requests are made at the behest of foreign authorities or partner services.*'[92] The Committee reiterated this intention to its Parliamentary Monitoring Committee.[93] However, the Committee did not receive any answers (in the case of GISS) or any satisfactory answers (in the case of State Security[94]) to its questions on this matter. It 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*

92 STANDING COMMITTEE I, *Activity Report 2017*, 39.

93 *Parl. Doc.* Chamber of Representatives 2018–19, no. 54K3375/001 (Activity report 2017 of the Standing Committee on the Intelligence and Security Services, Report on behalf of the Special Commission Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee).

94 According to State Security, the increase was only partly explained by a relaxation of the procedure by Parliament. The number of applications was also higher because they produced more results (among other things by removing the anonymity of prepaid cards). The final reason given was that – although these applications do not fall under Art. 16/2 of the Intelligence Services Act – the same format is used for the surveillance of targets on social media, as a result of which these applications (unfortunately) also end up in the statistics. Finally, State Security specified that the number of applications due to requests from foreign partner services had not increased in proportion to the total of applications.

or adapted by Parliament with respect to which the Standing Committee I has been allocated a special supervisory role' (free translation).

In what follows, the Committee confines itself 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.

II.1.1. METHODS WITH REGARD TO GISS

II.1.1.1. Ordinary methods

Identification of a telecommunication user

Under the Act of 5 February 2016 – following the recommendations of the Standing Committee I[95] – the identification of a user of telecommunication, such as a mobile phone number or IP address, or of a used means of communication is regarded as an ordinary method if it happens through a request to or direct access to the customer database of an operator. This was previously a 'specific method', but this changed with the addition of a new Article 16/2 to the Intelligence Services Act of 30 November 1998.[96] 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 receives the number of requests every month. This point will also be considered in the review investigation opened in 2019 (*supra*).

Identification of a prepaid card holder

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

---

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

96 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).

Access to PNR data

The Act of 25 December 2016 (*Belgian Official Journal* of 25 January 2017) introduced the possibility for the intelligence services of accessing the information held by the Passenger Information Unit by means of targeted searches (Article 16, 3° of the Intelligence Services Act and Article 27 of the PNR Act of 25 December 2016).[97] The Committee will be informed of the use of this method and may prohibit it, where appropriate.[98]

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 ordinary observation method was introduced to this end (Art. 16/4 of the Intelligence Services Act).[99] In the absence of an implementing decree, this provision has not yet entered into force.[100]

Statistics

Ordinary methods (GISS)	**Number of authorisations**
Identification of a telecommunication user	502
Identification of a prepaid card holder	0
Targeted PNR data searches	18
Referral of PNR data on basis of hits	Not provided
Use of police camera images	Not in force

97 See also the Protocol Agreement of 13 November 2018 concerning cooperation between the Passenger Information Unit and GISS in the context of the Passenger Data Processing Act (restricted dissemination, Art. 20 of the Royal Decree of 24 March 2000).

98 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.

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

100 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 opinion. This opinion 002/ VCI-BTA/2019 of 9 April 2019 can be consulted on the Committee's website (www.comiteri.be).

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)[101]	8
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)	1
Identification using technical means of the electronic communication services and resources to which a specific person has subscribed or that are usually used by a specific person and the request made to the operator of an electronic communications network or the provider of an electronic communication service to obtain payment method data, the identification of the payment 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)	5
Tracing the call-associated data of electronic means of communication and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act)	45
Monitoring of localisation data for electronic communications and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act).	43
TOTAL	**102**

[101] The Act of 21 March 2018 (*Belgian Official Journal* of 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.

II.1.1.3. Exceptional methods

GISS authorised the following 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 private 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)[102]	0
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)	1
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)	1
Collecting data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act)	12
Penetrating a computer system (Art. 18/16 of the Intelligence Services Act)	1
Tapping, intercepting and recording communications (Art. 18/17 of the Intelligence Services Act)	13
TOTAL	**28**

II.1.1.4. Interests and threats justifying the use of ordinary and special methods[103]

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;

[102] The Act of 21 March 2018 (*Belgian Official Journal* of 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.

[103] Each authorisation may involve multiple interests and threats.

- 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. **Task of ensuring the preservation of military security (Article 11, 2 of the Intelligence Services Act)**
   - the military security of personnel coming 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).**

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).

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

NATURE OF THE INTEREST	NUMBER IN 2018
Intelligence assignment	18
Military security	19
Protection of secrets	4
Monitoring the activities of foreign services in Belgium	89

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 2018
Espionage	85
Terrorism (and radicalisation process)	26
Extremism	1
Interference	18
Criminal organisation	–
Other	0

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.[104] This has not happened so far; the Committee therefore repeats its recommendation.

II.1.2. METHODS WITH REGARD TO STATE SECURITY

II.1.2.1. Ordinary methods

Ordinary methods (State Security)	**Number of authorisations**
Identification of a telecommunication user	6482
Identification of a prepaid card holder	0
Targeted PNR data searches	7
Referral of PNR data on basis of hits	Not provided
Use of police camera images	Not in force

As stated, the Committee will examine in more detail the way in which these methods are used in its review investigation launched in 2019.

104 STANDING COMMITTEE I, *Activity Report 2017*, 50–51.

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)	236
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)	1
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)	81
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)	55
Tracing the call-associated data of electronic means of communication and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act)	822
Monitoring of localisation data for electronic communications and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act).	776
TOTAL	**1971**

II.1.2.3. Exceptional methods

Exceptional methods (State Security)	**Number of authorisations**
Surveillance, whether or not using technical means, in private 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)	13
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)	25
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)	5
Collecting data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act)	80
Penetrating a computer system (Art. 18/16 of the Intelligence Services Act)	40
Tapping, intercepting and recording communications (Art. 18/17 of the Intelligence Services Act)	181
TOTAL	**344**

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;
   Radicalisation process: a process whereby an individual or a group of individuals is influenced in such a manner that this individual or group of individuals is mentally shaped or is prepared to commit terrorist acts;
3. Extremism: racist, xenophobic, anarchistic, nationalistic, authoritarian or totalitarian views or 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 2018
Espionage	815
Terrorism (radicalisation process)	1159
Extremism	312
Proliferation	5
Harmful sectarian organisations	0
Interference	24
Criminal organisations	0
Monitoring the activities of foreign services in Belgium	(included in above figures)
TOTAL	**2315**

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

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

1. The internal security of the State and maintenance of democratic and constitutional order, namely:
   a) the security of the institutions of the State and the protection of the continuity of the smooth operation of the constitutional state, the democratic institutions, the elementary principles which are inherent to every constitutional state, as well as human rights and fundamental freedoms;
   b) the safety and physical and moral protection of persons and the safety and protection of goods;
2. The external security of the State and international relations: the protection of the inviolability of the national territory, the sovereignty and independence of the State, the interests of the countries with which Belgium is striving towards a common goal, and the international and other relationships which Belgium maintains with other States and international or supranational institutions;
3. Safeguarding the key elements of the scientific or economic potential.

NATURE OF THE INTEREST	NUMBER IN 2018
Internal security of the State and maintenance of democratic and constitutional order	106
External security of the State and international relations	10
Internal and external security of the State combined	1375
Safeguarding the key elements of the scientific or economic potential	3
Activities of foreign intelligence services	821
TOTAL	**2315**

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.[105] In view of other priorities, this idea was abandoned. 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*' (*supra*).

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

105 STANDING COMMITTEE I, *Activity Report 2017*, 35, footnote 41.

satisfactory justification. The Committee must be informed of this and '*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). No such prohibition was issued by the Committee in 2018.

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[106] and an *a posteriori* check.[107] 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. Statistics

This section deals with the activities of the Standing Committee I in relation to specific and exceptional intelligence methods. Attention will only be paid to the jurisdictional decisions made in this regard and not to the operational information. However, it must first be stressed that the Committee subjects *all* authorisations to use special methods to a *prima facie* investigation, with a view to whether or not they should be referred. A member of the Investigation Service has also attended the (fortnightly) meetings at which State Security informs the SIM Commission about the implementation of the exceptional methods. A report on this subject is prepared for the Standing Committee I, giving it a better insight into the use of these methods.[108]

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

---

106 '*The assessment criteria referred to in the first paragraph, 2°, shall be submitted to the Standing Committee I in advance*' (free translation).

107 '*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).

108 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. At its own initiative;
2. At the request of the Privacy Commission/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* BCCP). 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
1. At its own initiative	16	12	16	3	1	1
2. Privacy Commission / Data Protection Authority	0	0	0	0	0	0
3. Complaint	0	0	0	1	0	0
4. Suspension by SIM Commission	5	5	11	19	15	10
5. Authorisation by Minister	2	1	0	0	0	0
6. Pre-judicial consulting body	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**

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.

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 given as a pre-judicial consulting body (Articles 131*bis*, 189*quater* and 279*bis* BCCP).

NATURE OF THE DECISION	2013	2014	2015	2016	2017	2018
Decisions prior to the referral						
1. Invalid complaint	0	0	0	0	0	0
2. Manifestly unfounded complaint	0	0	0	0	0	0
Interim decisions						
3. Suspension of method	0	3	2	1	0	0
4. Additional information from SIM Commission	0	0	0	0	0	0
5. Additional information from intelligence service	0	1	1	4	0	0
6. Investigation assignment of Investigation Service	50	54	48	60	35	52
7. Hearing of SIM Commission members	0	0	2	0	0	0
8. Hearing of intelligence service members	0	0	2	0	0	0
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	9	3	3	6	9	4
12. Partial discontinuation of method	5	10	13	4	6	6
13. Lifting or partial lifting of ban imposed by SIM Commission	2	0	4	11	0	0
14. No legal competence	0	0	0	0	0	0
15. Lawful authorisation / No discontinuation of method / Unfounded	7	4	6	2	1	1
Pre-judicial opinion						
16. Pre-judicial opinion	0	0	0	0	0	0

II.2.2.2. Jurisdiction

The final decisions delivered by the Standing Committee I in 2018 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;
– 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;
- Consequences of an unlawful method or an unlawfully implemented method.

Legal formal or other requirements prior to the implementation of a method: prior decision by the head of service and notification of the SIM Commission

Use of a method without prior decision

In dossier 2018/7250, the intelligence service in question had established in an internal audit that an irregularity had taken place: a request for identification and location data had been sent to a provider without a decision having been made by the head of service. In addition, the method concerned a journalist, for which the SIM Commission should have given a prior opinion. The SIM Commission, when informed, suspended the use of the method and the Committee confirmed this decision and had the data collected as a result of the request destroyed.

No decision from the head of service

An intelligence service wanted to use a specific method for a period of two months from a specific date. However, an agent from the service changed the start date, putting it a few days earlier. The Committee ruled '*that the "corrections" made by a State Security agent were not signed by the Director-General and therefore have no legal value whatsoever*' (free translation). The data collected before the start date stipulated by the head of service was therefore illegal. Moreover, the use of the method was not automatically discontinued at the end of the stipulated period; it was continued for two more days. This data was also obtained illegally (2018/6794).

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

Flaw in the justification of the decision

When the intelligence service in question notified the SIM Commission that part of the justification initially given for a specific method did not correspond to reality, the Commission reviewed its earlier decision and suspended the use of the method (dossier 2018/7684). The Committee, in turn, found that the justification for the SIM decision in question contained many errors. '*That the inaccuracies in the justification are such as to fundamentally and seriously undermine the justification itself. As it must therefore be concluded that Article 18/3 of the Intelligence Services Act, which states, among other things, that*

the decision of the head of service must indicate the factual circumstances that justify the specific method (…), has not been complied with. […] As the obligation to provide due justification is prescribed on pain of illegality' (free translation). The data obtained therefore had to be destroyed.

The wrong subject

In dossier 2018/7167, the intelligence service was found to have mistakenly indicated an incorrect telephone number, both in the decision and in the request to the operator. The service noticed this itself, suspended the use of the method and informed the SIM Commission. The latter in turn suspended the use of the method, and the Committee then decided that the illegally obtained data should be destroyed.

The duration of a measure

An intelligence service wished to monitor communication and location data for a period of exactly one year (dossier 2018/7464). Given the nature of the threat, this was the maximum permitted period. However, the law states that this year runs from the decision of the head of service (Art. 18/8 §2, first paragraph, 3° of the Intelligence Services Act). The start date therefore cannot be freely chosen if access to data is wanted for a whole year. The result was that the use of the method had to be 'shortened' so that the start coincided with the decision of the head of service and the end fell exactly a year later.

The same problem arose in dossier 2018/7493: an intelligence service wanted to obtain information about a telephone number for a period of nine months. Given the threat (espionage), this period was permitted. However, it was supposed to be counted from the date on which the decision was taken (Art. 18/8 §2, 2° of the Intelligence Services Act). The service failed to do this, so that the collection of telephone data was not covered by a lawful method for a period of six days.

In another dossier (2018/7470), the problem was that the decision itself did not explicitly state the period for which certain data was to be obtained. '*[T]hat the method specified a period by referring to the period of another method*' (free translation). This other SIM method did have a defined period, however, so that the Committee was certain of the intended duration. Moreover, the mention of the period is not required on pain of invalidity: '*Whereas under Art. 18/3, §2, first paragraph, 5° of the Intelligence Services Act, the decision of the head of service states the period during which the specific method may be applied, counting from the notification of the decision to the Commission; Whereas, however, only the statements referred to in 1° to 4°, 7°, 9°, 10°, 11° and 14° of Article 18/3, §2, first paragraph of the Intelligence Services Act are required on pain of invalidity*' (free translation). The method was therefore lawful, but the Committee added the

following consideration: '*Whereas, in the end, the process of not mentioning the period specific to the method but referring to that of another method, which is moreover not concurrent, does not in fact allow the Committee to assess, first, the principle of proportionality that must be satisfied by the use of any method, and second, compliance with Article 18/8 of the Intelligence Services Act; Whereas this practice therefore damages the general principle of good administration and must be avoided'* (free translation).

The subject of the use of the method

Dossier 2018/7464 described above had another omission: the decision did not mention the mobile phone number to which the use of the method would relate. '*Whereas under Art. 18/3, §2, first paragraph, 2° of the Intelligence Services Act, the decision of the head of service must, on pain of illegality, mention the subject to which the specific method may be applied; in the present case, the subject was not mentioned*' (free translation).

The legality of the implementation of a lawful method

Difference between the decision of the head of service and the request

In four decisions, the authorisation of the head of service to use a specific or exceptional method was found to be completely legal, but there was a problem with implementation in the sense that the request for the data was inconsistent with the initial warrant.

For example, the SIM Commission had noted in dossier 2018/6951 that there was a difference between the decision of the head of service to monitor means of communication and the actual request to the operator: the two documents mentioned partly different periods. The Committee therefore decided that the data relating to the days not included in the initially envisaged period had been obtained illegally.

In dossier 2018/7107 there was also a difference between the decision of the head of service and the request to the operator. Here too, the Committee decided that all collected data that fell outside the scope of the decision of the head of service should be destroyed.

In dossier 2018/7769, the head of service authorised the collection of data from a specific bank account number. However, the following request to the banking institution was much broader: the service requested all bank account numbers, bank vaults and financial instruments of the target. The Committee therefore ruled that only the request for the account number data was legal.

In connection with the use of a specific method, an intelligence service received unsolicited data from another agency about the content of conversations and not just the desired metadata (dossier 2018/7650). The intelligence service

kept the information about the content of the conversations separate and informed the SIM Commission, which decided on a ban on the use of the data. The Committee came to the following decision: '*Whereas, after an investigation carried out in accordance with Article 43/5 §§1 and 2 of the Intelligence Services Act, it appears that the request addressed to [X] in implementation of the above-mentioned decision of the head of service does not in any way mention a telephone tap in application of Article 18/17, §1 of the Intelligence Services Act, and that the implementation of this method is entirely based on a mistake by the […]; this relieves State Security of all responsibility; moreover, the [intelligence service] immediately asked [X] to interrupt the use of the method as soon as it became aware of this; Whereas the intercepted telephone data was unlawfully provided to the [intelligence service] in the absence of a valid decision*' (free translation).

Consequences of an unlawful method or an unlawfully implemented method

Moreover, in the aforementioned dossier 2018/7250, in which the data collected as a result of an illegal request had to be destroyed, it was found that the use of the method had led to the preparation of two intelligence reports. The Committee made the following recommendation on this subject: '*that the two reports, without reference, as well as any other document referring to them, using the results of the request […] may not be used and must be destroyed*' (free translation).

II.3. CONCLUSIONS AND RECOMMENDATIONS

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

- In the use of SIM methods, as always GISS focused more on the threat of espionage, followed by terrorism and interference; for State Security, the nature of the threat was primarily terrorism, followed by espionage and extremism.
- The number of special methods used by State Security continued to rise sharply in 2018. In terms of proportions, the increase was primarily in the area of exceptional methods.
- GISS also made more use of special intelligence methods in 2018, thus reversing the downward trend of recent years. However, GISS still makes significantly less use of SIMs than State Security.
- Same picture for the ordinary methods with requests made to operators to identify certain means of communication: in 2018 State Security made 6482 requests, while GISS made 502. The Committee cannot ignore the finding that the number of identifications has again increased considerably since the

introduction of the streamlined procedure under Article 16/2 of the Intelligence Services Act. The Committee did not receive any answers (in the case of GISS) or any satisfactory answers (in the case of State Security) to its questions on this matter. It was therefore decided to include the issue in a review investigation opened in 2019.

– 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 under Article 16/2 of the Intelligence Services Act. The Committee recommends the services also record these data and provide them to the Standing Committee I.
– The Committee found illegality in 11 dossiers only. The number of decisions taken by the Committee thus continues to fall, despite the significant increase in the frequency of use of SIM methods. All but one of the referrals resulted from a suspension by the SIM Commission. As the analysis shows, in a number of cases the authorisation to use a SIM turned out to be completely legal, but problems arose with implementation in the sense that the request for the data was inconsistent with the initial warrant. Other irregularities concerned a lack of justification, the absence of a prior decision by the head of service, or even the incorrect indication of the subject of the use of the method, leading the Committee to decide that the data obtained unlawfully should be destroyed.

CHAPTER III

MONITORING OF FOREIGN INTERCEPTIONS, IMAGE RECORDINGS AND IT INTRUSIONS

The Act of 30 November 1998 granted GISS limited interception powers: '*intercepting, listening to, monitoring or recording, […] for military reasons, military radio communications transmitted abroad*' (free translation).

In 2003, these powers were considerably extended, with regard to both the nature of the communication and the threat. Since then, GISS has been permitted to direct its interceptions at '*any form of communication transmitted abroad both for reasons of a military nature within the context of the duties defined in Article 11, §2, 1° and 2° of this Act and for reasons relating to the security and protection of our forces and those of our allies during operations abroad and of our nationals who are based abroad, as defined in the same Article 11, §2, 3° and 4°*' (free translation).

In view of these extended powers, a specific monitoring role was entrusted to the Standing Committee I (see below).

In 2010, the Act was again amended[109]: in addition to intercepting, listening, monitoring or recording, GISS was from then on also able to 'search' for communications. The reason for this was that, prior to any interception, listening, monitoring or recording, GISS must be able to monitor the entire electromagnetic spectrum and cyberspace, for example in order to search for and identify new operational possibilities or have sufficient information to establish with certainty that specific interceptions are permitted.

In 2017, the powers of GISS were extended for a third time, as was the monitoring role of the Standing Committee I.[110] The first part of this chapter briefly recapitulates this legislative amendment. The second part summarises the way in which the Committee carried out its specific monitoring role in this regard in 2018.

---

109 This possibility was introduced by the so-called Special Intelligence Methods Act. This Act also made it possible for State Security Service and GISS to listen to and record communications within Belgium (Art. 18/17, §1 of the Intelligence Services Act and Chapter II). A clear distinction must be made between interceptions as a special intelligence method and the security interceptions described in this chapter, in terms of both scope and control.

110 STANDING COMMITTEE I, *Activiteitenverslag 2017* (Activity Report 2017), 46–47.

III.1. POWERS OF GISS AND MONITORING ROLE OF THE STANDING COMMITTEE I[111]

In 2017, the powers of GISS in connection with security interceptions were extended. Since then, interceptions have been possible for communications transmitted or received abroad. Before the amendment of the Act, they were restricted to communications that were transmitted abroad. Moreover this possibility now applies to almost all GISS roles.[112] It is also significant that the descriptions of the GISS roles themselves were also made broader in scope by the same amendment.[113]

In addition, the Act introduced two other methods, namely 'intrusion in an IT system'[114] and the 'capture of moving images'.[115]

The way in which the Committee can monitor these methods also changed in some respects.

