Activity Report 2020

Belgian Standing Committee I

Belgian Standing Intelligence Agencies
Review Committee

ACTIVITY REPORT 2020

Belgian Standing Intelligence Agencies Review Committee

Belgian Standing Intelligence Agencies Review Committee

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

Activity Report 2020
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

CONTENTS

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
BSS	British Security Service (MI5)
CDB HP	Common database Hate Propagandist
CDB TF	Common database Terrorist Fighters
CHOD	Chief of Defence
CI	Counterintelligence
Classification and Security Clearances Act	Act of 11 December 1998 on classification and security clearances, certificates and advice
CNCIS	*Commission nationale de contrôle des interceptions de sécurité*
CNCTR	*Commission nationale de contrôle des techniques de renseignement*
C.O.C.	Supervisory Body for Police Information
CSA	Competent Supervisory Authority
CTIVD	*Commissie van Toezicht op de inlichtingen- en veiligheidsdiensten*
CUTA	Coordination Unit for Threat Assessment
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
DRI	Directorate of Police Information and ICT Resources of the Federal Police
EU	European Union
FANC	Federal Agency for Nuclear Control
FIRM	Federal Institute for the Protection and Promotion of Human Rights
FPS	Federal Public Service
FTF	Foreign Terrorist Fighter
GCHQ	General Communications Headquarters
GDPR	General Data Protection Regulation

GISS	General Intelligence and Security Service of the Armed Forces (*Algemene Dienst Inlichting en Veiligheid van de Krijgsmacht – Service Général du Renseignement et de la Sécurité des Forces armées*)
HP	Hate Propagandist
HTF	Homegrown Terrorist Fighter
HUMINT	Human intelligence
ICT	Information and communications technology
Intelligence Services Act	Act of 30 November 1998 governing the intelligence and security services
IOWG	Intelligence Oversight Working Group
IPCO	Investigatory Powers Commissioner's Office
ISTAR	Intelligence, Surveillance, Target Acquisition & Reconnaissance
IT	Information Technology
MoU	Memorandum of Understanding
NATO	North Atlantic Treaty Organisation
NSA	National Security Authority
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
Policing Act	Act of 5 August 1992 on the police function
PVE	Potentially Violent Extremist
RD	Royal Decree
RD Classification and Security Clearances	Royal Decree of 24 March 2000 implementing the Act of 11 December 1998 and security clearances, certificates and advice
RD CUTA	Royal Decree of 28 November 2006 implementing the Act of 10 July 2006 on Threat Assessment
RD FTF	Royal Decree of 21 July 2016 on the common database of foreign terrorist fighters and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Policing
RD HP	Royal Decree of 23 April 2018 on the common database of Hate Propagandists and implementing certain provisions of section 1*bis* 'Information Management' of Chapter IV of the Policing Act
RD TF	Royal Decree of 23 April 2018 amending the Royal Decree of 21 July 2016 and redesigning the common database of foreign terrorist fighters as the common database of terrorist fighters

Review Act	Act of 18 July 1991 governing the review of police and intelligence services and of the Coordination Unit for Threat Assessment
SIGINT	Signals Intelligence
SIM	Special Intelligence Methods
SIM Act	Act of 4 February 2010 governing the intelligence collection methods used by the intelligence and security services
SIM Commission	Administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services
SIS	Secret Intelligence Service (MI6)
SIUN	*Statens inspektion av försvarunderättelse-verksamhet*
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*
SUN	*Statens uppfinnarnämnd*
TC	Terrorism Convict
TF	Terrorist Fighter
Threat Assessment Act	Act of 10 July 2006 on Threat Assessment

INTRODUCTION

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

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

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

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

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

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

---

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

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

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

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

Pursuant to Article 35 of the Review Act of 18 July 1991, the Standing Committee I annually draws up a general activity report. These activity reports are drawn up in Belgium's national languages Dutch and French and can be found on the website of the Committee (see www.comiteri.be). From 2006, with increased globalisation in mind, the Standing Committee I wished to meet the expectations of a broader public: the sections of the activity reports that were most relevant to the international intelligence community (the review investigations, the control of special and certain ordinary intelligence methods, the recommendations), have been translated into English. As a result, seven books have been published in English by the Standing Committee I (the *Activity Report 2006-2007,* the *Activity Report 2008-2009,* the *Activity Report 2010-2011,* the *Activity Report 2012-2013,* the *Activity Report 2014-2015,* the *Activity Report 2016,* the *Activity Report 2017* and the *Activity Report 2018* (see www.comiteri.be).