The review *prior* to interceptions, intrusions or image capture is done on the basis of lists drawn up annually.[116] This means that in addition to an annual interception plan, an intrusion and image plan must now also be drawn up by GISS. In these plans, GISS draws up a list of '*organisations or institutions that will be the subject of interception of their communications, intrusions in 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[117], which in turn sends the lists, with the minister's authorisation, to the Standing Committee I.[118]

---

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

112 '*[I]n the context of the roles referred to in Article 11, §1, 1° to 3° and 5 of the Intelligence Services Act*' (free translation).

113 If intervention is required in a communication network to enable the interception of communications transmitted or received abroad, GISS may request the cooperation of a network operator or the provider of an electronic communication service (Art. 44/5 of the Intelligence Services Act).

114 In this context GISS may '*proceed to penetrate a computer system that is located abroad, disable its security features, operate technical procedures on it in order to decipher, decode, save and manipulate the data stored, processed or forwarded by the computer system, as well as disrupt and neutralise the computer system*' (Art. 44/1 of the Intelligence Services Act) (free translation).

115 In this context, GISS may '*use resources abroad for the capture of fixed or moving images*' (Art. 44/2 of the Intelligence Services Act) (free translation).

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

117 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.

118 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

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 has been considerably tightened up. It 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 in case of 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). However, the Royal Decree referred to here has not yet been issued. The Committee recommends doing so as soon as possible. The Committee must provide a detailed justification of its decision and communicate it to the minister and GISS.

III.2. REVIEW ACTIVITIES CARRIED OUT IN 2018

III.2.1. REVIEWS PRIOR TO INTERCEPTION, INTRUSION OR RECORDING

The Standing Committee I made a number of important comments on the 'Interception Plan 2017'. The most important comments concerned the differences in priority between, on the one hand, the Intelligence Steering Plan[119] and, on the other, the intended SIGINT interceptions, and the fact that 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.

119 A plan prepared by the Intelligence Directorate of GISS setting out the countries to be monitored and the prioritisation.

definition of the organisations and institutions that were to be the object of interceptions was too general. In the 'Interception Plan 2018', which was sent to the Committee at the end of April 2018, GISS described in more detail the organisations that could be the object of interceptions. The Committee only had a few minor comments to make on the plan.

The Standing Committee I was also provided with the – rather scanty – image and intrusion plan in mid-February 2018. The Committee 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).

III.2.2. REVIEWS DURING INTERCEPTION, INTRUSION OR RECORDING

At the end of 2018, the Committee visited the installations from which the interceptions take place. During the visit, the Committee checked whether there were any differences between the targets approved in the interception plan and the interceptions being carried out at that time. No irregularity was found.

III.2.3. REVIEWS AFTER THE USE OF THE METHOD

The Committee received nine '*monthly lists*[120] *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°*' (free translation).

The review of the monthly intrusion and image capture lists will be carried out in the context of the 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).

As required, the Committee also carried out a review of the logs that have to be kept in connection with interceptions. Only a few administrative irregularities were noted.

Finally, the Committee carried out for the first time a review of the analysis output prepared in the context of international SIGINT cooperation.

---

120 These nine reports related to the twelve months of the year.

III.2.4. FINDINGS AND CONCLUSIONS

During working meetings and inspections, the Committee found that GISS was making every effort to continue the reforms initiated in the area of national and international cooperation and on the technical front.

In order to achieve its objectives and to be able to perform its statutory duties, GISS needs to have sufficient human and technical resources in the SIGINT field. In 2018, as previously, it was concluded that the recruitment of personnel to handle translations must be a priority in this regard.

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

As mentioned earlier[121], the Standing Committee I had already taken 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[122], 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 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

121 See 'Chapter I.2. The activities of GISS in a foreign operations zone'.

122 Protocol agreement of 24 May 2018 between the CHOD and GISS regarding the HUMINT and analysis capabilities of the ISTAR Bn.

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 report on each investigation assignment. The Committee received a number of these reports in 2018. The analysis of these reports will be the object of further investigation.

IV.2. MONITORING OF SPECIAL FUNDS

On behalf of the Chamber of Representatives, the Court of Audit oversees the use of financial resources by government services. 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 Service and GISS (in particular the 'special funds' including spending on operations and informants, for example) is not examined by the Court of Audit. For State Security Service, this expenditure is audited by the General Policy Director of the minister of Justice. Midway through 2018, the Court of Audit expressed its intention of conducting a periodic audit of these funds from the closure of the 2018 account.

The audit of the GISS special funds is conducted by a representative of the office of the minister of Defence four times a year. Since 2010 this has been done in the presence of the chair of the Standing Committee I, and the chair was duly present at these four audits in 2018.

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, the Belgian intelligence services (may) monitor political representatives and which rules they must observe in that regard.

Previously, there were two directives that obliged State Security to notify the minister of Justice if politicians were the subject of intelligence activities: a ministerial directive of 25 May 2009 (drawn up in response to recommendations of the Standing Committee I as part of an earlier review investigation[123, 124]) and

---

123 STANDING COMMITTEE I, *Activity Report 2008*, 24–34 ('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.).

124 The recommendation was as follows: *'More generally speaking, the Standing Committee I wants State Security to develop clear and unambiguous guidelines with regard to the collection,*

an internal instruction of 27 March 2012. The directive of 25 May 2009 stipulated that the minister of Justice had to be informed whenever the name of a current federal member of parliament was mentioned in a report. The scope of the internal instruction of 27 March 2012 was both narrower and broader than that of the ministerial directive: on the one hand, it related only to any reference made in the reports of State Security's external services but, on the other hand, included all ministers and political representatives, including those of the Communities and Regions.[125]

From 1 January 2018, a new service memorandum (classified as confidential) of 13 December 2017 is applied within State Security. 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 and a quarterly overview of all documents in which political representatives are mentioned.

The Minister of Justice previously agreed with *'[le] principe de vérifications par le Comité R qui s'avèrent nécessaires conformément à la loi organique du 18 juillet 1991*'.[126] In line with its reporting obligation, State Security kept the Committee informed about both types of reports.

Despite repeated requests, the Committee was unable to obtain any information from GISS on this subject.

The Standing Committee I intends to perform a legality test on these files on a random-sample basis.

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.

---

processing, cons ultation (including internal shielding, if any), storage, and archiving of data regarding certain categories of persons who have or had special responsibilities. For the development of these guidelines and the actual monitoring of (former) political representatives, State Security must take into consideration the guidelines outlined in the judgement of the European Court for Human Rights in the case Segerstedt-Wiberg and Others v. Sweden.'

125 For more detailed information see: STANDING COMMITTEE I, *Activity Report 2013*, 117 *et seq.* ('II.4. Monitoring of political representatives by the intelligence services'). Also see STANDING COMMITTEE I, *Activity Report 2013*, 106 *et seq.* ('II.2. Confidential memoranda about the Church of Scientology in the press') and 112 *et seq.* ('II.3. An informant within Vlaams Belang?').

126 '*the oversight/verification principle that appears necessary under the terms of the Organic Act of 18 July 1991.*' (free translation). In: Letter from the Minister of Justice to the Standing Committee I of 26 July 2018 on *'Le recueil d'informations par un service de renseignement concernant une personne exerçant un mandat politique*'.

For decades all kinds of theories have been put forward about its cause.[127] In a publication by Susan Williams, a researcher at the University of London[128], several hypotheses regarding the crash of the UN plane were examined; the author decided that all the evidence pointed to a deliberate intervention by one or more aircraft, and the names of Belgians active in the region at the time were among those that came up. Williams called for the truth to be brought to light by opening the 'intelligence, security and defence archives' of countries involved in the conflict in Congo at that time, such as the US, the United Kingdom, France, Germany, South Africa but also Belgium.

Former UN Secretary-General Ban Ki-Moon picked up on the idea and launched a new investigation, led by Eminent Person Mohamed Chande Othman. The United Nations adopted a Resolution on this subject on 24 December 2017[129], 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. Othman also wanted to know from the 'independent persons' appointed by the Member States about any difficulties they encountered in their investigation (such as the denial of access to certain archives).

On 16 April 2018, the Ministers of Justice and Defence appointed the then chairman of the Standing Committee I, Guy Rapaille, 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. The Chairman of the Monitoring Committee was informed of this appointment in April 2018. The chairman of the Standing Committee I took responsibility for the classified information from the archives of State Security and the General Intelligence and Security Service, while Quanten investigated the archives of the Ministry of Defence. They submitted their report to the UN in late September 2018. Their conclusion, *'after a thorough and meticulous analysis of these archives, is that they do not contain any direct information related to the death of Dag Hammerskjöld. Although, some elements which may shed an additional light on the proposed research, have been selected'*.

In early November 2018, the United Nations General Assembly received a first interim report from Othman.[130] This revealed, among other things, that

---

127 Partly as a result of research by G. BJÖRKDAHL (J. BORGER, *The Guardian*, 17 Aug 2011, 'Dag Hammarskjöld: evidence suggests UN chief's plane was shot down').

128 S. WILLIAMS, *Who killed Hammarskjöld? The UN, the cold war and white supremacy in Africa*, Hurst Publishers, London, 2016.

129 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).

130 See: www.hammarskjoldinquiry.info/pdf/ham_187_EP_interim_report_081118.pdf.The report was explained orally on 3 December 2018 (Oral briefing by Mr Miguel de Serpa Soares,

neither South Africa nor the United Kingdom had appointed experts. With regard to the Belgian part of the investigation, it was stated that the two experts *'provided a comprehensive interim report indicating the substantial work undertaken by them. The interim report confirms that full access*[131] *was given by Belgium to all files and archives kept by the Ministry of Defence, the State security Service (VSSE) and the General Intelligence and Security service (GISS, military intelligence service). The report observes that the mandate has not covered a review of the archives of non-state actors or private organisations. The interim report from Belgium identifies information relevant to the presence of foreign paramilitary and intelligence personnel in and around the Congo at the relevant time, as well as to the capacity of the aerial forces of Katanga.*'[132]

Following Guy Rapaille's retirement, the Ministers of 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.

Under-Secretary-General for Legal Affairs and United Nations Legal Counsel). The theme was the subject of further publications in early 2019 (E. GRAHAM HARRISON et al., *The Observer*, 12 Jan 2019, 'Man accused of shooting down UN chief').

131 However, the Belgian report did state that the fact that *'the searching of archives of the military intelligence service GISS and of het Ministry of Defence has yielded less useful documentation than at the State Security Service, can be called somewhat astonishing. […] It should be noted that, at this stage, all GISS sub-archives have not yet been fully investigated.*'

132 See: www.hammarskjoldinquiry.info/pdf/ham_187_EP_interim_report_081118.pdf.

CHAPTER V

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

V.1. NEW EUROPEAN LEGAL INSTRUMENTS WITH SIGNIFICANT EFFECTS AT NATIONAL LEVEL

On 4 May 2016, two important legal instruments relating to the processing of personal data were published in the Official Journal of the European Union: the General Data Protection Regulation 2016/679 (GDPR)[133] and Directive 2016/680 (the Directive).[134] Both instruments regulate the actions of public- and private-sector bodies when they collect, store, retain and transfer personal data: when is such processing legitimate and fair? What rights does the data subject have and what are the exceptions to these rights? Who is the data controller and who is the processor? Can personal data be transferred to third countries? Who is the supervisory authority? What sanctions apply in the event of breaches? – and so on.

The GDPR, which entered into force on 25 May 2018, and the Directive gave rise to a number of important legislative changes at national level. For example, the Act of 8 December 1992 on the protection of privacy with regard to the processing of personal data was repealed and the Commission for the Protection of Privacy (the Privacy Commission) was replaced under the Act of 3 December

---

133 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.

134 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.

2017 by the Data Protection Authority (DPA).[135] In addition, an entirely new Data Protection Act was approved.[136]

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'. Such processing activities fall outside the scope of EU law and are therefore not covered by the GDPR or the Directive, but Parliament opted to subject the services performing such processing to the same data protection rules to a certain extent.

This was in fact already the case in the past: the 1992 Privacy Act was only partially applicable to processing carried out by State Security, GISS, the security authorities, security agents and the Standing Committee I and its Investigation Service. There is nothing surprising about the fact that certain data protection rules applied to these services, since Belgium is bound by the Council of Europe Convention 108 of 28 January 1981 relating to the protection of individuals with regard to automatic processing of personal data.[137] As far as Belgium is concerned, this Convention also applies to services that process data relating to national security. Moreover, the Additional Protocol to this Convention also applies in Belgium.[138] It contains specific rules with regard to independent supervisory bodies and information exchange across national borders.

In what follows, the new role of the Standing Committee I is first explained. This role is described in the Act of 3 December 2017 establishing the Data Protection Authority (DPA Act), in the Data Protection Act (DP Act) and in the Review Act, in which a number of changes were made. The Committee was involved, initially in an informal manner and subsequently formally, in the establishment of this new system.[139] As will be seen, some further changes were made to the text by Parliament. Nevertheless, the new system will need to be further amended or supplemented on a number of important points. The second part briefly considers the Standing Committee I as a processor of personal data. Finally, the first activities of the Committee as 'Competent Supervisory Authority' (CSA) are described.

---

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

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

137 Https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/verdrag_108.pdf.

138 Https://www.gegevensbeschermingsautoriteit.be/sites/privacycommission/files/documents/aanvullend_protocol_verdrag_108.pdf.

139 The Committee's opinion provided at the request of the Parliamentary Committee on Justice can be found on the Committee's website (www.comiteri.be). On 26 June 2018, the Chairman of the Committee presented its opinion orally at a session of the competent Parliamentary Committee. On this opinion, see also 'Chapter VII. Opinions '.

V.2. NEW ROLES FOR THE COMMITTEE AS A COMPETENT SUPERVISORY AUTHORITY

The new roles of the Committee and the way in which they must be performed are set out in various provisions of the Data Protection Act and the Review Act. They are summarised below. First, however, an indication is given of the processing activities for which the Committee is competent, and how the Committee relates to the other Competent Supervisory Authorities.

V.2.1. FOR WHAT PROCESSING ACTIVITIES OF WHAT SERVICES AND INDIVIDUALS IS THE COMMITTEE COMPETENT?

The Standing Committee I is competent for the monitoring of all or certain personal data processing activities by several services, authorities and individuals, which are listed in Title 3 of the Data Protection Act.

- Subtitle 1 specifically relates to all processing activities by State Security and GISS (Articles 73 and 95 DP Act);
- Subtitle 3 refers to any processing of personal data in the context of security clearances, certificates and advice as referred to in the Act of 11 December 1998 by the National Security Authority (NSA) and any member of that authority, the other security authorities as referred to in Articles 15, second paragraph and 22*ter* of the Classification and Security Clearances Act and the security agents referred to in Article 13, 1° of the Classification and Security Clearances Act or their processors (Articles 107 and 128 DP Act)[140];
- Subtitle 4 deals with any processing of personal data by CUTA and its processors, '*carried out in the context of the tasks referred to in the Act of 10 July 2006, and pursuant to special laws*' (free translation) (Articles 139 and 161 DP Act). Processing activities by supporting services of CUTA are therefore not referred to here;
- Subtitle 5 deals with any processing of personal data by the Passenger Information Unit (PIU) in the context of the purposes referred to in Article 8, §1, 4° of the Act of 25 December 2016, or in other words, processing activities with a view to '*oversight over activities referred to in Articles 7, 1° and 3°/1, and 11, §1, 1° to 3° and 5° of the Act of 30 November 1998 governing the*

140 This subtitle also applies to any processing of personal data by the Appeal Body in connection with the appeal procedures referred to in the Act of 11 December 1998 establishing the Appeal Body. However, in this context the Committee does not play the role of Competent Supervisory Authority (Art. 128 §2 DP Act).

intelligence and security services' (free translation) (Articles 169 and 184 DP Act);[141, 142]
– Finally, Subtitle 6 deals with processing activities by the SIM Commission (Art. 185 DP Act).

Each of these services or persons has specific data protection obligations. Although they are broadly similar, there are a few differences. For example, as far as the SIM Commission alone is concerned, the Standing Committee I is stipulated as the CSA. The rules that the SIM Commission must follow when processing personal data and the rights of the citizen were only very briefly described in the Data Protection Act. However, the few general provisions from the Review Act also apply to the SIM Commission.

V.2.2. WHAT COOPERATION IS THERE BETWEEN THE COMPETENT SUPERVISORY AUTHORITIES?

Belgium has four competent supervisory authorities at federal level. As well as the Standing Committee I, there is the Data Protection Authority (DPA) – the successor to the Privacy Commission – 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 that in certain cases there must or may be cooperation or that information must be exchanged. For example, Articles 98 and 131 of the DP Act stipulate that the other CSAs must inform the Standing Committee I about breaches of the rules governing the processing of personal data by the intelligence services or security authorities as soon as they become aware of them. They must also consult with the Committee when they are involved in a case that may have consequences for the processing

141 In this regard, see: Protocol Agreement of 13 November 2018 concerning cooperation between the Passenger Information Unit and GISS in the context of the Passenger Data Processing Act (restricted dissemination, Art. 20 of the Royal Decree of 24 March 2000).

142 On the relation between the data protection officer of the Passenger Information Unit and the Standing Committee I, see also Article 27 of the Royal Decree implementing the Act of 25 December 2016 on passenger data processing, containing various provisions regarding the Passenger Information Unit and the data protection officer, *Belgian Official Journal* 29 December 2017.

of personal data by one of these bodies.[143] Furthermore, the CSAs must in certain cases exchange investigation reports (*infra*).

More important, however, 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 will be performed by the Data Protection Authority. The CSAs are also required to agree on a protocol in order to achieve the required cooperation.

Finally, the legislators provided 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.

V.2.3. WHAT NEW ROLES?

V.2.3.1. Conducting investigations

Who can initiate an investigation?

The Committee may, on its own initiative or at the request of a competent authority, initiate investigations into the processing of personal data by the intelligence services (and the persons and authorities mentioned above[144]) and their processors (Art. 33 Review Act). It thus '*watches over the […] protection of the fundamental rights and freedoms of natural persons with regard to this processing*' (free translation) (Articles 95 and 128 DP Act; see also Article 144 DP Act).

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 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).[145] If the

---

143 For the other services to be monitored by the Standing Committee I, no similar provision was included in the DP Act. This is clearly an oversight on the part of the legislators.

144 Article 33 Review Act refers only to the intelligence services and not to the other persons and authorities for whom the Committee is the competent data protection authority. The Committee assumes that this is an oversight.

145 This provision also states that the request '*[must] justify the identity of the data subject*.' It is not immediately clear what this means. Probably it means that the data subject must provide

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.[146]

In addition, Article 51/1 of the DP Act states that the Committee '*shall act in its capacity as a data protection authority […] on its own initiative, either at the request of another data protection authority or at the request of any data subject*' (free translation). This provision thus opens up the possibility for the DPA, the Supervisory Body for Police Information or the Standing Committee P to refer a request to the Standing Committee I. A referral by the DPA or by the Supervisory Body for Police Information will, for example, be required if a request or complaint is submitted to the DPA (Art. 11 §5 DP Act) or to the Supervisory Body for Police Information (Art. 45 §6 DP Act) in which the data controller mentions the fact that it processes data from, for example, an intelligence service or from CUTA.[147] In this case, the DPA or Supervisory Body for Police Information is not allowed to handle the case itself, but must refer it to the Standing Committee I, which will then carry out the necessary checks.

What investigative powers and possibilities does the Standing Committee I hold?

The monitoring of processing activities is conducted '*in accordance with the detailed rules set out in the Act of 18 July 1991*' (free translation) (Art. 95 DP Act; see also Articles 106, 5°, 161 and 174 DP Act). In other words, here too, the Committee may use all the powers which it holds in the context of its traditional review role.

In addition, the Committee may, if necessary, cooperate with the other Belgian supervisory authorities, without prejudice to '*the physical integrity of persons, or the duties of the intelligence and security services and the Act of 11 December 1998*' (Art. 96 DP Act), or provided that this is done '*in compliance with the Act of 11 December 1998*' and '*without precluding the interests referred to in Article 5 of the Act of 11 December 1998 on the establishment of an Appeal Body*' (Art. 129 DP Act) (free translations).