Given the new assignments that have been entrusted to the Standing Committee I, the Committee considered it useful to translate the entire report. Being all faced with similar challenges, the Committee felt that the new translated chapters were indeed likely to interest the international audience. The Activity Report 2018 was the first to be fully translated into English and was the first to be presented in a new format, followed by the Activity Report 2019. The reports are now only available in pdf format on the Committee's website.

Serge Lipszyc, Chairman
Pieter-Alexander De Brock, Counsellor
Thibaut Vandamme, Counsellor
Wauter Van Laethem, Acting registrar

25 April 2022

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

PREFACE 2020

The year 2020 began for the Standing Committee I with the organisation of an international symposium on the theme "Ten years of the SIM Act". The President of the Chamber, the Deputy Prime Minister and Minister of Justice, the UN Special Rapporteur, the Heads of the intelligence services and the Federal Prosecutor as well as the Bar Association, the press and representatives of civil society all spoke at the symposium. Their valuable contributions focused on the validity of the special intelligence methods used in Belgium. The speakers reflected on the importance of protecting both the State and individual freedoms. Our colleagues from the French and Swiss independent supervisory authorities also contributed to the discussion of this fragile balance.

A few weeks later, SARS-CoV-2 invited itself in our lives. Its spread around the world raised – and continues to raise – questions relating to protecting citizens and safeguarding individual rights and freedoms, but also gave renewed vigour to the scourge of "fake news" and attempts to destabilise our democracies.

Our society has been harmed by the impact this pandemic has had on people and institutions. Our daily lives were turned upside down.

To take just one aspect, working from home was compulsory for both public companies and the private sector during a long period. However, the security actors found this impossible to implement, in the case of both the two intelligence services and the Standing Committee I. No doubt this was partly inherent to the nature of the task and – to use the standard expression – because of the need to ensure continuity of service. However, the main reason why we were obliged to remain in our secure offices was the lack of a secure external communication and work system in Belgium.

Even in the 21st century, it is still impossible to work on a classified document or to communicate SECRET or TOP SECRET information securely from home or anywhere other than within the confines of our institutions. The persistent lack of investment by the State in this sovereign power ultimately suggests that the public authorities are indifferent to the world of intelligence.

Despite this, the Standing Committee I wishes to underline and feels some satisfaction in the fact that the activities of the two intelligence services and of the review body continued without fail throughout the pandemic, often in a manner that placed a strain on the scrupulous compliance with all public health rules. This last point is illustrated by the lack of any vaccination plan for these women and men in the shadows who continued working throughout this period.

Democratic oversight of these services was strengthened. The Committee presented to the Chamber of Representatives its methodology for continuous verification, ensuring that the intelligence services' intervention in the activities of political representatives was not subject to surveillance or control conducted outside the legal framework.

The rise of the far-right, in Europe and in many democracies, prompted us to analyse the intelligence services' response to this threat for the first time in their history.

Our work in this area also focused on relations between the two intelligence services and foreign partners. The Standing Committee I stressed in this connection that government oversight must remain the keystone of the intelligence services' international policy.

We were keen to improve the functioning of the administrative jurisdiction in terms of security clearances, certificates and advice, and therefore communicated to Parliament the text for a revision of this area. The objective is not only to make the jurisdiction the natural adjudicator in matters of security, but also to ensure easier access for those wishing to take legal action. A specific site has therefore been created for the Appeal Body (https://beroepsorgaan.be/index.php/en/).