Finally, the Data Protection Act imposes an obligation of cooperation on the monitored services in two cases (the other cases have clearly been overlooked) (Articles 97 and 130 DP Act).

---

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).

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

147 Art. 11 DP Act only mentions in its first paragraph data from the two intelligence services and CUTA. In the remainder of the provision and in the similar Art. 45 DP Act mention is made of '*processed data deriving directly or indirectly from the authorities referred to in Title 3*' (free translation). This seems to be more in line with the intention of the legislators.

Decisions of the Standing Committee I

A new Section 4 of Chapter III of the Review Act describes the decisions that the Standing Committee I can take in its capacity as a data protection authority (Art. 51/3 of the Review Act). It can:

- conclude that the processing has been carried out in accordance with the provisions of the regulations concerning the processing of personal data;
- warn the relevant service or its processor that a planned processing of personal data may violate the regulations;
- reprimand the service concerned or its processor if a processing activity has resulted in the violation of a data protection rule;
- order the service or processor to bring a processing activity into line with the relevant provisions, where appropriate, in a specified manner and within a specified period;
- impose a temporary or definitive processing restriction, including a processing ban;
- order the rectification or deletion of personal data;
- refer the case to the Brussels public prosecutor, who will inform the Committee of what action it has taken on the case.

Notification or reporting by the Standing Committee I

Various rules determine which person, services or authorities the Committee should inform, and in what manner, of the result of its monitoring.

For example, the report on investigations started on its own initiative or at the request of a competent authority must be sent to the competent minister or government agency and to the Chamber of Representatives (Article 33, third paragraph of the Review Act). The findings of the investigation will, depending on the case, be communicated to the managing officer of the intelligence service or the director of CUTA (Art. 34, last paragraph of the Review Act) or – here too, the legislators have neglected to provide a general rule – to any other person or service concerned.

In the event of an investigation following a complaint from a citizen, the Committee will merely inform the latter that '*the necessary verifications have been made*'.[148] The managing officer of the intelligence service or the director of CUTA – and, the Committee assumes, any other body or person – will receive '*the conclusions of the investigation*' (free translations) (Art. 34, last paragraph of the Review Act).

148 See also Articles 80, 114, 146 and 174 DP Act. In an 'ordinary' complaint investigation, the Committee may, when the investigation is closed, communicate the result '*in general terms*' (free translation) (Article 34 of the Review Act).

If another supervisory authority initiated an investigation (e.g. Articles 11 §5, 45 §6 and 51/1 DP Act), the Committee sends its '*response*' to this other authority which in turn informs the data subject, but only of '*the results of the verification that relate to personal data that does not derive from the intelligence service or CUTA*'(free translation).[149]

In addition, Articles 96 and 128 of the DP Act provide that, '*in the context of the exercise of supervision referred to in Article 95, […] the Standing Committee I shall in general terms communicate the result thereof to the other competent supervisory authorities*' (free translation). No similar obligation has been introduced for investigations into other bodies. Moreover, only for investigations relating to the intelligence services has it been specified that the other CSAs may not disclose the Committee's investigation results to the data subject (Art. 95 DP Act).

Finally, account must be taken of Article 51/4 of the Review Act. Under this provision, the intelligence service in question must be notified if the investigation concerns a processor from that service. This provision also states the following: *'If it becomes aware of them, the Standing Committee I shall also inform the service concerned of violations of the regulations concerning the processing of personal data by other data controllers'* (free translation).

V.2.3.2. Issuing opinions

The Committee may in two circumstances issue an opinion '*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 (Art. 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.[150] 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.

V.2.3.3. Handling of offences reported by Investigation Service I

If a member of the Investigation Service I becomes aware of a crime or offence, he or she must draw up a formal report that is sent to the public prosecutor (Art. 46 of the Review Act). This rule does not apply to the offences described in

149 If the request or complaint relates only to personal data from an intelligence service or CUTA, the DPA or the Supervisory Body for Police Information will respond, after receiving confirmation from the Standing Committee I that the necessary verifications have been conducted.

150 See 'Chapter VII. Opinions'.

Articles 226, 227 and 230 DP Act.[151] In those cases, the service must inform the Standing Committee I as soon as possible which '*will ensure the follow-up in accordance with the detailed rules set out in Article 54*[152] *[of the Review Act]*' (free translation).

V.2.3.4. Information from the monitored services

The services monitored by the Committee must keep or make certain information available to the Standing Committee I[153] in the following circumstances:

- log files and other data if an intelligence service or the SIM Commission has direct access to or the right to consult a database belonging to a private- or public-sector body (Articles 13 and 47 DP Act);
- 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 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[154]).

V.2.3.5. Decisions about the dismissal of a Data Protection Officer

Each service monitored by the Committee is required to appoint a Data Protection Officer (DPO) who must be able to operate independently. This person therefore cannot be penalised for performing his or her duties. A dismissal is only possible if he or she is guilty of gross misconduct or no longer fulfils the conditions for the exercise of the role. He or she can contest this decision with the Standing Committee I (Articles 91, 124 and 157 DP Act[155]).

---

151 The same exception has also been included if the Investigation Service discovers an offence as referred to in Art. 13/1 of the Intelligence Services Act.

152 In all likelihood, this is a mistake and reference should be made to Art. 51/3 of the Review Act.

153 Not every service has to keep or provide all of the data mentioned here. This is unlikely to have been the intention of the legislators. This is certainly true of the SIM Commission, which apparently is not required to communicate any information to the Standing Committee I.

154 No similar provision was included for the Passenger Information Unit. This was probably an oversight on the part of the legislators.

155 *Idem*.

V.2.3.6. Drafting of an annual report

Under Article 35 §3 of the Review Act, the Standing Committee I '*shall report annually to the Chamber of Representatives on the 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). A copy of this report is sent to the competent ministers and to the two intelligence services[156], who have the option of submitting comments to the Standing Committee I.

V.3. THE STANDING COMMITTEE I AS A PROCESSOR OF PERSONAL DATA

A provision has been included in the Data Protection Act that permits the Standing Committee I to process, '*to the extent necessary for the performance of its duties, personal data of all kinds, including those revealing racial or ethnic origin, political views, religious or philosophical beliefs or membership of a trade union, as well as genetic and biometric data, data on health, data relating to sexual behaviour or sexual orientation, and data relating to criminal prosecutions and to breaches or associated security measures*,' doing so '*in the context of its duties referred to in the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment, in the Act of 30 November 1998 governing the intelligence and security services, and in special laws*' (free translation) (Art. 185 §1 DP Act).

In order to guarantee the confidentiality and effectiveness of the performance of these duties, the data subject's access to these personal data is limited to what is provided for in the special laws. However, the data subject has the right to ask for any inaccurate personal data to be rectified or erased.

Article 185 §4 of the DP Act states that the Committee, '*in the context of its duties as a supervisory authority, is not subject to the supervision of the Data Protection Authority referred to in the Act of 3 December 2017 establishing the Data Protection Authority*' (free translation).

The above rule only relates to data processing activities relating to national security. Other processing activities, such as the management of its own personnel, fall under the normal data protection rules.

Finally, it should be noted that the Investigation Service I, with regard to its judicial duties, falls under the supervision of the Supervisory Body for Police Information in its capacity as a Competent Supervisory Authority.

156 Again, the text of the law erroneously fails to mention the other persons and authorities listed in Title 3 of the Data Protection Act.

V.4. ACTIVITIES OF THE STANDING COMMITTEE I AS A COMPETENT SUPERVISORY AUTHORITY

V.4.1. PREPARATORY WORK

In 2018 the Committee made numerous preparations to fulfil its new duties and obligations.

Firstly, a Data Protection Officer (DPO) was appointed to deal with all processing activities carried out by the Committee that fall outside 'national security' (for example, processing in the context of personnel management and logistics).

In addition, various meetings were held with the three other competent supervisory authorities. Discussions at these meetings concerned the drafting of a protocol in which, among other things, the 'one-stop shop mechanism' for citizens will be worked out, practical working arrangements and the exchange of best practices.

Initial 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.

V.4.2. EIGHT DPA ADVICE

In 2018 the Committee, working alone or together with the Standing Committee P, issued eight opinions on draft bills or draft decrees. These opinions may be consulted in full on the Committee's website. A list of the opinions issued is sufficient here:

- Opinion 001/VCI-BTA/2018 of 26 September 2018 on '*draft Royal Decrees implementing the Act of 25 December 2016 on passenger data processing, which sets out the respective obligations for bus transport companies and high-speed rail transport and ticket distributors*' (free translation);
- Opinion 002/VCI-BTA/2018 of 26 September 2018 on '*the preliminary draft bill on the organisation of prison services and the status of prison personnel*' (free translation), which included provisions on the screening of applicants for jobs as prison officers;
- Opinion 003/VCI-VCP-BTA/2018 of 26 September 2018 in connection with the same preliminary draft bill, issued together with the Standing Committee P since the draft text stated that the screening of these applicants should be partly based on data from CUTA;

- Opinion 004/VCI-BTA/2018 of 1 October 2018 on '*the preliminary draft bill amending the Act of 21 December 2013 on the Consular Code and the Act of 10 February 2015 on automated processing of the personal data necessary for Belgian passports and travel documents*' (free translation);
- Opinion 005/VCI-VCP-BTA/2018 of 1 October 2018 in connection with the same preliminary draft bill, issued together with the Standing Committee P since the draft text also referred to CUTA;
- Opinion 006/VCI-BTA/2018 of 24 October 2018 on the '*preliminary draft bill containing various provisions on the computerisation of the justice system and modernisation of the status of judges in corporate cases*' (free translation) in which reference was made to a right for the intelligence services to access the SIDIS Suite;
- Opinion 007/VCI-VCP-BTA/2018 of 24 October 2018 in connection with the same preliminary draft bill, issued together with the Standing Committee P since reference was made to a right for CUTA to access the SIDIS suite;
- Opinion 008/VCI-BTA/2018 of 16 November 2018 on the '*preliminary draft bill containing various provisions in criminal cases*'(free translation) which introduced new methods of intelligence and protection and support measures.

V.4.3. TWO INDIVIDUAL DPA COMPLAINTS

In 2018 the Standing Committee I received five DPA complaints from citizens regarding potential processing of personal data by State Security and GISS, two of which were fully dealt with in 2018. The required verifications were carried out in both cases. The complainants were informed of this.[157]

157 *'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'* (free translations) (Art. 80 DP Act), so no further explanation may be provided.

CHAPTER VI
MONITORING OF THE COMMON DATABASES

In 2016, the Act of 5 August 1992 on the police function (the Policing Act) was amended: a statutory basis was created for the establishment of common databases in connection with the prevention and monitoring of terrorism and extremism that can lead to terrorism.[158] The underlying idea was to allow different services to share their data and information in order to be more effective in the fight against these phenomena.

On the basis of this new possibility, the Ministers of Home Affairs and Justice set up the common database of foreign terrorist fighters (CDB FTF) in 2016.[159] Its purpose was to contribute to the analysis, evaluation and monitoring of individuals with links to this issue.

In 2018[160] 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[161] of 'hate propagandists' (CDB HP). These changes and additions will be explained in the first part of this chapter (VI.1).

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. This supervisory task is discussed in the second part of the chapter (VI.2).

The two bodies also issued a joint opinion on two 'prior reports' submitted by the competent ministers in 2018. As required, these reports set out the details of

158 Act of 27 April 2016 on additional measures to combat terrorism, *Belgian Official Journal* 9 May 2016.

159 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 Act, *Belgian Official Journal* 22 September 2016.

160 Royal Decree of 23 April 2018 amending the aforementioned Royal Decree of 21 July 2016 and redesigning the common database of foreign terrorist fighters as the common database of terrorist fighters, *Belgian Official Journal* 30 May 2018 (RD TF).

161 Royal Decree of 23 April 2018 on the common database for Hate Propagandists and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Policing Act (RD HP).

how the new database and the expanded database will function. A third section of this chapter summarises the opinions formulated in this context (VI.3).

VI.1. CHANGES IMPLEMENTED IN 2018

VI.1.1. FROM FOREIGN TERRORIST FIGHTERS TO TERRORIST FIGHTERS

The database has been changed to include intelligence records on both foreign terrorist fighters (the original category from 2016) and homegrown terrorist fighters (the category added in 2018).

Apart from two adjustments that will be discussed below, the Royal Decree of 23 April 2018 made no changes to the functioning of the common database established in 2016.[162]

This expansion was considered necessary in view of the many attacks in Europe since 2016 which have been of a jihadist nature or linked to the far right, but which have not had any direct link to a jihadist conflict zone. The modification enables personal data and information on homegrown terrorist fighters also to be included in the database.

Homegrown terrorist fighters are persons with links to Belgium for whom at least one of the following criteria is met:

a) there are serious indications that the person intends to use force against persons or material interests for ideological or political reasons with the aim of achieving his or her objective by means of terror, intimidation or threats;
b) there are serious indications that he or she is deliberately providing support, including logistically, financially or for training or recruitment purposes, to persons referred to in a) or to persons registered as FTFs and for whom there are serious indications that they intend to carry out a violent action (Art. 6, §1, 1°/1 RD TF).

The data of persons who meet these requirements can be included in the database. The same applies to persons for whom there are serious indications that they could meet these criteria, so that additional personal data or information can be collected that may or may not confirm that the person concerned meets the criteria for terrorist fighters.

---

[162] For a detailed discussion of the functioning of the common databases, see STANDING COMMITTEE I, *Activiteitenverslag 2016* (Activity Report 2016), 127–139 (www.comiteri.be).

VI.1.2. THE ESTABLISHMENT OF A COMMON DATABASE OF HATE PROPAGANDISTS (HP)

The Royal Decree of 23 April 2018 (RD HP) created a new common database of hate propagandists.

This database is complementary to the CDB TF and focuses in particular on the radicalising influence that often lies behind the perpetration of acts of terrorism or extremism that can lead to terrorism. The aim is to bring together data and information about vectors of radicalisation (natural persons, legal entities, de facto associations) and the resources they use.[163] The shared data and information are intended to contribute to the analysis, evaluation and monitoring of these entities.[164]

The CDB HP is primarily aimed at natural persons or legal entities, regardless of their nationality or where they live or have their head office, meeting the following combined conditions:

a) they are harmful to the principles of democracy or human rights, the proper functioning of democratic institutions or other principles of the rule of law. It is not necessary for any damage of this nature to have already occurred: potential damage is sufficient;
b) they justify the use of violence (physical and psychological violence, violence within and outside the family, homophobic violence, cyberattacks, etc.) or coercion as methods of action. Hate propagandists express their intention to do harm and justify the use of violence or coercion through concrete actions or channels. This intention must be openly advertised (e.g. through a publication);
c) they spread this conviction to others with the intention of exerting a radicalising influence. The hate propagandist seeks to support or contribute to the radicalisation process;
d) there are links with Belgium.

Those for whom there are serious indications that they meet these criteria will be included in the CDB HP for a maximum of six months. When this period expires, the data is deleted unless the entity is found to meet the criteria.

The functioning of this database is identical to that of the CDB TF. The protagonists are also the same: the Ministers of Home Affairs and Justice are the data controllers, the Federal Police has been designated as the administrator (Art. 3 RD HP) and CUTA as operational manager (Art. 4 RD HP). The position

163 For example websites, tracts, messages on radio or TV, radio stations or television channels, cultural or propaganda centres, rooms, etc.

164 This database replaces the 'Joint Information Box' (JIB) that was managed by CUTA. The JIB was the subject of a joint review investigation I and P (STANDING COMMITTEE I, *Activity Report 2015*, 107–111).

of security and privacy adviser has also been included (Art. 5 RD HP). However, it has not been specified which person or service should perform this role.

VI.1.3. COMMUNICATION OF INFORMATION CARDS TO THE LIVC-R

Another change that took place in 2018 was the result of the establishment of local integrated security units on radicalism, extremism and terrorism (LIVC-Rs).[165] The LIVC-R is a platform where specialists from local government and local social prevention organisations come together to come up with a case-by-case approach to radicalised persons. The formation of an LIVC-R is the responsibility of the mayor. Article 4 of the Act of 30 July 2018 authorises the local chief of police (or the representative appointed by him or her) to communicate to the members of the LIVC-R the information card of a person whose case is being discussed. This information card is an extract from the intelligence record and contains personal data and information that is strictly limited to what the recipient needs to know (Article 44/11/3*quater* Policing Act and Article 11 RD FTF).

VI.1.4. DIRECT ACCESS FOR THE NATIONAL SECURITY AUTHORITY

The Royal Decrees of 23 April 2018 granted the National Security Authority direct access to the databases, in connection with its competence for granting security clearances, certificates and advice.

VI.1.5. NEW DIRECTIVE ON THE EXCHANGE OF INFORMATION

On 22 May 2018, the Ministers of Home Affairs and Justice issued a circular letter concerning the exchange of information on and the monitoring of terrorist fighters and hate propagandists. This directive – which has been classified as 'Restricted dissemination' – regulates in detail the functioning of the common databases and determines the role of all actors, such as the police and intelligence services, CUTA, the Local Task Force and the LIVC-R.

---

165 Act of 30 July 2018 establishing the local integrated security units on radicalism, extremism and terrorism, *Belgian Official Journal* 14 September 2018.

VI.2. MONITORING ASSIGNMENT

VI.2.1. OBJECT OF MONITORING

The Supervisory Body for Police Information and the Standing Committee I jointly monitored the implementation of certain recommendations they had made in 2017. In addition, it was decided to check the way in which information was provided to mayors and to third parties by the local police chiefs and the basic services.[166]

VI.2.2. FOLLOW-UP ON THE RECOMMENDATIONS MADE IN 2017

VI.2.2.1. A statutory basis for the processing of data on HTFs and HPs

The Supervisory Body for Police Information and the Standing Committee I noted in their 2017 report that data on hate propagandists and homegrown terrorist fighters was being processed without the RD FTF having been modified or a new Royal Decree having been issued. This omission was remedied by the Royal Decrees published in May 2018.

However, the necessary 'prior reports' were not made. After reminders had been sent to the data controllers, these reports were received at the end of November 2018 (see *infra*, VI.3).

VI.2.2.2. The appointment of a security adviser

Following a new question from both oversight bodies in 2018, the Ministers stated that they had not yet appointed a security and privacy adviser pending the adaptation of the legislative framework for the protection of privacy.[167, 168]

VI.2.2.3. Implementation of a mechanism for reporting security incidents

On the basis of its competence as database administrator, the Federal Police reported that a procedure was implemented in 2018 to enable any user to report a security incident. The Federal Police added that a procedure was being developed within the CDB Steering Committee to make it possible to follow up on and manage any security incidents that might be caused by a user.

---

166 The report was approved by both bodies on 20 December 2018.

167 All services had appointed an adviser internally by this time, however.

168 The Supervisory Body for Police Information and the Standing Committee I were unable to accept this justification, as they conduct checks on the basis of the applicable (and not the future) regulations. They therefore maintained their previous recommendation.

The Supervisory Body for Police Information and the Standing Committee I welcomed this initiative. However, they pointed out that IT security is a matter for professionals and that it is not enough only to deal with security incidents that have been caused/detected/reported by users, for whom IT security is not the core business.

In this context, the lack of a security adviser – who plays the leading role in ensuring the security of information systems – was a cause for concern.

VI.2.2.4. Development of an additional IT tool

Persons for whom there are only 'serious indications' that they belong to one of the five FTF categories of the database may be included in the database for a maximum of six months. If there is no additional information during this period that justifies registration within one of the five categories, the names of these persons must be deleted. The Supervisory Body for Police Information and the Standing Committee I therefore recommended a system of automatic notification. In response to this recommendation, a warning system was installed.

In addition, CUTA did not have an IT tool for monitoring the retention periods and the deletion of data about persons who appear (or appeared) in one of the five FTF categories. In 2017 CUTA had explained that such a technical tool was not (yet) a priority. Questioned about this in 2018, the Federal Police indicated that until CUTA decides to delete an entity, its data will remain available for use in the CDB. This means that if CUTA fails to act on its own initiative, a person can be kept indefinitely in the common database, which is contrary to the obligation to investigate at least every three years whether the registration of an entity is still appropriate. The recommendation to develop an IT tool was therefore maintained.

VI.2.2.5. Information cards and communications to third parties

The law states that the mayor is the recipient of the information cards on FTFs who have their place of residence or domicile in his or her municipality, regularly visit the municipality or regularly organise activities there. In 2017, CUTA had no insight at all into how this obligation was being met, which prompted the Supervisory Body for Police Information and the Standing Committee I to recommend the development of an IT tool that would enable compliance with this obligation to be monitored.

With regard to notifications to third-party services, the Supervisory Body for Police Information and the Standing Committee I pointed out back in 2017 that it follows from Article 44/11/3*quater* of the Policing Act and Article 11 §2 of the RD (F)TF that such notifications must be evaluated in advance by the Federal Police (in its capacity as database administrator), CUTA (in its capacity as

operational manager and service referred to in Article 44/11/3*ter* §1 of the Policing Act) and the intelligence services. The Supervisory Body for Police Information and the Standing Committee I stressed that this evaluation must include the information security aspect. This question was resubmitted to CUTA in 2018, which detailed the implementing measures it had taken at its level.

CUTA did not explicitly state that the evaluation referred to in Article 44/11/3*quater* of the Policing Act is carried out (systematically and) in advance with regard to the transfer of (extracts from) the information card to third-party bodies (i.e. bodies not referred to in Article 44/11/3*ter* of the Policing Act). In this context, it is important to note that since the previous check in 2017, Article 11 RD (F)TF has been amended by the Royal Decree of 23 April 2018 as regards the extraction and forwarding of lists.[169, 170] It follows from this amendment that the extraction of lists is explicitly permitted for services that have direct access, but only for internal handling by a personnel member with security clearance. Once this extraction is technically possible (which did not yet seem to be the case at the time of the investigation), the transmission of lists from CUTA to these services will cease to be of value.

The transfer of lists to other services or institutions (i.e. those without direct access) is in principle not allowed unless certain conditions are met. During the mid-2018 inspection, CUTA explained that it had taken measures at its level with regard to the transfer of lists. The Supervisory Body for Police Information and the Standing Committee I 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 of the conditions for its communication.[171]

VI.2.2.6. Performance of spontaneous checking of logged information

The Supervisory Body for Police Information and the Standing Committee I concluded in 2017 that '*even though the logged information is not immediately available for the user services, they must request it through their security and privacy adviser from the common database administrator (i.e. the Federal Police). This proactive approach will enable the service concerned to monitor the legitimacy of access to the common database*' (free translation). With the exception of one inspected service, the recommendation to spontaneously check logged information was not followed.

---

169 A list contains at least the anonymised data of several FTFs (statistics) and at most all personal data included in the information cards of these FTFs.

170 With regard to the purpose of the list in light of the recipient's statutory role, the use of the list solely for that purpose, the time-limited preservation of the list, security, etc.

171 For example, this could be set out in a protocol.

VI.2.3. USE OF THE FTF DATABASE BY PARTNER SERVICES AND LAW CENTRES[172]

VI.2.3.1. Insufficient access to the production environment

By mid-2018, a significant number of partner services and law centres did not yet have access to the production environment of the common database and were therefore not using it.[173] According to the Supervisory Body for Police Information and the Standing Committee I, this situation could be detrimental firstly to the completeness of the common database and secondly to the taking of appropriate action by the relevant services or authorities.

The Supervisory Body for Police Information and the Standing Committee I gave the following clarifications in this connection:

- The Governmental Coordination and Crisis Centre is a service that has (or must have) direct information retrieval rights to the database. If this has not yet been realised, measures must be taken to put this right (and obligation) into practice.
- In practice, not all penal institutions have direct access to the databases, but only a few services in the DGPI's central management, yet the regulations provide for an obligation for all penal institutions to supply information to the CDBs. If this practice is to be maintained, the statutory framework must be adapted accordingly.

VI.2.3.2. The security clearance situation

At the time of the inspection, the members of the services with access to the common database had the required security clearance. The Supervisory Body for Police Information and the Standing Committee I recommended in this context that the (fairly lengthy) procedures for applying for the security clearances be initiated promptly. Conversely, any loss of a personnel member's need-to-know status must be systematically reported in order to prevent unnecessary access rights from being maintained or security investigations that no longer serve any purpose from being continued.

VI.2.3.3. The appointment of a security adviser within each service

All services that had a direct access or direct information retrieval rights at the time of the inspection had appointed a security adviser.

---

172 Maisons de justice/Justitiehuizen.

173 Some services simply lacked access at the technical level (e.g. the *Administration générale des Maisons de Justice de la Communauté française*).

VI.2.3.4. Satisfaction of the partner services

Various parties emphasised the usefulness and collaborative character of the database. In practice, however, different services expressed the wish to be able to work with a system that allows individuals included in the common database to be automatically compared with their own database. As a result of the amendment of Article 11 RD (F)TF in 2018, services with direct access now have the option of extracting lists from the database, '*for internal use only*'. This provision was also amended to allow the basic services, after the required evaluation, to communicate lists '*to other services or institutions*' (free translations) (i.e. services or institutions that do not have direct access).

At the operational level, this demand for an IT application is logical and understandable: automatic comparisons save time and capacity. However, they require extensive testing, and it is also necessary to ensure that all decisions are made after human intervention and validation. In addition, measures must be taken to ensure that the use of these lists by third parties meets the required security conditions (confidentiality, integrity, etc.).

The Federal Police expected this functionality to be introduced by the beginning of 2019. The Supervisory Body for Police Information and the Standing Committee I will follow up on this point.

VI.2.3.5. Adaptation of the validation procedures following the changes to the regulatory framework

The validation procedures communicated by certain services prior to or on the occasion of the inspection by the Supervisory Body for Police Information and the Standing Committee I related only to FTFs and need to be updated for HTFs and HPs. Moreover, the *Vlaams Agentschap Jongerenwelzijn* (Youth Welfare Agency of the Flemish Community) must proceed with the implementation of the internal validation system referred to in Article 8 of the RD TF.

VI.2.4. THE PROVISION OF INFORMATION TO MAYORS AND THE TRANSFER OF (EXTRACTS FROM) INFORMATION CARDS OR OF LISTS TO THIRD-PARTY BODIES

In the absence of a reliable means of monitoring, the examination by the Supervisory Body for Police Information and the Standing Committee I of the transfer of the information card by local police chiefs to mayors was postponed. In this context, both authorities recommended that CUTA and the Federal Police raise awareness among the basic services (and in particular the police zones) of the need to systematically supply the computerised indicators (data on

the transmission of an (update of the) information card) in order to facilitate future monitoring.

During the investigation period, CUTA did not communicate any (extracts from) information cards to third-party government bodies or units (i.e. to bodies not covered by Article 44/11/3*ter* of the Policing Act in accordance with the preparatory work for that legislation).[174]

In July 2018, CUTA stated that it had sent monthly lists of the names of the people in the common database to '*a small number of services*' without specifying which services these were. The service explained that the '*the sending of the lists to these "partners" was approved by consensus among the four basic services*' (free translations).

The regulations on extracting and transferring lists were amended in 2018. The extraction of lists is now explicitly permitted for services that have direct access, but only for internal handling and when that handling is performed by a personnel member with security clearance. The transfer of the lists to other services or institutions is only permitted under certain conditions (*supra*). The Supervisory Body for Police Information and the Standing Committee I will verify compliance with these new regulations during a subsequent audit.

VI.3. TWO JOINT OPINIONS

Following the changes made by the two Royal Decrees of 23 April 2018 and in accordance with 44/11/3*bis* §3 of the Policing Act, the Ministers of Home Affairs and Justice submitted two 'prior reports' to the Supervisory Body for Police Information and the Standing Committee I for opinions.[175] The most important comments are summarised below:

– A start was made on processing personal data and processing information concerning HTFs and HPs respectively without first adjusting the legal framework (Art. 44/11/3*bis* §4, second paragraph Policing Act) and without a prior report being submitted (Art. 44/11/3*bis* §3 Policing Act). The Supervisory Body for Police Information and the Standing Committee I pointed out that compliance with these two provisions is one of the cornerstones of the monitoring of the common databases;
– Although the RD TF and RD HP had been published several months earlier, the report did not contain any concrete information about the direct access of the NSA;

174 Such a transfer would have required a prior joint assessment by the Federal Police, CUTA and the (other) basic services (Art. 44/11/3*quater* of the Policing Act). CUTA did not provide any clarification about possible transfers by other basic services in this context (it is not certain, however, that CUTA has this information).

175 These joint opinions 001/CPR-C.O.C./2018 and 002/CPR-C.O.C./2018 can be consulted at www.comiteri.be.

- The reports also failed to discuss the possibility of extracting lists of personal data and information from the database, despite the fact that this was an important change;
- The Supervisory Body for Police Information and the Standing Committee I again noted that no mention was made of the appointment of a security adviser;
- Both bodies regretted the fact that, with regard to the communication of the information cards to mayors, the report did not give any details of the frequency of application of Article 12 of the RD TF and RD HP.[176] Moreover, the report made no mention of the Act of 30 July 2018 establishing the local integrated security units on radicalism, extremism and terrorism (LIVC-R). This states that the local police chief and/or his or her representative are permitted to communicate to the members of the LIVC-R the information card of a person whose case is under discussion.

[176] For example, what is to be understood by the 'municipalities that are *regularly* visited' by a body, or another municipality in which an entity '*regularly*' organises one or more activities'?

CHAPTER VII
OPINIONS

Article 33, seventh paragraph, of the Review Act states that the Standing Committee I '*may only advise on a bill, Royal Decree, circular letter, or any other document expressing the lines of policy of the competent ministers at the request of the Chamber of Representatives or the competent minister.*' In 2018 an advisory opinion was requested from the Committee just once on the basis of this provision, by the Parliamentary Committee on Justice (*infra*).

In addition, the Committee is required to issue advice in its role as a Competent Supervisory Authority (CSA) in connection with the processing of personal data as well as in regard to the statutory arrangements concerning common databases – in this latter case in conjunction with the Supervisory Body for Police Information. These last two advisory competences are dealt with in Chapters V and VI.

VII.1. OPINION ON THE BILL ON THE PROCESSING OF PERSONAL DATA

On 14 December 2017 the Standing Committee I was asked by the Parliamentary Committee on Justice to issue an opinion on the bill on the protection of natural persons with regard to the processing of personal data. The bill, which was particularly complex and technical in nature and which related to a theme of major social importance, contained no fewer than 280 articles. As the text was the subject of political debate until just before its submission to Parliament, with certain options still under discussion and certain changes also being made, the Committee was unable to examine the entire bill in detail.

The Committee was therefore unable to formulate a considered opinion on all aspects of the legislation of relevance to it. The Committee pointed in particular to two features: first, the complexity and scope of the bill – raising the question of whether actual control over the processing of personal data was always the primary concern – and the sometimes illogical and incomprehensible way in which it was written, and second, the absolute need for extra personnel

for the Committee in order for it to perform the numerous and important tasks assigned to it in the bill.[177]

In its opinion[178], the Committee stressed that it welcomed the decision not to fully exclude data relating to national security from all protection mechanisms. However, the way in which this decision had been implemented (among other things through the creation of several different data protection authorities), led to a particularly complex system of monitoring in which uncertainties would inevitably arise for all parties involved: the administrative authorities, the various Data Protection Authorities and – not least – the citizens for whom the protection is intended.

177 The Act of 3 December 2017 which established the Data Protection Authority provided for an extensive structure with six different entities, but no additional budgetary, personnel or IT resources were allocated to the Committee. The Committee called for an immediate enlargement of its personnel. Without this, it argued, not only would the Committee's other roles, which had also become more onerous, be adversely affected, but it would hardly be possible to carry out the new duties as well. Such a situation seriously jeopardises the independent and democratic control of the intelligence sector.

178 The entire opinion is available in Dutch and French on www.comiteri.be.

CHAPTER VIII
CRIMINAL INVESTIGATIONS AND JUDICIAL INQUIRIES

As well as contributing to review investigations, the Committee's 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). With regard to the members of the other 'supporting services', 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).

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

In 2018, the Investigation Service I carried out investigative actions in the context of its judicial role, in three criminal investigations.

First, an investigation which had been started in 2017 was continued. It was being conducted at the request of the Federal 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. The investigation was not completed in 2018.

A second case concerned a follow-up to a complaint from a private person against a GISS personnel member. The person concerned submitted a complaint to the Standing Committee I in 2014. The Committee also carried out an investigation into this in the context of its general powers of review.[179]

Finally, the Investigation Service I assisted in an investigation by the Federal Police department in charge of specialised judicial assignments in a military setting, relating to suspected bullying within an intelligence service.

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 shall draw up an information report and send it to the Head of the Investigation Service I within a period of fifteen days*' (free translation). In 2018, the investigation service received one notification to this effect.

[179] STANDING COMMITTEE I, *Activity Report 2015*, 139–140 ('II.9. Complaint regarding the disclosure of personal information by an intelligence agent to a third party').

CHAPTER IX
EXPERTISE AND EXTERNAL CONTACTS

IX.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 2018:

- At the end of February 2018 at the invitation of the Geneva Centre for the Democratic Control of Armed Forces (DCAF) in Skopje (Macedonia), the registrar took part in the panel discussion on 'Why, When and How to Engage in Oversight Field Visits' in the context of the DCAF Assistance Programme for the Parliament of the Republic of Macedonia. Among other things, the draft of the 'Guidelines for intelligence oversight for parliamentary committees in the Assembly of the Republic of Macedonia' was presented on this occasion[180];
- The then chair of the Committee was a member of the panel of examiners for a doctoral defence at the Faculty of Economic, Social, Political Sciences and Communication of the University of Louvain (UCL) in February 2018[181];
- The Committee contributed to an exploration of parliamentary oversight of intelligence and security services abroad at the request of the Dutch Chamber of Representatives;
- On 25 May 2018 the Standing Committee I and the Standing Committee P organised a session in Parliament on the occasion of their 25th anniversary. As well as a number of politicians and international guest speakers, representatives from the monitored services were also invited to express their views.
- From 24 to 31 May 2018 the United Nations Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism, Ms Fionnuala Ní Aoláin, paid an official visit to Belgium. The Standing Committee I was among the bodies she visited and had the opportunity to explain its vision.[182]

---

180 DCAF, *Guidelines for intelligence oversight for parliamentary committees in the Assembly of the Republic of Macedonia*, May 2018, (www.dcaf.ch).

181 A. LELIEVRE, *La communication web des services de renseignement. Étude sémio-pragmatique. Thèse présentée dans le cadre du Doctorat en Information et Communication*, UCL, February 2018.

182 In this regard, see: Human Rights Council, Report of the Special Rapporteur on the protection and promotion of human rights and fundamental freedoms while countering terrorism – Visit to Belgium, A/HRC/40/52/Add. 5, 27 February 2019, 33 p.

- An honorary chair of the Standing Committee I has chaired the Belgian Intelligence Studies Centre (BISC) since 2011. The aim of this centre is to bring the intelligence and security services and the academic world closer together and to contribute to thinking on intelligence issues. In June 2018, the BISC organised a study day on 'International collaboration on intelligence services and intelligence studies'.[183]
- The director of the Investigation Service I wrote a piece in the 'Cahiers Intelligence Studies' reflecting on the functioning of the Standing Committee I since 2013[184];
- In early April 2018 the Chair of the Committee moderated the panel discussion 'L'Europe et le renseignement' at the seminar on 'Le renseignement et son contrôle' organised by the French 'Conseil d'État' and the 'Commission nationale de contrôle des techniques de renseignement' (CNCTR);
- The Committee's registrar participated in the European Intelligence Oversight Network (EION), where experts from various supervisory authorities, NGOs (e.g. 'Stiftung Neue Verantwortung') and from the academic world reflected on oversight innovation and the exchange of information between national oversight bodies;
- In September 2018 a three-day seminar took place in Paris entitled 'SIGINT intelligence transnational activities and national security in France and Europe – a changing landscape'. An honorary chair gave a keynote address on SIGINT Intelligence, Surveillance, Ethics and Control. The opportunity was taken to explain the role of the Standing Committee I as an oversight body and emphasise the growing importance of SIGINT in an intelligence context;
- 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);
- The Standing Committee I was the discussion partner of the 'Stiftung Neue Verantwortung' in an exchange of views on new challenges and changes to democratic control of intelligence in Belgium and Germany;
- The Committee's legal expertise was called upon in a practical seminar for police, the judiciary and legal professionals on the subject of classification and security clearances;
- The head of the legal service published a scientific contribution in 2018 on 25 years of Belgian oversight of the intelligence and security services[185];

---

183 The BISC devoted the 9th volume of its 'Cahiers Intelligence Studies' series to the honorary chair of the Committee (M. COOLS et al, eds., *Methodologie inlichtingenstudies – Méthodologie des études de renseignement. Liber Amicorum Guy Rapaille*, Gompel&Svacina, Oud-Turnhout, 2018, 280 p.).

184 F. FRANCEUS, 'Et demain? Het Vast Comité I sinds 2013', in M. COOLS et al, *op. cit*., 2018, 19–26.

185 W. VAN LAETHEM, 'The Rule of Law and 25 Years of Intelligence Oversight in an Ever-changing World: the Belgian Case' in I. LEIGH and N. WEGGE (eds.), *Intelligence Oversight in the Twenty-First Century. Accountability in a Changing World*, London, Routledge, 2018, 208 p.

– The chair and honorary chairs and counsellors of the Standing Committee I spoke at the two-day 'Conférence européenne des autorités de contrôle du renseignement' (Paris, 6 and 7 December 2018).

IX.2. COOPERATION PROTOCOL BETWEEN HUMAN RIGHTS INSTITUTES

The creation of a National Human Rights Institute, which was committed to when the Protocol to the UN Convention against Torture was signed, had not yet taken place in Belgium in 2018.[186] The actual establishment of such an institute is only possible after the ratification of the protocol, to which – in addition to the Federal Parliament – all the Belgian Communities and Regions must also consent. In implementation of this, the instrument of consent of the Flemish, French-speaking and German-speaking Communities and of the Walloon Region appeared in the Belgian Official Journal, and that of the United Assembly of the Common Community Commission was also published.

Pending the actual creation of the institute, meetings with various institutions with a human rights mandate[187] resulted in a cooperation protocol in January 2015[188], in which the participating bodies agreed to exchange practices and methods, to investigate common issues and to promote mutual cooperation.

In 2018 the activities of this platform took the form of consultative meetings at which both general issues (e.g. Belgium and the promotion and protection of human rights, the establishment of the Central Supervisory Board for the Prison System, presentations of the various participating institutions etc.) and the exchange of working methods and methodologies on specific individual cases were discussed. In 2018 Myria – formerly the Centre for Equal Opportunities and Combating Racism – took over the chair from the National Commission on the Rights of the Child.

IX.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

186 The Act of 12 May 2019 establishing a Federal Institute for the Protection and Promotion of Human Rights (*Belgian Official Journal* 21 June 2019) also settled the matter at federal level.

187 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.

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

Netherlands, Norway and Switzerland)[189] are therefore working together to meet these challenges by finding ways to reduce the risk of a supervisory gap.

Since 2015 these oversight bodies have simultaneously – but each within the framework of its own mandate and powers – conducted an investigation into the international exchange of personal data in the context of the fight against FTFs (see I.6.1.). 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.

At the beginning of November 2018 a joint statement and press release were prepared by the participating oversight bodies.[190] The joint statement listed a number of ways to make progress in this area, given that, in order to prevent the risk of 'blind spots' in oversight, there is a need for intensified cooperation between the oversight bodies. One valuable and necessary step towards closer cooperation in oversight is to reduce the level of secrecy between the oversight bodies. As the intelligence services exchange data frequently, the oversight bodies need to be able to do likewise: they must be able to discuss the intelligence that is exchanged. Another step in the right direction is the development of new legal and technical monitoring methods for the factual assessment of international data exchange and the existence and functioning of common safeguards for the protection of fundamental rights.

IX.4. CONTACTS WITH FOREIGN REVIEW BODIES

The Standing Committee I also maintained close contacts with various foreign oversight bodies in 2018.

During a seminar that took place in early April 2018 at the French 'Conseil d'État', jointly organised by the 'Commission nationale de contrôle des techniques de renseignement' (CNCTR), which was attended by a contingent from the Standing Committee I, relations were developed further. Ties were reinforced with the 'Délégation parlementaire au renseignement' (DPR), and there was also an exchange of views with, among others, the Dutch 'Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten' (CTIVD), the British Investigatory Powers Commissioner's Office (IPCO), the German 'Parlamentarisches Kontrollgremium' (PKGr).