Our daily work also includes processing complaints submitted by citizens. They receive a response, either from the Standing Committee I alone, or in consultation with the other competent bodies, namely the Standing Committee P, the Supervisory Body for Police Information (C.O.C.), the Data Protection Authority and the Federal Ombudsman. Citizens have to deal with an overwhelming multitude of institutions where data protection is concerned, and the Standing Committee I is calling for simplification in this area as part of the planned revision of the law.

The above, incidentally, merely offers a glimpse of the multifaceted activities that we carry out in our many different capacities: we are inspectors/auditors in the context of our investigations, we provide legal opinions in several areas at the parliamentary level, we listen carefully to the debate on the employment status of intelligence service personnel, we are reformers seeking changes in management practices within GISS, we initiate draft legislation, we author or co-author the various activity reports we are required to produce by law (e.g. in the context of BELPIU, the common databases, as data protection authority and the use of special intelligence methods), and we act as accountants for the special funds and as judges, with more than 200 decisions taken by the Appeal Body for security clearances, certificates and advice. And, as Aristotle noted, 'The whole is more than the sum of the parts'.

Given that these roles continue to expand, we believe that, at a time when the Chamber has launched a review of the synergies between certain institutions and on the status of their personnel, the questions regarding the budget allocated to the Standing Committee I and about its secure computer networks can no longer be avoided. We need to strengthen the Standing Committee I, and we need to act

fast. Our personnel are worried, and this can easily undermine morale in a way that would be most unwelcome in these troubled times. Administrative inertia in the broad sense, uncertainty about the future of our institution and the fragility of the Committee's position in law have prompted the resignation of one of the three members of the Committee, incidentally. However, it is not just the fate of our institution and our people but the future of democracy that is at stake.

Our political leaders have the very serious responsibility of providing the Standing Committee I with the means it needs to perform its legal roles. The Committee is the satellite monitoring system of our State: we can go to sea without it, of course, but if the vessel hits rough conditions, it alone will enable the rescuers to be directed to where they are needed.

The attacks in Zaventem and Brussels are the most obvious examples of this need to invest in the fight against various threats that are not just theoretical. We know today that no one is immune. Together with the intelligence services, the Standing Committee I participates in this daily fight against deadly forces such as terrorism, extremism, espionage, interference, proliferation, organised crime, sectarian organisations and cyberattacks.

Serge Lipszyc,
Chairman of the Standing Intelligence
Agencies Review Committee

28 June 2021

CHAPTER I.
REVIEW INVESTIGATIONS

In 2020, the Standing Committee I finalised eight review investigations, including one in conjunction with the Standing Police Monitoring Committee (Standing Committee P). These investigations are briefly presented below (I.1 to I.8). The investigation reports are available in full in French and Dutch on the Standing Committee I website. An extensive summary of each investigation is also included in the Activity Report 2020, available in French and Dutch on the Standing Committee I website.

Various bodies and people can refer a review investigation to the Standing Committee I: the Parliamentary Monitoring Committee, the competent ministers and any (legal) entity wishing to make a complaint or report. The Committee may also take the initiative of opening an investigation itself. This was the case for seven of the eight investigations finalised in 2020. Only one of these investigations was carried out at the request of the Parliamentary Monitoring Committee. The Committee also initiated seven new investigations in 2020. A brief description of the investigations still in progress at the end of 2020 follows in I.11. The recommendations made following the review investigations are set out in Chapter XII.

The Standing Committee I received a total of 62 complaints or reports in 2020.[1] After a brief preliminary investigation and after verifying some objective information, the Committee rejected 55 complaints or reports because they were manifestly unfounded (Article 34 of the Review Act), and in one case because the Committee did not have jurisdiction for the matter in question. In this latter case, the complainant was referred to the competent authorities (in this case, the Public Prosecutor of Brussels). Three of the six complaints that were processed were completed in 2020, and one was reclassified as a DPA complaint (see Chapter V).