In June 2018 a working visit was organised in Berlin between a contingent from the Standing Committee I and the German 'Parlamentarisches Kontrollgremium', during which the Belgian contingent explained its activity

189 See STANDING COMMITTEE I, *Activiteitenverslag 2015* (Activity report 2015), 80–81.

190 See Appendix 'Strengthening the oversight of international data exchange between intelligence and security services'.

reports and the investigations that took place after the terrorist attacks in Paris and Brussels.

In the same month a briefing was jointly organised with the Speaker of the Chamber of Representatives in Brussels for the Georgian Office of the Personal Data Protection Inspector and representatives of the Georgian Parliament. State Security and the Coordination Unit for Threat Assessment were also involved in this initiative. The aim was to improve understanding of independent oversight of the intelligence services, with a particular focus on the methodology, means and techniques used to meet the requirements of efficient and effective democratic control.

In October 2018, at the request of the Norwegian Ministry of Justice, a meeting was held at the Norwegian Embassy in Brussels with representatives of the Norwegian Ministry of Justice and embassy staff on the subject of strategic planning in the context of cooperation between intelligence services.

In early November 2018 a meeting was held at the French embassy in Brussels with a parliamentary delegation composed of members of the 'Délégation parlementaire au Renseignement', the 'Commission de vérification des fonds spéciaux' and the National Assembly. The exchange of views took place in the context of the preparation of a joint initiative by the Speakers of the National Assembly and of the Belgian Senate on '10 years of parliamentary monitoring of intelligence: is the democratic requirement being fulfilled?'.

Also in November 2018 the International Intelligence Oversight Forum was organised in Valletta (Malta) by the United Nations Special Rapporteur for Privacy (SRP) on the subject of 'Latest Challenges to Intelligence Oversight in a Democracy'. 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.

On 21 and 22 November 2018 the Committee was invited by the Swiss oversight body 'Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten' ('Autorité de surveillance indépendante des activités de renseignement') on a visit to Bern with a view to strengthening links between the two oversight bodies.

The Standing Committee I, together with the 'Commission nationale de contrôle des techniques de renseignement', organised the two-day 'Conférence européenne des autorités de contrôle du renseignement' (Paris, 6 and 7 December 2018). The conference took place behind closed doors, and participants from 15 different European countries were represented (*supra*).

Finally, 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.

IX.5. MEDIA PRESENCE

The Standing Committee I is regularly asked by the media to explain its work or that of the intelligence services. The Standing Committee I responded to a number of such requests.

Date	Subject/title	Forum
16 January 2018	Inteligencia estratégica, hoy	Defensa.com
27 January 2018	Eindelijk controle op kas Staatsveiligheid	De Tijd
27 January 2018	Militair geheime dienst ontsnapt aan Rekenhof	De Tijd
30 January 2018	Eddy Testelmans, l'ancien chef des renseignements de l'armée, sous le feu des critiques	La Libre Belgique
13 February 2018	"Bruxelles est un nid d'espions": la capitale belge est un carrefour mondial de l'espionnage, confirme le patron du Comité R	Sud Presse
01 March 2018	Belgische terroristen-databank rammelt nog	De Tijd
06 March 2018	Ex-leden willen dat Comité I rol van Staatsveiligheid onderzoekt	Knack
06 March 2018	Des anciens du Comité R réclament une enquête sur la Sûreté de l'État	Le Vif
13 March 2018	Serge Lipszyc, seul candidat à la présidence du Comité R	Le Vif
23 March 2018	Omstreden benoeming voor adviseur premier	De Standaard
23 March 2018	Candidate to head security committee draws fire from the opposition	The Brussels Times
28 March 2018	Adviseur premier Michel aan het hoofd van Comité I	De Standaard
13 April 2018	België opent geheime archieven om mysterieuze dood VN-baas op te helderen	De Morgen
18 April 2018	Comment la Belgique a rendu la liberté au commanditaire présumé des attentats de Paris et de Bruxelles	Paris Match
19 April 2018	La Chambre désigne un collaborateur de Charles Michel à la tête du Comité R	Sudinfo.be
19 April 2018	Kamer keurt omstreden benoeming van adviseur premier goed	De Standaard
24 May 2018	Guy Rapaille, président du Comité R: "Il a fallu attendre les attentats pour obtenir plus de moyens"	Rtbf.be
24 May 2018	Contrôler la police et les renseignements: Guy Rapaille invité de Jeudi en Prime	Rtbf.be

Date	Subject/title	Forum
25 May 2018	Belgische militairen zetten in 2016 voet aan de grond in Syrië	Vrt.be
05 June 2018	Ça roule entre le FBI et la Belgique	Le Soir
06 June 2018	Wat vertellen Belgische archieven over dood Dag Hammarskjöld in 1961?	Mo.be
06 June 2018	Rekenkamer: "Privacycommissie, Comité P en andere aan Kamer verbonden instellingen moeten gesaneerd worden"	Het Laatste Nieuws
12 June 2018	Guy Rapaille (Comité I): 'Russische inmenging bij onze verkiezingen? Dat valt te vrezen, ja'	Knack
13 June 2018	"Gare à l'action des services turcs et marocains"	Le Soir
13 June 2018	Bélgica investiga si sus servicios de inteligencia conocían el supuesto espionaje del CNI a Puigdemont	Público
13 June 2018	Belgique: interrogations sur un possible espionnage de Puigdemont par l'Espagne sans préavis	Le Point
13 June 2018	België laat schaduwoperatie tegen Puigdemont onderzoeken	De Tijd
13 June 2018	Guy Rapaille: "Une ingérence russe lors des élections est à craindre"	Le Vif
13 June 2018	Le renseignement belge s'inquiète d'une possible ingérence de la Russie lors des élections	Sudinfo.be
13 June 2018	Steven Vandeput confirme un risque d'actions de désinformation russes en Belgique: "on se prépare"	Rtbf.be
14 June 2018	Militaire veiligheidsdienst draait vierkant	De Standaard
14 June 2018	Dysfonctionnements au sein du service de renseignement militaire	Rtbf.be
15 June 2018	Comité I-voorzitter Guy Rapaille spreekt	Apache
16 June 2018	Guy Rapaille, président du Comité R: "La Belgique doit craindre l'ingérence russe"	Le Soir – Le Vif
24 June 2018	Élections en Turquie: la propagande passe aussi par les mosquées	La Libre Belgique
25 July 2018	À Bruxelles, une incroyable histoire de faux papiers et d'espions russes	Le Monde
30 August 2018	Les services de renseignement doivent pouvoir déplaire au politique. Entretien avec Guy Rapaille	Le Vif
11 September 2018	Guy Rapaille " Les services de renseignement doivent pouvoir déplaire aux politiques"	Rtbf.be
11 September 2018	Au bout du jour: interview de Monsieur Rapaille	Rtbf.be

Date	Subject/title	Forum
12 November 2018	Filip Dewinter, espion…pour la Chine?	La Libre Belgique
12 November 2018	Filip Dewinter vraagt onderzoek van Comité I	De Standaard
02 December 2018	Guy Rapaille: "La transparence des services de renseignements a été parfaite"	Le Soir
21 December 2018	Elk bedrijf moet info geven aan Staatsveiligheid	De Tijd
21 December 2018	Les entreprises doivent fournir des informations sur demande de la Sûreté de l'État	Rtbf.be

CHAPTER X

THE APPEAL BODY FOR SECURITY CLEARANCES, CERTIFICATES AND ADVICE

The Appeal Body is an 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 event.[191]

The Appeal Body is composed of the chairs of the Standing Committee I, of the Standing Committee P and, since mid-2018 (see X.2.2.), of the Dispute Chamber of the Data Protection Authority. The chair of the Standing Committee I chairs the Appeal Body. The registry function is performed by the registrar and administration of the Standing Committee I.

The Appeal Body's activities have a direct impact on both the budgetary and human resources of the Standing Committee I, as all operating costs are borne by the Standing Committee I, which in addition supplies not only the chair and the registrar, but also the necessary administrative personnel for the preparation, handling and processing of appeals. These activities are very time-consuming.

X.1. A SOMETIMES CUMBERSOME AND COMPLEX PROCEDURE

Although a decrease in the number of cases was recorded in 2018 (down from 192 to 158), this did not mean a reduction of the workload, as the cases are becoming increasingly complex in terms of administrative management, hearings and decisions. This results in an increasing workload.

---

191 In this regard, see STANDING COMMITTEE I, *Activiteitenverslag 2006* (Activity Report 2006), 91–119. However, the rules explained there do not take account of the changes regarding security advice introduced by the acts of 23 February 2018 and 13 September 2018, which are summarised below (see X.2.1.2 and X.2.2).

For example, 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 shall be sent to the Appeal Body by registered letter*' and that '*the deed of appeal shall be signed and dated by the applicant or by a lawyer*' (free translations). The registrar was therefore compelled to point this out to the applicants with a view to regularising the situation within the statutory deadline.[192]

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. Delays of this kind can obviously be harmful to the applicant'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 in turn makes it difficult for the Appeal Body to adhere to the period within which it must make a decision.
- The administrative files sent by the various security authorities are not always complete, so that, again, 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 certain documents from the file that is made available for the inspection of the applicant or his or her 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 applicant and his or her 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 requirements of the law – a duly justified decision is not drawn up where Article 22, fifth paragraph of the Classification and Security Clearances Act allows certain information to be omitted from the decision

[192] Because of the very short deadlines, the appeal in these cases is often late and therefore inadmissible.

notified to the person concerned. The security authority must make clear in its justification which specific facts constitute a contra-indication to disclosure in light of the regulatory purpose of a given 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 also shown a lack of care and respect for the principles of administrative law at the formal level (decisions without the details and identity of the official taking the decision; the person concerned has never been heard; use of language in administrative matters).
- The security authorities appear to have difficulty in accepting certain decisions arising from the established case law of the Appeal Body (for example, on the issue of investigations into or verifications of persons who do not hold Belgian citizenship).

It should also be noted that the sessions take much more time than they used to a few years ago. There are various reasons for this. More and more applicants are being assisted by one or two lawyers. Given the complexity of certain cases, a lot of time is spent on them. Finally – unlike in the past – many cases have to be resumed at a second or third session, whether because an applicant requests an extension, because additional information is being awaited, or due to a change in the location of the Appeal Body.

The decision-making process itself also takes more time than a few years ago. There are two reasons for this. First, more procedural issues are being raised (e.g. admissibility, language issues, rights of defence, the obligation to state the grounds for a decision, etc.). Second, the Appeal Body is encountering more cases of an extremely sensitive nature relating to espionage, radicalisation and the threat of terrorism. Such cases naturally require extremely careful handling and appropriate justification. In addition, they sometimes require specific security measures.

X.2. CHANGES IN THE STATUTORY FRAMEWORK

Various factors suggest that the workload of the Appeal Body will undergo a further (significant) increase in the future. Following the Paris and Brussels attacks, the government announced an increase in the number of security screenings, particularly with a view to increasing the security of critical infrastructure.

This intention resulted at the end of 2017 in the submission of a bill[193] with a view to amending the Classification and Security Clearances Act. The Standing

193 *Parl. Doc.* Chamber of Representatives 2017–2018, no. 54K2767/001.

Committee I issued an opinion on this.[194] The bill was approved in early 2018[195] and also entailed a minor amendment of the Appeal Body Act. Four Royal Decrees were issued to implement the law. A number of the changes affected the composition of the Appeal Body. The new framework law on data protection also contained rules that apply in particular to the Appeal Body. These adjustments to the statutory framework are explained below.

X.2.1. CHANGES TO THE REGULATIONS ON CLASSIFICATION AND ON SECURITY CLEARANCES, CERTIFICATION AND ADVICE

X.2.1.1. The competence and role of the security officer

The amendment of the Classification and Security Clearances Act extends the duties of the security officer in connection with security verifications (certificates and advice) and also anchors this function within the Public Prosecutor's Office.

The security officer is assigned competence for '*ensuring compliance with the security rules in the context of security advice or a security certificate*' (free translation) at the relevant entities incorporated under private or public law.

X.2.1.2. The reform of the security advice procedure[196]

The security advice procedure has been reformed both at the level of regulatory decision-making by the administrative authority and at the level of individual decision-making. These new regulations came into effect on 1 June 2018.

With regard to regulatory decisions, the new procedure stipulates that it is up to the King to determine which 'activity sectors' are subject to the application of security advice and to designate the competent (sectoral) administrative authorities.[197] Both private- and public-law entities that belong to a relevant

194 This opinion can be consulted on the website of the Standing Committee I (www.comiteri.be). The Committee stressed that the bill did not provide an answer to the many problems that the application of the rules in force at the time entailed (complexity, excessively short appeal deadlines, etc.), in terms both of the administrations and citizens involved and of the Appeal Body. The Committee had previously formulated a number of proposals to address these problems. The bill not only failed to pick up on these, but inevitably created additional problems for all actors. The Committee therefore took the view that both laws of 11 December 1998 (the Classification and Security Clearances Act and the Appeal Body Act) needed to be reformed in a coherent manner.

195 Act of 23 February 2018 amending the Act of 11 December 1998 on classification and security clearances, certificates and advice (*Belgian Official Journal* 1 June 2018).

196 See Articles 22*quinquies* and 22*quinquies*/1 of the Classification and Security Clearances Act and the Royal Decree of 8 May 2018 amending the Royal Decree of 24 March 2000 implementing the Act of 11 December 1998 on classification and security clearances, certificates and advice (*Belgian Official Journal* 1 June 2018).

197 This represents an important difference from the initial regulation on security advice, which stated that 'an' (i.e. any) administrative authority could initiate the procedure. This provision was implemented by the Royal Decree of 8 May 2018 determining the activity sectors and the

activity sector will then perform a 'risk analysis' at the request of the competent administrative authority or on their own initiative and send it to the latter. The administrative authority then requests a specific 'threat analysis' from 'the competent services'. Once it is in possession of this analysis, the competent administrative authority in turn draws up an 'impact analysis'. The purpose of this is to assess the potential damage to fundamental state interests. On the basis of these analyses, the administrative authority sends an application file relating to security verification to the National Security Authority (NSA). Finally, the NSA decides whether or not security verifications may be carried out.

For individual decisions, the new rules state that legal entities must inform the person concerned of the obligation to undergo a security verification. The security officer of the legal entity must request the consent of the person concerned prior to the security verification. The security officer of the competent administrative authority will monitor the conformity of verification requests among other things. He or she will then in turn communicate the request to the NSA. The NSA will make a decision on the individual application within the set deadline (maximum one month). If the NSA fails to formulate its security advice within this period, it may be pressed to make a decision within a period at least as long as the initially prescribed period. If this does not happen, the advice is deemed to be positive. The new rules stipulate that the advice is granted for a maximum of five years[198], and is subject to reappraisal by the NSA (based on new information). The administrative authority informs the employer's security officer of the security advice that has been issued. If negative security advice is issued, the person concerned will be informed of this by registered mail, omitting any grounds for the negative advice whose disclosure might damage one of the fundamental interests listed in the law, the protection of sources, the secrecy of a criminal investigation or judicial inquiry or the protection of the privacy of third parties.[199]

X.2.1.3. Content of the security verification

The last important pillar of the change in the law concerns the modification of the content of the security verification (Art. 22*sexies* Classification and Security Clearances Act). There are three objectives here.

---

competent administrative authorities referred to in Art. 22*quinquies* §7 of the Act of 11 December 1998 on classification and on security clearances, certificates and security advice (*Belgian Official Journal* 1 June 2018).

198 This too is a difference from the previous rules, which did not include a 'maximum' validity period. Furthermore, under the previous rules, the security verification had to be carried out 'prior' to the authorisation to exercise or perform a profession, role, assignment or mandate. The change introduces the possibility of subjecting persons who are already in a particular job to a security verification.

199 See Art. 22, paragraph 5 Classification and Security Clearances Act (unamended).

First of all, the intention is to make security verifications possible with regard to minors. The aim is also to take account of offences committed by the subject as a minor in the context of adult safety checks.

In addition, the new law allows the police and intelligence services to request data from their foreign counterparts when the person for whom the security verification is required lives (or has lived) abroad, has passed through a foreign country or has spent time abroad.

Finally, the new law increases the number of databases to be searched. Article 22*sexies* of the Classification and Security Clearances Act already provided for the consultation and evaluation of judicial data[200], information from the intelligence services, the central criminal record, the criminal record and the population and alien registers kept at the municipalities, the National Register, the waiting list for aliens and the police data available to police officers when running identity checks. The amended text adds the following data: data and information from the international police databases resulting from treaties to which Belgium is signatory, data from the administrative police, data from common databases and '*other data and information*'(free translation). The law states that the nature of this data (which must be sufficient, relevant and non-excessive) and the list of databases must be determined by Royal Decree. The decree in question also appeared in the course of 2018.[201]

X.2.1.4. Fees

In mid-2018, a Royal Decree was also approved determining the fees due for issuing clearances, certificates and advice.[202] The fee for a clearance for natural persons is 150, 175 or 200 euros, depending on the level requested (confidential, secret or top secret respectively). Depending on the level, the fee for legal entities is 900, 1200 or 1500 euros. The standard charge for a security certificate or advice is set at 50 euros. These amounts are then distributed among the various authorities involved on the basis of a formula determined in the Royal Decree.

200 Sent with the permission of the competent judicial authorities.

201 Royal Decree of 8 May 2018 determining the list of data and information that may be consulted in the context of the implementation of a security verification (*Belgian Official Journal* 1 June 2018).

202 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. 22*septies*, sixth and eighth paragraphs, of the 1998 Act on classification and on security clearances, certificates and advice (*Belgian Official Journal* 1 June 2018).

X.2.2. CHANGES TO THE OPERATION OF THE APPEAL BODY[203]

In 2018, three laws changed the composition of the Appeal Body and the appeal procedure.

First the Appeal Body Act was amended to bring it in line with the changes introduced by the Classification and Security Clearances Act, with a view to maintaining the right to appeal for those who have received negative security advice. Those in this situation must lodge an appeal within eight days of receiving the advice. Article 12 of the Appeal Body Act was also adapted to make an appeal against a (positive or negative) regulatory decision[204] possible for anyone with a legitimate interest. But the administrative authority concerned has also been given the option of lodging an appeal with the Appeal Body if the NSA has turned down its request for verification. Such appeals must be lodged within eight days after the administrative authority has been informed of the NSA's decision.

In addition, the composition of the Appeal Body was amended by the Act of 13 September 2018 in order to take account of the abolition of the Commission for the Protection of Privacy. The Appeal Body Act stipulates that the chair of the Dispute Chamber of the Data Protection Authority (DPA) sits on the Appeal Body. In order to ensure continuity, the Act of 13 September 2018 included a transitional measure to allow the chair of the DPA to continue to perform his or her role within the Appeal Body until the appointment of the chair of the DPA's Dispute Chamber. This appointment came at the end of the first quarter of 2019.[205]

Finally, taking account of the fact that the Act of 3 December 2017[206] does not stipulate that the chairman of the DPA's Dispute Chamber (or anyone else in

---

203 Act of 13 September 2018 amending the Act of 11 December 1998 on classification and on security clearances, certificates and advice (*Belgian Official Journal* 5 October 2018).

204 The preparatory documents state that '*[t]his appeal may therefore not only be lodged by a natural person who performs such a function or who has access to the place concerned, but also by a legal entity under private law that belongs to the sector. […] This appeal therefore relates to the approval or refusal of the administrative authority's request on the grounds of Article 12 of the law on security clearances. In the context of this appeal, an investigation will be conducted into the relevance of the security aspects of the request. The elements of the administrative authority's request relating to security aspects will also undergo de facto examination when considering the appeal. The experience and expertise of the members of the appeal body in terms of security and protection of liberties and fundamental rights justify that body acting as an appeal body. Obviously, the sector or anyone demonstrating an interest may also appeal against the request submitted by the administrative authority (impact analysis). This specific appeal may be lodged with the Council of State, since it does not fall under the competence of the appeal body*' (free translation) (*Parl. Doc.*, Chamber of Representatives, 2017–18, 54K3107/005, 4).

205 Hielke Hijmans was appointed chair of the Data Protection Authority Dispute Chamber (*Proceedings* Chamber of Representatives 2018–19, 28 March 2019, CRIV54PLEN278) and was sworn in on 24 April 2019.