Besides review investigations, the Standing Committee I opens 'information dossiers', the purpose of which is to provide a response to questions relating to the

[1] The admissibility of the complaint is first examined. It is then assigned to a category ('ordinary', DPA complaint, SIM complaint, etc.). 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).

operations of the intelligence services and CUTA.[2] If such dossiers reveal indications of dysfunction or of aspects of the intelligence services that require further examination, the Committee may open a formal review investigation. In 2020, among other topics, an information dossier was opened on the dysfunctionality (more specifically the inadequate flow of information) of government agencies and public services, i.e. the compartmentalisation that hinders efforts to protect citizens' safety. The development of a Crossroads Bank for Security was another subject of reflection. Three of these information dossiers (on coronavirus and the competence of the intelligence services, social dialogue within State Security and incidents that occurred in a foreign operations zone) were discussed with the Parliamentary Monitoring Committee and are described in this chapter.

I.1. SUPPORTING SERVICES OF CUTA

The Standing Committee I, together with the Standing Committee P, conducted a review investigation of the supporting services of the Coordination Unit for Threat Assessment (CUTA).[3] This investigation focused in particular on four supporting services: the FPS Interior (Immigration Office), the FPS Foreign Affairs, the FPS Mobility and Transport and the FPS Finances (Customs and Excises Administration). Its purpose was to examine the relationship between these supporting services and CUTA in terms of collaboration and exchange of information, with particular reference to legality, efficiency and coordination.[4]

The legal framework, which regulates the exchange of information between CUTA and its supporting services, imposes a duty on the latter to provide information to CUTA[5] and requires a central point of contact to be designated. It also stipulates that the CUTA consists in part of experts who are seconded from the supporting services. These experts, as liaison officers, are supposed to maintain

---

2 The Standing Committee I may open an information dossier for a wide variety of reasons: a complaint has been submitted and the Standing Committee I wishes to rule out the possibility that it is manifestly unfounded as quickly as possible; the management of an intelligence service reports an incident and the Committee wishes to check how the incident has been handled; the media reports an incident and the Committee wishes to know whether the reported facts correspond to reality and whether there is a more general underlying issue.

3 CUTA's primary role is to conduct terrorism and extremism threat assessments. For a more complete overview of its roles, see the Threat Assessment Act of 10 July 2006.

4 This investigation did not concern the intelligence services (State Security and GISS) or the police services (the Federal Police and the local police zones), since they had already been the subject of a joint review investigation (STANDING COMMITTEE I, *Activity Report 2011*, 25-33 (II.4. 'Information flows between CUTA and its supporting services'). The services that were added to the CUTA's list of supporting services in 2018 were likewise excluded from the investigation: the Standing Committees conducted a review investigation of them in 2021 (see I.11.9).

5 The supporting services are required to pass on to CUTA any information they have that is relevant to CUTA's assessment tasks. Failure to comply with this obligation is subject to criminal sanctions.

a link with their service of origin and facilitate the flow of information between it and CUTA. Moreover, the exchange of information between CUTA and its supporting services must be organised according to the level of classification of the information shared, with strict standards being applied regarding the retention, consultation, reproduction, transmission and destruction of classified information.

The Committees found that the four supporting services have a clearly identifiable main point of contact for CUTA. In terms of the volume of information exchanged, the Committees noted that the flow was very large with the Immigration Office and the FPS Foreign Affairs, and much limited with the FPS Mobility and Transport and the Customs and Excises Administration. The latter two organisations had a less well-established culture of information exchange and their personnel were less aware of the central point of contact with CUTA.

The investigation revealed room for improvement within the Customs and Excises Administration in terms of compliance with minimum security standards for the retention of classified documents.

Concerning the exchange of information within CUTA itself, the Committees found that the communication between the various departments could be improved, in particular internal communication relating to the competencies of experts could be increased.