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

the Dispute Chamber) must be a magistrate, the requirement to have this qualification in order to be a member of the Appeal Body has been scrapped.[207]

X.2.3. THE NEW FRAMEWORK LAW ON THE PROTECTION OF PERSONAL DATA

Title 3 of the Act of 30 July 2018[208] (DP Act) contains a subtitle 3 specifically devoted to the protection of natural persons with regard to the processing of personal data in the context of the Classification and Security Clearances Act (Articles 106 to 137 DP Act). The rules included in this subtitle also apply to any processing of this type of data by the Appeal Body (Article 107, §2 DP Act). It should be noted, however, that the Appeal Body, in its capacity as a judicial authority, is not subject to review by a supervisory authority for the protection of personal data (Article 128, §2 DP Act).

X.3. DETAILED STATISTICS

This section gives a statistical picture of the nature of the contested decisions, the capacity of the competent authorities and of the applicants[209] 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 five years have also been included.

Three trends can be identified in 2018. First, after two years of significant increase, there was a fall in the number of appeals, from 192 in 2017 to 158 in 2018. In addition, the number of cases relating to military personnel also decreased, from 20 in 2017 to 8 in 2018. A final trend consists on the one hand of an increase in the number of appeals against refusals of security certificates in the nuclear sector (7 in 2016 and 2017 and 11 in 2018) and on the other hand of a clear drop in the number of appeals against negative security advice (101 in 2016, 122 in 2017 and 92 in 2018).[210]

---

207 The preparatory documents state the following: '*This therefore means that the conditions laid down in the laws establishing the bodies concerned have to be taken into account. The appeal body will still consist of at least two magistrates. The presence of two magistrates (from the Committee P and Committee I respectively) on that body is guaranteed by the law establishing the bodies concerned*' (*Parl. Doc.*, Chamber of Representatives, 2017–18, 54K3107/003, 9) (free translation).

208 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).

209 Ten 'requests' failed to meet the minimum requirements of the law (the typical example being the absence of a signature) and could therefore not be regarded as admissible appeals.

210 The fall in the number of appeals against negative security advice can be explained by the case law of the Appeal Body pronounced in the course of 2017, which found that, on the basis of the applications for security verification presented (at that time), the security advice formulated by the NSA for external personnel of European institutions lacked an adequate legal basis. The analysis of the adjustment of the statutory framework

There were 14 sessions of the Appeal Body in 2018.

Table 1. Security authority concerned

	2014	2015	2016	2017	2018
National Security Authority	99	68	92	129	113
State Security	0	1	0	0	0
General Intelligence and Security Service	60	47	68	53	32
Federal Agency for Nuclear Control	8	10	8	7	10
Federal Police	3	3	1	3	3
Local Police	1	1	0	0	0
TOTAL	**171**	**130**	**169**	**192**	**158**

Table 2. Nature of the disputed decision

	2014	2015	2016	2017	2018
Security clearances (Art. 12 ff. Classification and Security Clearances Act)					
Confidential	5	9	5	1	2
Secret	43	35	38	33	31
Top secret	4	4	7	6	3
Refusal	25	36	28	30	26
Withdrawal	9	7	9	7	4
Refusal and withdrawal	0	0	0	0	0
Clearance for a limited duration	2	3	4	1	1
Clearance for a lower level	1	0	1	0	0
No decision within time limit	15	2	7	2	5
No decision within extended time limit	0	0	1	0	0
Security clearances subtotal	**52**	**48**	**50**	**40**	**36**

(summarised above) suggests that the subject matter covered by security advice on the personnel of European institutions will soon be submitted (again) to the Appeal Body, given that the Royal Decree of 8 May 2018 (see above) designates the managing officer of the FPS Foreign Affairs or his or her delegate as the administrative authority competent for the international authorities.

	2014	2015	2016	2017	2018
Security certificates for access to classified zones (Art. 22*bis*, para.1 Classification and Security Clearances Act)					
Refusal	4	6	1	3	3
Withdrawal	0	0	0	0	0
No decision within 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	16	12	9	20	15
Withdrawal	0	1	0	0	0
No decision within time limit	0	0	0	0	0
Security certificates for the nuclear sector (Art. 8*bis*, §2 Classification and Security Clearances Act)					
Refusal	–	–	7	7	11
Withdrawal	–	–	1	0	0
No decision within time limit	–	–	0	0	1
Security advice (Art. 22*quinquies* Classification and Security Clearances Act)					
Negative advice	99	63	101	122	92
No advice	0	0	0	0	0
Retraction of positive advice	0	0	0	0	0
Normative legal acts (Art. 12 Appeal Body Act)					
Decision by public authority to request certificates	0	0	0	0	0
Refusal by NSA to carry out verifications for certificates	0	0	0	0	0
Decision by administrative authority to request advice	0	0	0	0	0
Refusal by NSA to carry out verifications for advice	0	0	0	0	0
Certificates and advice subtotal	119	82	119	152	122
TOTAL DISPUTED DECISIONS	**171**	**130**	**169**	**192**	**158**

Table 3. Capacity of requesting party

	2014	2015	2016	2017	2018
Official	0	4	2	4	5
Military personnel	17	29	23	20	8
Private individual	145	93	139	164	140
Legal entity	6	4	5	4	5

Table 4. Requesting party's language

	2014	2015	2016	2017	2018
French	92	75	99	115	83
Dutch	76	54	70	77	75
German	0	0	0	0	0
Other	0	1	0	0	0

Table 5. Nature of the preparatory decisions taken by the Appeal Body[211]

	2014	2015	2016	2017	2018
Complete file requested (1)	168	130	167	191	154
Supplementary information requested (2)	16	7	23	36	12
Representative of authority heard (3)	11	7	10	0	1
Decision by chair (4)	0	0	0	0	0
Information removed from file by Appeal Body (5)	78	50	54	80[212]	72
Information removed from file by intelligence service (6)	0	0	0	0	0

(1) The Appeal Body has the option to request the entire investigation file from the security authorities. As this file contains more information than the investigation report alone, this request is made 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.

211 The 'nature of the preparatory decisions taken' (Table 5), the 'use made by the applicant of his or her rights of defence' (Table 6) or, the 'nature of the decisions of the Appeal Body' (Table 7) are not necessarily the same as the number of requests submitted as shown in Tables 1 to 4. This is because some applications were started in 2017, for example, but the decision was not made until 2018.

212 See above regarding Art. 5 §3 of the Appeal Body Act. It should be noted that in many cases the request to deny inspection was only partially granted (sometimes due to a failure on the part of the service concerned to justify its request).

(3) 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 verification.
(4) 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.
(5) If the intelligence or police department concerned so requests, the chair of the Appeal Body may decide that certain information will be removed from the file that will be submitted to the applicant for inspection.[213]
(6) If the information concerned originates from a foreign intelligence service, the Belgian intelligence service itself will decide whether the information will be made available for inspection. This is an aspect of the application of the so-called 'third-party rule'.

Table 6. Use made by the applicant of his or her rights of defence

	2014	2015	2016	2017	2018
Inspection of file by complainant/ lawyer	84	84	87	105	69
Hearing of the complainant/ lawyer[214]	115	107	127	158	111

Table 7. Nature of the Appeal Body's decisions

	2014	2015	2016	2017	2018
Security clearance (Art. 12 ff. Classification and Security Clearances Act)					
Appeal inadmissible	0	4	0	3	0
Appeal devoid of purpose	3	3	7	0	4
Appeal unfounded	12	19	18	13	12
Appeal well-founded (full or partial adjudication)	14	24	24	24	12
Additional investigative actions by authority	0	0	2	0	1
Additional time for authority	12	1	2	1	1
Case dropped	0	1	0	0	3
Security certificates for access to classified zones (Art. 22*bis*, para. 1 Classification and Security Clearances Act).					
Appeal inadmissible	0	0	0	1	0

213 See above regarding Art. 5 §3 of the Appeal Body Act.
214 In certain cases, the complainant (whether or not assisted by a lawyer) is heard more than once.

	2014	2015	2016	2017	2018
Appeal devoid of purpose	0	0	0	1	0
Appeal unfounded	2	4	1	0	1
Appeal well-founded (adjudication)	0	2	1	1	0
Security certificates for a place or event (Art. 22*bis*, para. 2 Classification and Security Clearances Act).					
Appeal inadmissible	0	0	0	1	2
Appeal devoid of purpose	0	0	0	1	0
Appeal unfounded	6	8	2	12	2
Appeal well-founded (adjudication)	8	10	4	7	3
Waiver of appeal granted	0	2	0	1	2
Security certificates for the nuclear sector (Art. 8*bis* §2 Classification and Security Clearances Act)					
Appeal inadmissible	-	-	1	1	0
Appeal devoid of purpose	-	-	1	0	1
Appeal unfounded	-	-	0	1	1
Appeal well-founded (adjudication)	-	-	7	5	6
Waiver of appeal granted	-	-	-	-	2
Security advice (Art. 22*quinquies* Classification and Security Clearances Act)					
Appeal Body did not have jurisdiction	4	0	0	20[215]	12[216]
Appeal inadmissible	4	6	15	10	3
Appeal devoid of purpose	4	0	0	1	3

215 The appeals in question had been lodged against (negative) security advice from the National Security Authority with regard to the personnel of subcontractors active at European institutions established in Belgium. The Appeal Body decided that there was no statutory basis for the advice formulated by the National Security Authority because the authority requesting the advice was not the same as the authority that wanted to use the advice to make a decision. Consequently, the Appeal Body declared itself lacking in jurisdiction to judge whether or not the security advice provided by the National Security Authority was well-founded.

216 Following the Appeal Body decisions referred to in the previous footnote, the authority changed its method of issuing advice for persons working for the European institutions. As no response was made to the criticism of the Appeal Body, it also had to declare itself lacking in jurisdiction in ten similar cases.

	2014	2015	2016	2017	2018
Confirmation of negative advice	53	28	42	49	46
Conversion to positive advice	41	23	46	41	27
Waiver of appeal granted	0	0	0	1	0
Appeal against normative legal actions (Art. 12 Appeal Body Act)	0	0	0	0	0
TOTAL	**163**	**137**	**173**	**195**	**144**

CHAPTER XI
INTERNAL FUNCTIONING OF THE STANDING COMMITTEE I

XI.1. COMPOSITION OF THE STANDING COMMITTEE I

The composition of the Committee changed considerably in 2018: the chair, Guy Rapaille[217] (F), Advocate-General of the Court of Appeal in Liège, was succeeded by Serge Lipszyc, first substitute labour prosecutor at the Labour Court in Liège (F), who was sworn in as the new chair on 25 September 2018.[218] Counsellor Gérald Vande Walle (F) reached retirement age on 31 December 2017 and was replaced in early 2018 by Laurent Van Doren, a former chief superintendent.[219] Counsellor Pieter-Alexander De Brock (N) remained in office.[220]

There were no changes at the Investigation Service I. The service thus continued to be composed of five 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 with 18 administrative personnel members. However, 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 personnel management and logistics).

---

217 In accordance with the opinion of the Chairpersons' Conference of 10 October 2018, Guy Rapaille was given the title of honorary chair of the Standing Committee I (CRIV54PLEN251).

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

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

220 On 26 September 2018, the Chamber of Representatives decided (CRIV54PLEN245) to publish a call for candidates for the position of Dutch-speaking member (*Belgian Official Journal* 27 September 2018) and for the positions of first and second Dutch-speaking substitute member, as Counsellor De Brock's term of office had expired on 7 May 2019. On the date of approval of this activity report no decision had yet been taken.

XI.2. MEETINGS WITH THE MONITORING COMMITTEE

In the course of 2018, four meetings were held with the Special Commission Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee.[221] The thirteen voting members of the Commission were: Koenraad Degroote (N-VA), Peter Buysrogge (N-VA), Peter De Roover (N-VA), Laurette Onkelinx (PS), André Frédéric (PS), David Clarinval (MR), Philippe Pivin (MR), Servais Verherstraeten (CD&V), Franky Demon (CD&V), Patrick Dewael (Open Vld), Hans Bonte (sp.a), Stefaan Van Hecke (Ecolo-Groen) and Georges Dallemagne (cdH). The Commission was chaired by the Speaker of the Chamber of Representatives Siegfried Bracke (N-VA).

During the Special Commission 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 overview provided by the Committee of all recommendations not yet implemented from the past ten years was also the subject of discussion.

In November 2018, the Activity Report 2017 of the Standing Committee I was discussed and the Special Commission took note of the Committee's prospective memorandum 2018–2020. The Special Commission '*took note of the Activity Report 2017 of the Standing Committee I and approved the Committee's recommendations*' (free translation).[222]

XI.3. JOINT MEETINGS WITH THE STANDING COMMITTEE P

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

221 In July 2018, the Monitoring Committee also organised an exchange of views with the Minister of Defence and the Head of GISS in the presence of the then chair of the Committee on the subject of the review investigation into the workings of the Counterintelligence Directorate.

222 *Parl. Doc.* Chamber of Representatives 2018–19, no. 54K3375/001 (Activity report 2017 of the Standing Committee on the Intelligence and Security Services, Report on behalf of the Special Commission Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee).

organise joint meetings. These joint meetings are chaired alternately by the chairs 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.

Two joint review investigations were on the agenda in 2018: the investigation started earlier into CUTA's supporting services (cf. I.6.3) and the investigation started in May 2018 into the '*information position of CUTA before the attack perpetrated in Liège*' (free translation) (cf. I.4).

Various other items were also on the agenda, including the possible adjustment of the administrative status, the drafting of an ethical charter, the discussion of the audit of institutions entitled to appropriations, the new data protection legislation and, in the same context, the appointment of a common Data Protection Officer (DPO). The preparations for organising a celebration to mark the 25th anniversary of the two Standing Committees were also discussed.

As well as informal contacts in the workplace, eight joint meetings took place in 2018.

XI.4. FINANCIAL RESOURCES AND ADMINISTRATIVE ACTIVITIES

Article 57 paragraph 1 of the Review Act states that the funds required for the Committee's functioning should be imputed to the appropriations budget. 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.[223] Until 2017 this appropriation was insufficient to cover the Committee's actual expenses, resulting in a systematic loss.

Conscious of this precarious situation and of the importance of maintaining equilibrium, the Chamber of Representatives decided to adjust the appropriation to ensure that the Committee's additional statutory duties can be carried out.

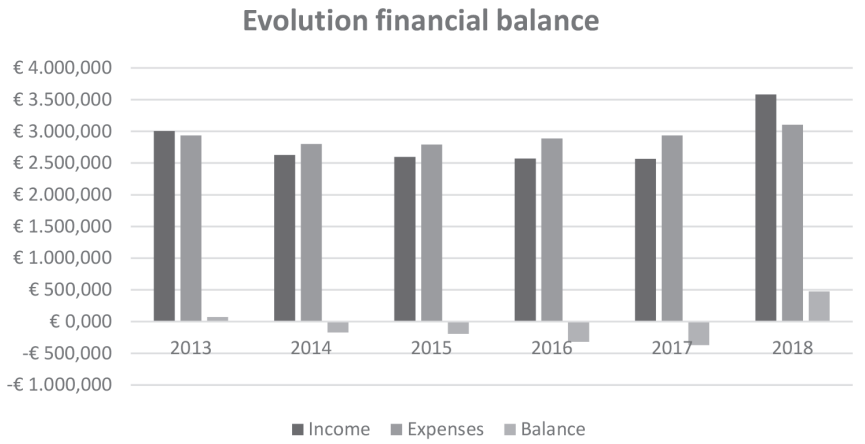
The Standing Committee I's 2018 budget was set at 3.759 million euros, up 3.4% on the 2017 budget. The sources of financing for this budget were allocated by the Chamber of Representatives[224] as follows: 95.26% appropriation budget and 4.74% surplus from 2016.

The implementation of the 2018 budget produced a budget surplus of 475,494 euros, consisting of the difference between income and combined expenses.

---

223 Act of 7 December 2017 on the general expenditure budget for the financial year 2018, *Belgian Official Journal* 28 December 2017.

224 *Parl. Doc.* 2017–2018 Chamber of Representatives, 54K2843/001, 24–29.



	2013	2014	2015	2016	2017	2018
Income	€ 3,005,000	€ 2,626,000	€ 2,597,000	€ 2,570,000	€ 2,565,000	€ 3,582,000
Expenses	€ 2,935,000	€ 2,799,000	€ 2,792,000	€ 2,889,000	€ 2,937,000	€ 3,106,000
Balance	€ 70,380	€ –173,000	€ –194,000	€ –318,000	€ –372,000	€ 475,400

Despite the surplus, the search for synergies between the various institutions entitled to appropriations remains high on the agenda. The development of these synergies has a very limited financial impact due to structural complications, such as the lack of mobility of personnel members from the various institutions (caused in turn by differences in employment status). However, they lead to better collaboration between the institutions, which improves the quality of the work carried out.

XI.5. AN EXTERNAL AUDIT AT ALL INSTITUTIONS ENTITLED TO APPROPRIATIONS

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 was to focus 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.

To enable this work to be carried out, the institutions had to provide numerous documents and information and answer a detailed series of questions on particular points (December 2017). Based on the information obtained, the investigation teams from the Court of Audit and Ernst and Young conducted interviews with a

number of key figures within the Committee (January-February 2018). At the end of February the draft report was submitted for comment during an exit meeting.

This audit created a lot of extra work for the Standing Committee I in addition to the already increased workload (*supra*).

The audit report[225] was delivered at the end of March 2018 and discussed by the Accounts Committee on 12 June 2018.

XI.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.[226] With regard to the latter category, the following study days were attended by one or more personnel or other members of the Standing Committee I.

DATE	TITLE	ORGANISATION	LOCATION
15 February 2018	Naar een herbekijking van de Belgische veiligheidsarchitectuur: de vaststellingen en aanbevelingen van de parlementaire onderzoekscommissie 'Terroristische aanslagen'	KU Leuven	Leuven
20–22 February 2018	Roundtable discussion 'on the outline of the guidelines for intelligence oversight'	Democratic Centre for Armed Forces (DCAF)	Skopje
15 March 2018	Cybercriminalité & cyberterrorisme	UC Liège	Liège
06 April 2018	Le renseignement et son contrôle	Council of State, France	Paris
04 May 2018	High Level Round Table on Public Security	European Corporate Security Association (ECSA) and SAS Institute	Leuven
30 May 2018	Info session – Implementation of the EU directive 2016/1148	European Corporate Security Association (ECSA) and Center for Cybersecurity Belgium (CCB)	Brussels
29 June 2018	International collaboration regarding intelligence services and intelligence studies	Belgian Intelligence Studies Centre (BISC)	Brussels

225 *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.

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

DATE	TITLE	ORGANISATION	LOCATION
24 September 2018	'SIGINT intelligence, surveillance, ethics and control' & 'Round table intelligence, surveillance and technology'	Université de Bordeaux	Paris
16 October 2018	Crypto War	KU Leuven	Brussels
12–19 October 2018	Sweepstakes	SHAPE	Lisbon
22 November 2018	10 ans de contrôle parlementaire du renseignement	Parliament, France	Paris
26 November 2018	Le futur de la Défense belge	Egmont Royal Institute for International Relations	Brussels
29–30 November 2018	International Intelligence Oversight Forum (IIOF 2018)	UN-High Commissioner for Human Rights	Malta
29 November 2018	20 jaar Wet houdende regeling van de inlichtingen- en veiligheidsdiensten	GISS/State Security	Brussels
6–7 December 2018	European Conference for Intelligence Oversight Bodies	Commission nationale de contrôle des techniques de renseignement (CNCTR) and the Standing Committee I	Paris

CHAPTER XII
RECOMMENDATIONS

Based on the review investigations, controls and inspections concluded in 2018, the Standing Committee I – in some cases with the Standing Committee P or the Supervisory Body for Police Information – has formulated the following recommendations. These relate, in particular, to the protection of the rights conferred on individuals by the Constitution and the law (XII.1), the coordination and efficiency of the intelligence services, CUTA and the supporting services (XII.2) and, finally, the optimisation of the review capabilities of the Standing Committee I (XII.3).

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

XII.1.1. 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). However, the Royal Decree referred to here has not yet been issued. The Standing Committee I urges that this be done as soon as possible.

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

XII.2.1. VARIOUS RECOMMENDATIONS FOR GISS ARISING FROM THE REVIEW INVESTIGATION INTO HOW THE COUNTERINTELLIGENCE DIRECTORATE OPERATES

The investigation into how the Counterintelligence (CI) Directorate of GISS operates provided an insight into the seriousness, complexity and multifaceted nature of the shortcomings within the CI Directorate.[227] 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. A number of recommendations were formulated to this end. 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).

XII.2.1.1. Recommendations with very high priority

Regarding mission, vision and planning cycle

- Formally determine a mission and vision for CI, including its role and duties with regard to counterterrorism, endorsed by all concerned and in line with the general policies, vision and ambition of GISS;
- Draw up an analysis and a plan concerning the nature of the intelligence (operational *versus* strategic) that CI must produce to meet the needs of users, paying due regard to the need for proactive and strategic analysis;
- Both internally (within GISS, within the CI Directorate and also vis-à-vis the I (Intelligence) Directorate) and externally (in relation to State Security, the Public Prosecutor's Office, CUTA and other agencies), GISS and the CI Directorate should work out an unequivocally supported position (set out in SLAs and protocols) on what can and should be expected from the service, taking the available resources into account. Once the vision, ambition and strategy have been worked out, they must actually be adhered to, so that the service can show itself to be a valuable partner in Belgian anti-terrorism policy.

227 See 'Chapter I.1. Operations of the Counterintelligence (CI) Directorate of GISS'.

- Prepare and formally approve synchronised planning at all levels of CI, up to and including the preparation of intelligence requirements (IRs) and information collection plans (ICPs);
- Specify in an internal guideline the control and planning methodology, tools and processes used, and the method of monitoring and evaluation.

Regarding the organisation and deployment of resources, workload measurement and distribution

- Prepare a concrete plan of the needs and the resources required to carry out the duties and tasks, and define as to how they will be implemented and attracted;
- Prepare a consolidated organisation chart showing functions, staffing, roles and communication lines;
- Introduce measurement tools for the collection of quantitative data on workload and output, and collect measurement results arising from such data in order to be able to distribute the workload evenly.

Regarding the organisation of and cooperation between analysis and collection

- Develop a formal plan in which the necessary (balanced) collection and analysis capacity is determined for each area, along with a guarantee that these capacities are and will remain available. If necessary, consider reorganising the analysis function as an independent pillar within CI;
- Prepare and keep available designs to guide the collaboration between collection and analysis (integrated intelligence requirements and information collection plans).

Regarding information management

- Prepare a schedule and a system in order to eliminate the backlog in the inputting of information into the database and to guarantee that incoming information will be input within a reasonable period;
- Perform a needs analysis at CI, including in the provincial posts, in order to determine who needs which systems (access to internal and external databases, software, etc.), and implement its findings;
- Organise a refresher training cycle to improve the knowledge and use of the available IT tools;
- Develop methods and internal guidelines to prevent phenomena such as 'broken links' and the creation of personal files and storage spaces from continuing to occur;

- Establish internal guidelines to govern cooperation between CI and support department J-6 (responsible for communication and information systems) so that the latter can respond to CI's needs more effectively;
- Designate an IT officer within CI who has the necessary time and knowledge for the function.

Regarding infrastructure

- Improve material conditions in the building used by the CI Directorate, as a matter of urgency;
- Eliminate the security risks relating to Operations Security (OpSec) that arise from defective material infrastructure.

XII.2.1.2. Recommendations with high priority

Regarding process management and the Standing Operating Procedures
- Develop process descriptions and formal procedures that describe the different aspects of the service's functioning and maintain an updated collection of Standard Operating Procedures (SOPs) that is distributed and actively explained to personnel;
- Appoint an officer within CI who oversees process management.

Regarding internal control and risk management

- Develop and implement within CI (but also within GISS) an internal control system, in which processes are monitored and deviations from the defined standards are detected and corrected;
- Develop and implement a risk management system, in which operational and other risks are identified and measures are taken to deal with them.

Regarding support and logistics, inside and outside CI

- Assess the logistical support needs within CI and prepare a plan to meet them;
- Document the way in which cooperation between CI and the support departments takes place, so that they can respond to CI's needs more effectively, and designate responsible persons within CI to liaise in particular areas (personnel, safety, training, etc.). Arrangements should be made to ensure that the support services have access to all the information they need to perform their duties properly, taking due account of the need for discretion;
- Any plan that applies defence-wide systems (in particular with regard to IT, but also purchasing management, etc.) to GISS and CI must include a study

of their consequences for GISS and CI and details of how undesirable consequences can be avoided.

Regarding communication and feedback

- Establish clear and formal communication guidelines within CI (what, how, who, when, etc.), thus moving away from the current culture of imparting information and instructions by word of mouth. Explicitly allocate the task of and responsibility for internal communication to an executive personnel member at CI;
- Design and apply systems for internal and external feedback to the employees involved.

Regarding personnel management and careers, training and education

- Identify and mitigate the risks and define the measures to be taken as a result of the rapid increase in the numbers of data collection personnel, in order to avoid jeopardising the balance between collection and analysis;
- Develop 'intelligence' as a study specialisation for military personnel wishing to work in the intelligence service, so that with proper grounding they can be both deployed in the field and build a real military career in the intelligence sector;
- Determine training needs and prepare a training plan in the areas where CI personnel lack up-to-date knowledge (legal, operational), and provide continuing training to remedy this. The same applies to the knowledge of management techniques for managers and prospective managers.

Regarding culture and tradecraft

- Develop an approach to bridge the differences in identity, counteract the sense of us and them, and build a genuine GISS culture in which there is understanding and respect for everyone's role and position;
- Set down on paper a formal procedure for dealing with delicate CI cases involving persons and/or military personnel from outside and/or inside the service, taking account of the required confidentiality. This should include clear determination of what responsibilities are involved, who should intervene when and to whom reports should be made when;
- Organise consultation between the various directorates of GISS in order to arrive at a consensus on the principles of tradecraft (including OpSec), with due respect for differences of role and position. As a result, a jointly supported manual should be prepared on the common understanding of tradecraft;
- Hold refresher training in the rules of tradecraft and OpSec, in particular when new personnel members arrive who do not have an intelligence background.

XII.2.1.3. Recommendations with moderate priority

Regarding the provincial detachments

- Conduct a study into the needs and areas of added value of the provincial detachments. Determine the job description and required resources to ensure at least a minimum staffing level and continuity (influence of holiday, illnesses, missions, meetings) for each post;
- Draw up and enforce rules to manage provincial detachments efficiently and to ensure the required flow of information and instructions;
- Start an investigation of IT needs in the provincial posts (including access to databases and IT tools).

Regarding employment statuses and the individual evaluation

- Investigate and prepare a plan for the elimination of inequalities (including financial) between personnel with different statuses;
- Identify the problems associated with the different statuses (recruitment, assessment, sanctioning, etc.), even if these cannot be tackled immediately.

XII.2.2. APPOINTMENT OF A STATION COMMANDER IN OPERATIONS ZONES

The Committee recommends that, in the event of military deployment in an operations zone, a station commander should be designated who is responsible for coordinating all the activities of GISS for all directorates, applying the principle of unity of command.

XII.2.3. EVALUATION OF THE GEOGRAPHICAL POSITIONING OF MILITARY UNITS

The Standing Committee I recommends that a regular evaluation be carried out on the optimal geographical location of the military units when deployed in an operation, taking into account the rapid changes that can happen in the security situation and the assignments given to the Belgian units.

XII.2.4. NO STRICT COMPARTMENTALISATION WITHIN GISS

With the exception of the specific circumstances in which GISS personnel members are themselves the subject of a security or intelligence investigation,

the Standing Committee I is not in favour of strict compartmentalisation between the GISS directorates. It should be made clear that anyone in possession of classified and sensitive information is bound to secrecy on pain of sanctions. Conversely, information that is classified and sensitive and that relates to Ministry of Defence personnel or to a threat must be shared within GISS.

XII.2.5. VARIOUS RECOMMENDATIONS TO IMPROVE THE FUNCTIONING OF AND COOPERATION BETWEEN THE SERVICES

In the context of the review investigation into the attack perpetrated in Liège, no findings were made that pointed to shortcomings in the police, intelligence and security services. In view of the recommendations of the parliamentary inquiry committee on terrorist attacks[228], the Standing Committees I and P formulated the following recommendations to improve the functioning of and cooperation between the services.

XII.2.5.1. The DGPI as a support service for CUTA

The competent ministers should take the initiative of designating the DGPI as a support service of CUTA, as this service occupies an important position in detecting and monitoring the radicalisation of prisoners.[229] In addition, the necessary conditions must be established to enable the DGPI to fulfil this role properly and effectively, such as the provision of quality collection and analysis capacity within the prison environment, the development of procedures, etc.

XII.2.5.2. Unambiguous terminology in the normative framework

The competent authorities must examine the various applicable normative texts (laws, decrees, circular letters, memoranda, etc.) in order to determine whether the terminology used (signs of radicalisation, violent/non-violent radicalisation, proselytism, etc.) is explicit, clear and defined consistently, and make any

---

228 *Parl. Doc.* Chamber of Representatives, 2017–18, 54K1752/009, title 2 (Fourth interim report on 'Radicalism', 23 October 2017, Chapter III, point 4, See in particular marginal numbers 151–152 on the development of training for prison officers to include the identification of signs of radicalism and the creation of contact persons for radicalism in each institution with a view to collecting and analysing information derived from the observation of prisoners, as well as marginal numbers 159–161 on the exchange of information between the prison service and other services.).

229 This recommendation was implemented by means of the Royal Decree of 17 August 2018 implementing Article 2, first paragraph, 2°, g) of the Act of 10 July 2006 on threat analysis (*Belgian Official Journal* 12 September 2018).

necessary adjustments. The use of the same terminology in all the services involved will help ensure effective exchange of data and cooperation.

XII.2.5.3. Databases of radicalised prisoners

The services which come together in the Radicalism Plan Prisons Working Group were supposed to submit a proposal to the competent ministers by the end of 2018 regarding what data on prisoners should be included in which databases/lists (and deleted if necessary), with whom it can be shared, and under what conditions. As part of this proposal:

- It should be determined which procedures for data exchange and creation of databases require further formalisation, and proposals should be made accordingly;
- A division of tasks should be agreed with a view to exchanging information about these individuals, analysing it and making it accessible to the various services, and determining what information and according to what procedures will be placed in the common database if necessary (subject to adjustment of the relevant regulatory framework);
- An estimate should be made of the resources needed to put this into practice.

The different purposes of the services involved should not be undermined in strengthening each party's information position (intelligence purpose, law enforcement and combating crime, threat analysis, prisoner management and deradicalisation).

XII.2.6. RECOMMENDATIONS CONCERNING THE COMMON DATABASES[230]

XII.2.6.1. Appointment of a security adviser[231]

The failure to appoint a security adviser or a Data Protection Officer (DPO) remains a major shortcoming, especially as they are points of contact for the Supervisory Body for Police Information and the Standing Committee I. The Ministers of Home Affairs and of Justice, who are the data controllers, justify this situation by stating that the Policing Act was going to be revised after the adjustment of the statutory framework on the protection of privacy. However, the Supervisory Body for Police Information and the Standing Committee I conduct checks on the basis of the applicable (and not the future) regulations.

230 The first recommendations repeat previously formulated recommendations (www.comiteri.be).

231 See STANDING COMMITTEE I, *Activity Report 2017*, 55.

Moreover, they noted that the absence of a security adviser causes practical problems (inadmissibility in the event of a logged information check requested by a service; sudden and inexplicable periods in which the database is unavailable; lack of a coordinated approach to security incidents, etc.). The Supervisory Body for Police Information and the Standing Committee I therefore maintain their previous recommendation to make the necessary appointments.[232]

XII.2.6.2. IT tool for monitoring retention periods

The Supervisory Body for Police Information and the Standing Committee I reiterate their recommendation that an IT tool should be developed that makes it possible to monitor the data retention periods referred to in Article 44/11/3*bis* §5 of the Policing Act.

XII.2.6.3. Information obligation regarding security incidents

The Supervisory Body for Police Information and the Standing Committee I wish to be kept closely informed in the event of a security incident that may affect the confidentiality of the common database.

XII.2.6.4. Need to ensure secure data transfer

The Supervisory Body for Police Information and the Standing Committee I did not receive formal confirmation on the occasion of their audit mission that the evaluation referred to in Article 44/11/3*quater* of the Policing Act is carried out systematically and in advance with regard to the transfer of (extracts from) the information card to third-party bodies (i.e. bodies not referred to in Article 44/11/3*ter* of the Policing Act). Moreover, they recall their earlier recommendation regarding the need to ensure secure transfer.

XII.2.6.5. Unannounced checking of logged information

With the exception of one inspected service, the recommendation to spontaneously check logged information was not followed. Some services reported that they have taken (or will soon take) initiatives in this regard. The previously formulated recommendation therefore remains applicable.

232 A DPO has now been appointed by the two Ministers.

XII.2.6.6. Recommendations concerning the lists of names intended for third parties

The modification of the statutory framework with regard to the extraction and transfer of lists to third parties has compelled the Supervisory Body for Police Information and the Standing Committee I to formulate various recommendations:

- Automatic comparisons require extensive testing, and all decisions must be made after human intervention and validation;
- The basic service providing a list must duly inform the recipient of the list (about the purpose of the list in light of the recipient's statutory duties, the use of the list solely for that purpose, the limited retention of the list, the required security and confidentiality measures, etc.), for example by concluding a protocol agreement with the receiving service;
- Precautions must be taken to ensure that the use of these lists by third parties meets security conditions (confidentiality, integrity, etc.) equivalent to those set out in the common database rules;
- The rules on the common databases give neither the Supervisory Body for Police Information nor the Standing Committee I the authority to monitor the use of the lists by third parties. Both recommend that the data controllers should assess whether the statutory framework is adequate in this regard, in particular in light of the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data.

XII.2.6.7. Operationalisation of direct access and direct information retrievals

By mid-2018, a significant number of partner services and law centres did not yet have access to the production environment of the common database and were therefore not using it. The Supervisory Body for Police Information and the Standing Committee naturally recommended that this situation be remedied.

In addition, the right of the Governmental Coordination and Crisis Centre to make direct information retrievals must be formalised.

Finally, the Supervisory Body for Police Information and the Standing Committee I stated that the regulatory framework should, if necessary, be adapted to the practical reality that certain central services of the DGPI input data into the database and not the prisons themselves, as stipulated in the RD (F) TF.

XII.2.6.8. Management of required security clearances

The Supervisory Body for Police Information and the Standing Committee I recommended that the (fairly lengthy) procedures for applying for security

clearances be initiated promptly. Conversely, any loss of a personnel member's need-to-know status must be systematically reported in order to prevent unnecessary access clearances from being maintained or security investigations that no longer serve any purpose from being continued.

XII.2.6.9. Updating of validation procedures

The validation procedures communicated by certain services prior to or on the occasion of the inspection conducted in 2018 related only to FTFs and need to be updated for HTFs and HPs. Moreover, the *Vlaamse Agentschap Jongerenwelzijn* (Agency for Youth Welfare of the Flemish Community) must implement an internal validation system[233] (Article 8 of the RD TF).

XII.2.7. ADDITIONAL TRANSLATION CAPACITY IN THE CONTEXT OF SIGINT DUTIES[234]

In order to achieve its objectives and to be able to perform its statutory duties, GISS needs to have sufficient human and technical resources in the SIGINT field. The elimination of the shortage of personnel able to handle translations must be a priority in this regard.

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

XII.3.1. REGISTRATION AND PROVISION OF DATA ON ORDINARY METHODS

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 under Article 16/2 of the Intelligence Services Act. In its previous activity report, the Committee recommended that the services also record this data and make it available.[235] This has not happened so far; the Committee therefore repeats its recommendation.

233 See 'Chapter VI. Monitoring of the common databases'.
234 See 'Chapter III. Monitoring of foreign interceptions, image recordings and IT intrusions'.
235 STANDING COMMITTEE I, *Activity Report 2017*, 50–51.

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 support services satisfy the obligation laid down in Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.
An Investigation Service shall be established for each of these committees.

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

The review referred to in this Act is governed without prejudice to the review or inspection governed by or by virtue of other legislation. In the event of review or inspection governed by or by virtue of other legislation, the review referred to in this Act relating to the activities, methods, documents and directives of the

police services and of the intelligence and security services, shall only be undertaken to ensure fulfilment of the assignments provided for in this Act.

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

1° "Police services": in addition to the local police and the federal police, the services that come under the authority of the public authorities and public interest institutions, whose members have been invested with the capacity of judicial police officer or judicial police agent;
2° "Intelligence services": State Security and the General Intelligence and Security Service of the Armed Forces;
3° "Coordination Unit for Threat Assessment": the service referred to in the Act of 10 July 2006 on threat assessment;
4° "Other support services": the services other than the police services and the intelligence and security services referred to in this Act, that are required, in accordance with the Act of 10 July 2006 on threat assessment, to pass on information to the Coordination Unit for Threat Assessment;
5° "Threat Assessment Act": the Act of 10 July 2006 on threat assessment;
6° "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 intelligence, criminal law or criminology, public law, personal data protection law or management techniques, acquired in positions related to the operation, activities and organisation of the police services or of the intelligence and security services, as well as having held positions requiring a high level of responsibility;
6° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

The members and their substitutes may not hold a public elected office. They may not perform a public or private function or activity that could jeopardise the independence or dignity of the office. They may not be members of the Standing Police Services Review Committee, nor of a police service, an intelligence service, the Coordination Unit for Threat Assessment, or another support service, 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, certificates and advice.

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 Home Affairs, with regard to the assignments of State Security relating to the maintenance of law and order and the protection of people […];
5° The National Security Council, with regard to the Coordination Unit for Threat Assessment or the other support services.

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

Subsection 3 – Assignments

Art. 32
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 support 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 support services shall, on their own initiative, send to the Standing Committee I the internal rules and directives, as well as all documents regulating the conduct of the members of these services. The Standing Committee I and the Investigation Service for the intelligence services shall have the right to be provided with all texts that they consider necessary for the performance of their assignment. The Standing Committee I may, based on a reasoned request of its Chairman, request the administrative authorities to provide it with the regulations, guidelines and documents issued by these authorities which the Committee considers essential for the performance of its assignment. The concerned administrative authority has the right to assess whether it is relevant to communicate the requested regulations, guidelines and documents to the Standing Committee I.

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

This report shall include the conclusions relating to the texts, activities, methods or the processing of personal data 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 66*bis* shall be informed of the request of the minister to the Standing Committee I and of the content of the report before the end of the term laid down in Article 35, §1, 3°.

Art. 34

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

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, a denunciation or a request 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, a denunciation or a request 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 support service, depending on the case, of the conclusions of the investigation.

Art. 35

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

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the Chamber of Representatives and the Senate, and to the competent ministers by 1 June at the latest. In this report, the Standing Committee I shall pay special attention to the specific and exceptional methods for gathering information, as referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, as also to the application of Chapter IV/2 of the same Act and to the implementation of the Act of 10 July 2006 on threat assessment.
2° When the Chamber of Representatives has entrusted it with an investigation.
3° When at the end of a period that it believes to be reasonable, it notes that no action has been taken concerning its conclusions, or that the measures taken are inappropriate or inadequate. This period may not be less than sixty days.

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

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

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

§ 3. The Standing Committee I shall present a 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 to State Security, the General and Security Service which are entitled to draw the Standing Committee I's attention 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 support services, on its own initiative, in which case it shall immediately inform the Chairman of the Standing Committee I, the Investigation Service for the intelligence services, hereinafter referred to as the "Investigation Service I", shall supervise the operations of the intelligence services, the Coordination Unit for Threat Assessment and the other support services, through investigations, within the limits of Article 1.

It shall examine the complaints, denunciations and requests of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another support service. Any public officer, any person performing a public function, and any member of the Armed Forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods, actions or processing of personal data, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

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

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

Art. 41

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

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

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

He must have knowledge of the French and Dutch languages.

He shall retain his right to advancement and salary increase.

He may be dismissed by the Standing Committee I.

Art. 42

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

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

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

Art. 43

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

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

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

Art. 44

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

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

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 support services which are being heard may testify about facts covered by professional secrecy.

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

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

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

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

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

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

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

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

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

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

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

SECTION 4 – POWERS OF THE STANDING COMMITTEE I AS DATA PROTECTION AUTHORITY

Art. 51/1
As a 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 subject.

Art. 51/2
To be admissible, the request if written, dated, signed and reasoned, and justify the identify of the person concerned.

Art. 51/3
The Standing Committee I on the follow-up he gives to the file and has the competence 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 file to the Brussels public prosecutor's office, who informs him of the action taken on the file.

Art. 51/4
The Standing Committee I informs the services concerned of the surveys carried out on the processing of personal data by its processors and their results.