I.2. OPERATIONS OF THE COUNTERINTELLIGENCE (CI) DIRECTORATE OF GISS: FOLLOW-UP ON RECOMMENDATIONS (2ND PART)

At the end of December 2016, the then Minister of Defence asked the Standing Committee I to conduct an investigation into how the Counterintelligence (CI) Directorate within GISS operates. This investigation revealed the seriousness, complexity and diversity of the functional problems within the CI Directorate. Following the investigation, detailed recommendations were made by the Standing Committee I.[6] After a first follow-up investigation, the Committee conducted a second follow-up investigation in 2020 to check on progress with the implementation of these recommendations.

During this second follow-up investigation, the Standing Committee I found that GISS had made significant efforts to correct the many problems identified in the former CI Directorate in 2018 and to develop the counterintelligence mission more effectively. However, a number of points remained in need of attention, including the backlog in inputting information into the database and the strengthening of

6 STANDING COMMITTEE I, *Activity Report 2018*, 2-12 (I.1 Operations of the Counterintelligence (CI) Directorate of GISS, and 128-132 (XII.2.1. Various recommendations for GISS arising from the review investigation into how the Counterintelligence Directorate operates).

internal controls. The Committee therefore decided to continue to closely monitor the implementation of its recommendations.

I.3. BREXIT AND THE RELATIONSHIP BETWEEN THE BELGIAN AND BRITISH INTELLIGENCE SERVICES

In May 2019, the Standing Committee I opened a review investigation into the impact of Brexit on the cooperation between the Belgian intelligence services (State Security and GISS) and the British intelligence services. In particular, the Committee wanted to check whether Brexit was likely to jeopardise this cooperation. It also wished to know how the Belgian intelligence services had prepared for Brexit.[7]

The Committee found during the investigation that bilateral cooperation and multilateral cooperation between the Belgian and British intelligence services lay outside the European structures, as the operation of the intelligence services is a matter for the exclusive competence of the Member States.

State Security cooperated bilaterally with two of the three British civilian intelligence services, namely the Security Service (BSS or MI5) and the Secret Intelligence Service (SIS or MI6). The Security Service collects and analyses intelligence relating to domestic threats, while the Secret Intelligence Service collects intelligence abroad. Cooperation with these two British intelligence services focused on the competences that the three services have in common, namely terrorism, espionage and the proliferation of weapons of mass destruction. There was no direct cooperation between State Security and the third British intelligence service, Government Communications Headquarters (GCHQ), which is responsible for signals intelligence (SIGINT). State Security also did not cooperate with the British military intelligence service. GISS cooperated bilaterally with the SIS (MI6), the BSS (MI5) and GCHQ, which was regarded by the service as the most important British partner. The services worked in particular on sharing expertise in SIGINT, on the fight against cyberthreats, and on the exchange of intelligence on the threat (of espionage). Although the United Kingdom also has a military intelligence service (Defence Intelligence), whose mission is to provide strategic military intelligence to the Ministry of Defence and the armed forces, GISS stated during the investigation that it had not established any direct bilateral cooperation with Defence Intelligence.

---

7 At the time the review investigation was carried out (October – November 2019), there was still no certainty about the timing or the precise circumstances of the withdrawal, due to the conflicting and uncertain political situation in the UK. The report was finalised in the first quarter of 2020.

Besides the bilateral contacts, contact also took place and intelligence was exchanged between the Belgian and British intelligence services via multilateral forums, which are independent of the structures of the European Union.

The review investigation revealed that the Belgian intelligence services had not been invited to participate in any consultation with the Belgian authorities on the potential impact of Brexit. The services had not received any questions, instructions or directives in this regard. The two services had also not drawn up a formal and structured analysis (including a risk assessment) of the possible repercussions of Brexit on their cooperation with the British services. After the launch of the investigation, however, the two services reflected on this matter and felt that the impact would be limited, since cooperation takes place directly between the two states and outside the structures of the EU. The Standing Committee I closed the investigation, concluding that it had found no evidence that the withdrawal of the United Kingdom from the EU would have a negative impact on the Belgian and British intelligence services. The identical conclusion was drawn across the Channel.