When it becomes aware of it, the Standing Committee I also informs the services concerned of breaches of the regulations relating to the processing of its personal data by other controllers.

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 Home Affairs, Justice and National Defence, or at the request of the Chamber of Representatives;
4° With regard to any question that each Standing Committee believes does not fall within its exclusive competence;

5° With regard to any question considered by a Standing Committee to be sufficiently important to warrant a joint meeting;
6° With regard to the Coordination Unit for Threat Assessment or another support service.

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

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

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

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

CHAPTER V – COMMON PROVISIONS

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

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

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

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

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

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

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

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

Art. 59

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

Art. 60

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

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

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

Art. 61

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

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

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

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

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

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

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

The following are excluded from this allowance:

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

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

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

Art. 61*bis*

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

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

Art. 62
Without prejudice to Article 58, the registrar shall act under the collegial authority and the supervision of the Standing Committee in question, the registrar of each Committee shall among others manage the following:

the administrative staff;

the infrastructure and equipment of the Committee;

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

the sending of documents;

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

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

Art. 63
The members of the Standing Committees are prohibited from attending the deliberations on affairs in which they have a direct or personal interest, or in which relatives by blood or marriage to the fourth degree inclusive, have a direct or personal interest.

Art. 64
The members of the Standing Committees, the registrars, the members of the Investigation Services, and the administrative staff shall be obliged to preserve the secrecy of the information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

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

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

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

Art. 66
Excluding its Chairman, each Standing Committee shall have as many French-speaking members as Dutch-speaking members.

The Chairman of one of the Standing Committees shall be French-speaking, the Chairman of the other Dutch-speaking.

Art. 66*bis*

§1. The Chamber of Representatives shall create a permanent committee responsible for monitoring the Standing Committee P and the Standing Committee I.

The Chamber of Representatives shall stipulate in its regulation, the rules relating to the composition and functioning of the monitoring committee.

§2. The monitoring committee shall supervise the operation of the Standing Committees, and ensure observance of the provisions of this Act and the rules of procedure.

The monitoring committee shall also perform the assignments assigned to the Chamber of Representatives by Articles 8, 9, 11, 1°bis, 2° and 3°, 12, 32, 33, 35, §1, 2° and 3°, 36 and 60.

§3. The monitoring committee shall meet at least once per quarter with the President or the members of each Standing Committee. The monitoring committee can also meet at the request of the majority of its members, at the request of the Chairman of one Standing Committee, or at the request of the majority of the members of a Standing Committee.

Every denunciation by a member of a Standing Committee relating to the inadequate functioning of that Standing Committee, the non-observance of this Act, or the rules of procedure, may be brought before the monitoring committee.

The monitoring committee may issue recommendations to each Standing Committee, or to each of its members, relating to the functioning of the Standing Committee, the observance of this Act, or the rules of procedure.

§4. The members of the monitoring committee shall take the necessary measures to safeguard the confidential nature of the facts, acts or intelligence that they have knowledge of by virtue of their position, and shall be subject to an obligation of confidentiality. They shall be obliged to preserve the secrecy of any information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Any violation of this obligation of confidentiality shall be penalised in accordance with the rules of the Chamber of Representatives.

30 NOVEMBER 1998
ACT GOVERNING THE INTELLIGENCE AND SECURITY SERVICES
(*extract updated in April 2020*)

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 44/4 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, authorizations, 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 judicial 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.]

(…)

STRENGTHENING OVERSIGHT OF INTERNATIONAL DATA EXCHANGE BETWEEN INTELLIGENCE AND SECURITY SERVICES

Belgian Standing Intelligence Agencies Review Committee

(Comité permanent de Contrôle des services de renseignement et de sécurité / Vast Comité van Toezicht op de inlichtingen- en veiligheidsdiensten)
www.comiteri.be

Danish Intelligence Oversight Board
(Tilsynet med Efterretningstjenesterne)
www.tet.dk

Review Committee on the Intelligence and Security Services - The Netherlands
(Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten)
www.ctivd.nl

EOS Committee - The Norwegian Parliamentary Intelligence Oversight Committee
(EOS-utvalget)
www.eos-utvalget.no

Independent Oversight Authority for Intelligence Activities (OA-IA)
(Unabhängige Aufsichtsbehörde über die nachrichtendienstlichen Tätigkeiten AB-ND/ Autorité de surveillance indépendante des activités de renseignement AS-Rens)
www.ab-nd.admin.ch

1. CONTENT

Five European intelligence oversight bodies have begun a new form of cooperation. In this statement, we will:

Describe our project, which entailed each of us conducting an investigation into our respective countries' services' use of information regarding foreign terrorist fighters and sharing our methods, best practices and experiences.

- Address the challenges we met when overseeing international data exchange, including the risk of an oversight gap when intelligence and security services cooperate internationally.
- Identify ways to move forward towards strengthening oversight cooperation, for example through minimizing secrecy between oversight bodies so that certain information can be shared, in order to improve our oversight of international data exchange.

2. INTRODUCTION

Recent terrorist attacks, such as in Paris, Brussels and London, were carried out by persons directed, encouraged or inspired by ISIS, Al-Qaeda or similar terrorist groups. To identify and investigate the threat of homegrown and returning foreign terrorist fighters is an important task for intelligence and security services across Europe.

The threat of jihadist terrorism has become more complex and widespread in recent years. Investigating this threat requires international cooperation between intelligence and security services, either bilaterally or multilaterally. Such cooperation exists within Europe and with other countries. As this cooperation has intensified, the exchange of personal data between services has increased. The exchange of data with foreign services is part of the intelligence and security services' day-to-day activities. Data may be exchanged in various ways, either orally or in writing.

The oversight bodies have naturally followed the development of international cooperation between intelligence and security services. As our respective oversight mandate is strictly national, we have been concerned with the risk of an "oversight gap" occurring. In an ideal situation, the national systems of oversight would be complementary to each other: where one oversight body reaches the boundaries of its national mandate, the other is competent to effectively oversee. However, national legislation regarding exchange of data and the oversight of such exchanges may not meet these requirements. Moreover, international cooperation between intelligence services could develop in such a way, that

national oversight can no longer keep up. Then an "accountability deficit" or "oversight gap" could emerge.

In light of this, the five oversight bodies from Belgium, Denmark, the Netherlands, Norway and Switzerland decided to start a joint project to exchange experiences and methods. Each of the oversight bodies conducted a national investigation into the international exchange of data on foreign terrorist fighters by the intelligence and security services they oversee.[236]

We conducted the national investigations more or less at the same time, each from our national context and within the framework of our national mandate. We have met regularly to compare investigation methods, interpret legal frameworks, discuss legal and practical problems and to collate our findings and conclusions. Classified information was not exchanged.

3. CURRENT PRACTICES IN OVERSIGHT OF DATA EXCHANGE

The participating oversight bodies oversee data exchange between intelligence and security services in several ways. We may

- assess cooperative relations or arrangements between intelligence and security services;
- assess the legitimacy and quality of specific data exchanges with foreign services;
- review the system of data exchange as a whole, including the safeguards;
- be involved in procedures concerning individual remedies and complaints.

Although the mandates of the oversight bodies are different, we all have a diverse range of instruments for overseeing international data exchange.

Assessment of the cooperative relationship

Oversight bodies may assess whether or not the cooperative relationship between their country's service and partner services in other countries meets certain criteria. Legislation governing the intelligence and security services may specifically state criteria for cooperation. Typically, criteria include the necessity for cooperation, the respect for human rights, the existence of legislation on data protection and/or reliability. The threshold for cooperating with services that do not meet the criteria should be high. The oversight bodies of Belgium, the Netherlands, Norway and Switzerland review the considerations made in that respect by their national services.

236 The report from CTIVD (The Netherlands) about the investigation in English – https://english.ctivd.nl/latest/ news/2018/04/26/index
The annual reports from the Danish Intelligence Oversight Board in English – www.tet.dk/redegorelser/?lang=en

Cooperative relationships between the services can be based on agreements, for example letters of intent or memorandums of understanding. Such agreements are usually not legally enforceable but offer a practical framework on the exchange of data by services. Even the existence of some of these agreements is classified. Other agreements are made public by governments or the services. Nevertheless, they may draw the outline of the cooperative relationship by addressing issues like the purpose of the cooperation, how the cooperation is expected to function, limitations concerning disclosure to third parties or procedural aspects of the cooperation. The oversight bodies of all five countries may either review or report on whether these agreements comply with national laws and regulations.

Assessment of the legitimacy of specific data exchanges

Oversight bodies may assess whether individual data exchanges meet the legal requirements imposed by national laws and regulations.

The national legislations of our countries share certain characteristics, most notably the principles of necessity and proportionality. These shared principles originate from international legal frameworks such as the European Convention on Human Rights. The principle of necessity includes the requirement of a clear and legal purpose for the data exchange and the reasonable expectation that this purpose will be met by exchanging the data. The principle of proportionality requires the service to balance the purpose of the exchange against the gravity of the infringement of fundamental rights. Most national legislation contains other requirements as well, such as the reasonableness, correctness, effectiveness and reliability of data exchange.

The internal policy of the services may provide additional rules for data exchange. Such policy may, for example, further specify which type of data exchange is allowed under which circumstances, which authorisation level is required and which use may be made of data received. When national law or bilateral and multilateral agreements are absent or silent on a specific matter, internal policy can provide additional safeguards.

Assessment of the quality of specific data exchanges

Quality may relate to the content of the data or the format of the data. When it comes to content, quality means the data is correct, sufficiently clear and precise in its wording, confirmed by underlying data, up to date and with an indication of probability or reliability. As for format, quality aspects relate to the inclusion of a classification level, the date of exchange, the designated receiving partner service(s) and caveats regarding further use of data. All five oversight bodies can review the quality of data exchange in this respect.

Quality may also have a different meaning. It may relate to efficiency or effectiveness, that is whether the data exchange is relevant, whether the exchange happened in a timely manner and whether it fulfilled its purpose. This type of quality review is less common for oversight bodies. The oversight bodies of Belgium and Switzerland are expressly authorised to review whether data exchange has been effective and efficient.

Review of the system of data exchange as a whole

Oversight bodies may adopt a broader approach when reviewing the legitimacy of data exchange. In reviewing certain multilateral cooperative frameworks, the oversight body in the Netherlands expressly looks at the system of data exchange as a whole and at the protection of individual rights within that system. Even though certain specific data exchanges may be legitimate, there can still be insufficient safeguards in the system to ensure the legitimacy of data exchange in the longer run. This type of review may help prevent unlawful data exchange between intelligence and security services.

One could take a similar approach when reviewing the quality of data exchange. When the purpose of exchanging data is to counter jihadism, the general quality of data exchange could be measured by investigating the amount of shared information that led to prosecution and conviction, or even to a direct prevention of a terrorist attack. However, measuring the usefulness of exchanged data in this way can be challenging. Such reviews are often initiated after a terrorist attack has occurred. Then the oversight body assesses if the relevant data had sufficiently and adequately been exchanged with national and international partners. The oversight body of Belgium has been involved in this type of review.

Involvement in individual remedies and complaints

In general, oversight bodies in all five countries can receive complaints from individuals regarding the activities of the national intelligence and security services. Usually oversight bodies may offer non-legally binding opinions or recommendations to the intelligence and security services and/or the ministers who are politically responsible. The services usually comply with such opinions or recommendations. A new law was adopted in the Netherlands in 2017, granting the oversight body the power to take binding decisions on complaints. This may also include ordering the exercise of a power to be terminated or the destruction or removal of processed data.

The secrecy that is necessary for the intelligence and security services to conduct their activities usually limits the right of the individual to access personal data. Some countries explicitly afford individuals the right to request the national

oversight body to review the personal data their services have processed about them. In Denmark, any person may ask the Danish oversight body to investigate whether the security service is unlawfully processing personal data about them. In case of the military intelligence service, this review is limited to residents of Denmark. In both cases, the Danish oversight body may order the deletion of personal data regarding the applicant.

In Belgium the oversight body has an obligation to investigate all complaints that are not manifestly unfounded. The complainant will receive the findings of the investigation in general terms. The complainant then has the possibility to use these findings before the court or an administrative authority. In some specific cases the oversight body must give an official advice to a criminal court following a complaint and regarding two other topics of complaint (use of special methods and data protection), the committee may take binding decisions.

In Norway, residents have the same right to complain to the oversight body if a citizen suspects that he/she is subject to unlawful surveillance. However, the Norwegian oversight body does not have the authority to order deletion of data. In Switzerland, the Federal Data Protection and Information Commissioner (FDPIC) handles individual requests on data processing.

4. CHALLENGES FOR OVERSIGHT OF INTERNATIONAL DATA EXCHANGE

In the course of our project we have found that the increased cooperation between intelligence and security services and the exchange of data between these services, especially on the multilateral level, may pose legal and practical challenges to the oversight bodies.

Oversight does not cross national borders

National legislation often promotes the cooperation and exchange of information between intelligence and security services, both bilaterally and multilaterally. However, it usually does not provide a specific legal basis for oversight bodies to cooperate or exchange information on individuals. None of the five oversight bodies working together in the context of this common publication has an explicit legal basis to exchange data with another oversight body, certainly not when this information is classified.

Where intelligence and security services cross national borders, oversight bodies cannot. Oversight is limited to national mandates. This reflects one side of data exchange: either oversight will focus on the provision of data and its prior collection, or it will focus on the reception of data and its use. National oversight

bodies will not independently be able to acquire a full picture of personal data exchange, let alone review the lawfulness of the entire process of exchange.

Such a limit to national oversight does not necessarily constitute an oversight gap. When oversight is exhaustive and effective on both sides of the border, no gap exists between the mandates of the oversight bodies. However, when it comes to cooperation between intelligence and security services – predominantly multilateral cooperation – the cooperation of oversight bodies is only as strong as its weakest link.

The challenge of cooperation in the face of secrecy

Oversight bodies are limited to national rules on secrecy and cannot share and discuss the substance of their investigations beyond what is designated as public information. In practice, this means that oversight bodies have very limited insight into whether 'the other side' of data exchange is effectively overseen or whether an oversight gap exists. Therefore, oversight activities are not only unable to cross borders; they are also largely unable to share with other oversight bodies what occurs within their borders.

As the joint project between the five oversight bodies progressed, we found ourselves on numerous occasions aware of the fact that we were not even in a position to discuss matters known to us all, e.g. the content of agreements between the services we oversee. In addition, we became aware that what is public information in one country might be deemed confidential in another. This has led to difficulties for this project, limiting the possibility to reach substantial discussion on the matter in question.

Assessment of necessity and proportionality

As mentioned above, oversight bodies continuously assess whether the exchange of data is necessary for a specific purpose and proportionate to the aim pursued. This requires that oversight bodies consider the level of protection of individual rights provided by the receiving service. As the volume of data exchanges and the number of foreign services with which the data is shared increase, this will be more and more challenging for oversight bodies. This test of necessity and proportionality can become more abstract and can lose value as the data exchanged is less specific or if it is exchanged within a larger group of intelligence and security services.

Different national legal regimes may include different legitimacy and quality standards for data collection, processing, retention and exchange. The level of protection of individual rights afforded by the service receiving the data is an

important element in assessing the proportionality of a particular data exchange. This is not always easy to determine as intelligence and security services may not be open about all aspects of the legal framework in place and the standards they apply.

In the context of multilateral data exchange, common standards and definitions could help define under which circumstances data exchange is regarded as necessary and proportionate, and which minimum level of data protection needs to be in place to sufficiently safeguard individual rights. There is a common interest of all parties – intelligence and security services and oversight bodies – in having such common standards and a common interpretation of existing legal safeguards. This may also add to the legitimacy of the multilateral exchange in question.

Some countries differentiate between citizens and foreigners

Some national legal frameworks offer nationals or residents a higher level of protection and more privileged access to individual remedies than foreigners or non-residents. The distinction between these groups may result in limited or no access to individual remedies for foreigners or non-residents whose data has been exchanged by the respective intelligence or security service.

A similar distinction may determine the mandate of the oversight body. Some oversight bodies only have the mandate to review data exchange with regard to nationals or residents. The provision of data with regard to other persons may lie beyond their reach. If no other oversight body may effectively review this part of the data exchange, an oversight gap exists.

Means and methods of data exchange

Intelligence and security services exchange data in various ways. Some means and methods of data exchange pose further challenges for oversight bodies. An example of such a challenge is the informal exchange of data, and how to provide efficient oversight of data exchanged during conferences and meetings, by phone and so on. The increase in international data exchange may require oversight bodies to come up with more advanced methods of oversight, as it is no longer feasible to review each exchange of data. With regard to data protection, developments in multilateral data exchange may invoke responsibilities for each of the participating services as well as the oversight bodies. To safeguard individual rights adequately, it may be required that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services.

5. OVERSIGHT OF INTERNATIONAL DATA EXCHANGE – MOVING FORWARD

Our project has shown us that the efforts of the intelligence and security services to find new ways to exchange data effectively, especially on a multilateral level, and the large increase in the volume of data exchanged, have in turn led to new challenges for the oversight bodies. This applies both to the limits of the oversight bodies' national mandates, their inability to adequately discuss international data exchange with other oversight bodies as well as to their own efforts to innovate their procedures and methods to ensure effective oversight.

National sovereignty and interests dictate the international cooperation between intelligence and security services. It is to be expected that, unlike other areas of international cooperation, oversight of the intelligence and security services will continue to be carried out by national oversight bodies. However, where intelligence and security services cross national borders, oversight bodies cannot. Consequently, over sight always reflects on one side of data exchange. Moreover, oversight bodies are largely unable to share with other oversight bodies their review of a particular data exchange. Because of these limits to national oversight, there is a risk of an oversight gap with regard to international data exchange by intelligence and security services. The question remains how to tackle such a risk.

By exchanging knowledge, experience and investigation methods, and by comparing their findings, conclusions and recommendations, oversight bodies may come closer together. Our experience is that this is precisely what this common project has accomplished. We have learned from each other's best practices, developed more understanding of each other's legal systems and we have built a level of trust. In order for oversight bodies to keep up with developments in international cooperation between intelligence and security services, we need to do just that: intensify our cooperation.

A valuable and necessary step towards closer cooperation is to minimize secrecy when sharing information between oversight bodies. At the minimum, oversight bodies could be able to discuss concrete bilateral and multilateral cooperative arrangements between the intelligence and security services they oversee. A logical additional step could be to share information with other oversight bodies that has already been shared by the intelligence and security services themselves. Once data has been exchanged, there is no need for oversight to lag behind. We do not suggest that all national secrecy limitations should be set aside, to the contrary. Cooperation between oversight bodies should take place within the limits and according to the standards set by national legislators.

Being able to discuss international cooperative arrangements and data exchange with other oversight bodies also comes with certain responsibilities. Adequately safeguarding individual rights while cooperating internationally, not only requires that intelligence and security services discuss the standards they apply and work towards an equal minimum level of protection offered by all participating services. It also requires oversight bodies to uphold such a minimum level of data protection and try to find common ground in interpreting existing legal safeguards.

Conducting spot checks, it is becoming increasingly important to assess the system and framework for data exchange and the existence and functioning of safeguards for the protection of fundamental rights.

To do this effectively, oversight bodies will need to develop new methods. One way forward may be to increasingly use computerized automation and tools developed for conducting oversight of large volumes of data. In order to achieve this, oversight bodies need to expand their IT expertise and knowledge of the services' systems. Another way to facilitate a more effective oversight would be to take the needs of the oversight bodies into account when the services implement new systems and to strengthen mechanisms of internal and external control.

The oversight bodies of Belgium, Denmark, the Netherlands, Norway and Switzerland will continue to exchange methods and best practices, as well as discuss international challenges to oversight, and the best approaches to overcoming these challenges. We invite oversight bodies from other countries to join us in our efforts to limit the risk of an oversight gap and to improve oversight of international data exchange between intelligence and security services.

Signed in Bern on 22 October 2018,

Mr. Serge Lipszyc, Chair of the Belgian Standing Intelligence Agencies Review Committee

Mr. Michael Kistrup, Chair of the Danish Intelligence Oversight Board

Mr. Harm Brouwer, Chair of the Dutch Review Committee on the Intelligence and Security Services

Mrs. Eldbjørg Løwer, Chair of the EOS Committee – The Norwegian Parliamentary Intelligence Oversight Committee

Mr. Thomas Fritschi, Director of the Independent Oversight Authority for Intelligence Activities