I.4. POSSIBLE INTERFERENCE BY FOREIGN SERVICES/STATES IN THE BELGIAN ELECTORAL PROCESS

Although the results of the investigation conducted on this matter in the United States have not been fully made public, there were strong indications that foreign services/states (in particular Russia) used cyber-resources to attempt to influence the 2016 US presidential elections. Such a scenario is also possible in Europe, and therefore in Belgium.

Online influencing of elections from abroad can take various forms. It may involve hacking, infiltration and manipulation of electoral technology through access to voting computers; the infiltration of computer systems to obtain information on party strategies or sensitive information and to organise leaks in the press or on social media; or the online dissemination of fake news and disinformation via social media platforms and media company websites.

The May 2019 elections[8] made this issue highly topical. The organisation of open, fair elections lies at the heart of democracy. State Security is responsible for identifying threats against Belgian institutions and informing the competent authorities. The Committee therefore decided, at the beginning of 2019, to open a review investigation into the Belgian intelligence services' response (intelligence gathering, warnings, international cooperation, potential obstacles, etc.) to signs of interference by foreign services or states in the Belgian electoral process.

[8] The elections in question were those of 26 May 2019 for the European Parliament, the Belgian Chamber of Representatives and the Parliaments of the Regions and the Communities.

At the end of the investigation, the Standing Committee I concluded that the two intelligence services had taken the necessary measures to counter potential threats to the Belgian and European elections of May 2019. The services:

- had acknowledged and assimilated the issue;
- had examined and identified the risks and threats;
- had taken the necessary organisational actions internally;
- had developed the necessary cooperation between themselves and with other actors;
- had raised awareness and informed the Government and other interested parties so that they could take appropriate measures if necessary.

According to the services, the large-scale interference that had been feared did not take place, although it had been observed that disinformation tactics were increasingly sophisticated.

I.5. THE MEMORANDUM OF UNDERSTANDING (MOU) BETWEEN GISS AND THE RWANDAN INTELLIGENCE SERVICES

The Standing Committee I conducted an investigation into the scope of the MoU concluded between GISS and the Rwandan intelligence services in October 2016 in particular, and more generally into the conclusion of partnerships between a Belgian intelligence service and foreign partners. The Belgian intelligence services must continue to collaborate with foreign services, both at bilateral and multilateral level. However, given its undeniably political nature, such collaboration must be fully transparent and fully traceable, what the Committee wished to investigate.

In September 2016, the Ministers of Justice and Defence submitted a directive classified as 'confidential' to the National Security Council concerning the relations of the Belgian intelligence services with foreign intelligence services. The directive describes the mechanisms that State Security and GISS must comply with. It specifies the manner of objectifying and structuring choices of foreign partners, the need to determine the scope of partnerships and, finally, the obligation to evaluate them regularly.[9]

The analysed MoU was signed by General Testelmans, Head of GISS at the time, and the Secretary General of the Rwandan intelligence service (NISS). The purpose of the unclassified document was: 'to regulate the terms and conditions of exchange of national classified information, to define areas of bilateral cooperation in the field of intelligence and to formalize the procedure regarding the meetings

[9] However, the directive does not unequivocally specify whether or not State Security and GISS must obtain prior ministerial approval or the approval of another authority. The Committee had already repeatedly expressed the need for political cover in this regard.

between the two Participants'. In this document, three areas of partnership are addressed, but what form the partnership should take in practice is not specified.

After analysis, the Committee concluded that GISS had not complied with the ministerial directive in the context of its partnership with the Rwandan service, either during the conclusion of the agreement or in the context of its implementation. The Committee noted:

- that the assessment of the partner was conducted late (two years after signing the MoU);
- that the assessment was undated, excessively brief and inadequately documented;
- that the assessment criteria prescribed by the Directive were applied inconsistently;
- the lack of incident notification;
- the lack of a biannual assessment.

I.6. INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE INTELLIGENCE PROCESS AT GISS

In May 2019, the Standing Committee I initiated a 'review investigation of the IT resources used by the Belgian intelligence services for the collection, processing, analysis and communication of information within the intelligence cycle'. The investigation focused on the IT resources specifically used to support elements of the intelligence cycle: for example, the systems used to collect information, the tools used for analysis and specific databases.[10]

The first part of the investigation focused on GISS, due to the impact of its restructuring in terms of IT tools and working methods.[11] The investigation sought to identify the risks[12] facing GISS and to give recommendations on how to reduce them. The 'CIA' model[13] was applied.

---

10 The Standing Committee I did not look at the generic/standard office tools used by the services (e.g. Windows, Word, Excel, etc.). The Committee also did not examine in detail the hardware available to the services, unless this was specific to the intelligence service concerned.

11 With regard to GISS, the investigation ended in May 2020, except for a specific section concerning the GISS Cyber Directorate, which ended in 2021. The section of the investigation relating to Security Service - IT continued in 2020-2021.

12 A risk has been defined as the possibility of the existence of a weakness or a more or less foreseeable threat that could affect the achievement or the efficient accomplishment of an organisation's objectives, combined with the probability that a harmful event will occur as a result of this weakness.

13 The use of the CIA model is recommended as a basis for risk assessment according to the ISO 270 international standards for information security. The model distinguishes between three types of risk: Confidentiality, Integrity and Availability.

During the investigation, the Committee identified certain risks, their likelihood and possible ways of mitigating them. An overview of the problems observed was given to GISS. Among the most significant risks incurred by the service, attention focused on:

- the speed of the network, given its importance for all applications and therefore for the proper performance of the service's roles;
- the monitoring of the network, and of the entire digital infrastructure, with a view to the proactive detection of warning signs of breakdowns or slowdowns;
- the logging of activities in order to protect against abuse, but also in order to be able to provide legal evidence concerning users' activities;
- the management of the active directory in order to limit the possibility of 'privilege creep'[14];
- change management, so that every change (update, new installation) takes place according to a strict procedure, including a method for returning to the previous situation.

Finally, the question of the lack of IT personnel was raised, as this was something that needed to be addressed urgently.

I.7. MONITORING OF THE FAR-RIGHT BY THE BELGIAN INTELLIGENCE SERVICES

Given the increase in the number of terrorist incidents around the world linked to individuals with extremist ideas, the rise of identity movements and the controversial report on '*Schild & Vrienden*'[15], the Standing Committee I decided to investigate the monitoring and reporting by intelligence services of the threat from the far-right in Belgium. The Committee wanted to examine whether and how the intelligence services perform their legal role of monitoring extremism, and more specifically right-wing extremism in Belgium.

The Committee noted in its report that the terminology used between CUTA, Security Service and GISS was inconsistent. Various concepts (such as 'far-right' and 'right-wing extremism') were used indiscriminately, without always referring to the same content.[16]

With regard to threat assessment, the Committee noted a clear absence of quantitative data on the extent of the threat from the far-right in Belgium. The

---

14 This term refers to the accumulation of access rights whenever a person changes position, without the old accesses being deleted.

15 https://www.vrt.be/vrtnws/nl/2018/09/05/pano-wie-is-schild-vrienden-echt/

16 These concepts have not been defined legally (contrary to 'extremism', for example) or politically (in guidelines from the National Security Council or the relevant ministers).

actual extent and development of the phenomenon were therefore difficult to assess, which made it hard to define the resources needed to monitor it.

As for the resources deployed within the services, concerning State Security, the Standing Committee I found that after a setback during the terrorist crisis of 2015-2016, the service had redoubled its efforts to monitor ideological extremism, including the far- right. Personnel had been assigned and tactical and operational objectives had been defined. Without a clear description of the threat and its scale however, it was hard to determine whether the resources were commensurate with the objective. The Standing Committee I also found that State Security was performing analyses, but that these mainly focused on detecting possible threats of violence from far-right circles. General phenomenon analyses, giving rise to hypotheses, scenarios and 'predictive information', were therefore rare. Nevertheless, the Committee felt that this should be a core mission of an intelligence service.

Concerning GISS, after its restructuring in early 2020 a new mixed platform was created to monitor (right-wing) extremism within the Armed Forces. Personnel were deployed and objectives set. However, there were signs that the support provided was insufficient. The Committee also noted that GISS' information position was limited and that no phenomenon analysis of the far-right in the Armed Forces had been performed.

The Standing Committee I concluded that close cooperation was necessary between State Security and GISS with regard to the threat of right-wing extremism, that regular consultation should be organised and that information should be exchanged on the issue.

I.8. THE CORONAVIRUS AND THE QUESTION OF THE COMPETENCE OF THE BELGIAN INTELLIGENCE SERVICES

International reports showed that the roles assigned to the various intelligence services in the fight against the coronavirus varied greatly from country to country. The media also revealed that in some countries the intelligence community had been warning about the threat of a pandemic for years. Based on these findings, the Committee examined the role and competence of the Belgian intelligence services in the fight against the coronavirus.

In its report, the Committee demonstrated that neither State Security nor GISS have legal powers to actively detect and combat medical risks that could constitute a threat to public health. They have no competence in disease prevention and control, and medical intelligence is not among the missions of either service.

Despite this, the two intelligence services have a role to play in the management of certain consequences of public health risks when those consequences fall within the services' area of competence, such as the rise of extremism, interference, etc.

The joint publication by State Security and GISS of the brochure entitled '*Le danger caché derrière le COVID-19*' (The hidden danger behind COVID-19) on 21 April 2020 is an example of this.[17] The publication focuses on right- and left-wing extremism, potential interference through pro-Russian reports and disinformation campaigns by foreign powers, as well as matters concerning the economic and scientific potential. The brochure showed that the two services had fulfilled their role conscientiously and proactively. It also showed that the law is sufficiently clear on this point and does not require adjustment.

If the Belgian intelligence services had obtained serious evidence that coronavirus was or had been used as a biological weapon, its spread would then have been regarded as an intentional act, making the Belgian intelligence services fully competent.

I.9. SOCIAL DIALOGUE WITHIN STATE SECURITY

The Standing Committee I was consulted about the revision of the employment status of State Security personnel. State Security is made up of personnel from internal and external services. In the past, each of these services had a separate status. The government submitted to the social partners a plan to converge the personnel status applicable within State Security and, in particular, to partially merge the personnel of the internal services into the administrative and financial status applicable to the personnel of the external services. This represented a first step within a more general reform of State Security and in line with the creation of a "single status", as recommended by the Parliamentary Inquiry Committee on 'Terrorist Attacks'.

However, the trade union representatives did not support this proposal and informed the Parliamentary Monitoring Committee and the Standing Committee I as such.

In accordance with the act governing its functioning, the Committee continued to pay attention to this dossier, as an employment dispute would affect the efficient functioning of State Security. The Committee felt that it was not competent with regard to social disputes, and that any disagreement should be settled within the negotiation and consultation committees and, if necessary, before the employment mediator. However, a meeting was held between the Standing Committee I and two representatives of a trade union organisation in August 2020.[18]

The Royal Decree of 24 September 2020 amending the Royal Decree of 13 December 2006 on the status of State Security external service personnel was

---

17 The brochure can be viewed on the State Security website: https://vsse.be/fr/le-danger-cache-derriere-le-covid-19.

18 The Director-General of State Security was informed of this meeting, with the consent of the trade union.

published in the Belgian Official Journal on 1 October 2020 and entered into force on 1 January 2021.

I.10. INCIDENTS IN A FOREIGN OPERATIONS ZONE

The provision of intelligence on the political and military situation in other parts of the world is an important part of the work of GISS.[19] In 2018, the Committee looked into the deployment of GISS in a specific operations zone.[20] GISS provides support to the Belgian military commanders on the ground . The service also carries out support duties for Belgian embassies and helps ensure the safety of expatriates. During the investigation, the Committee identified several vulnerabilities that presented potential security risks to operations or military personnel.

Subsequently, the Committee again received information about a series of serious incidents that represented a security risk. A classified report was sent to the Head of GISS, with the CHOD and the Minister of Defence copied in, in which GISS was called on to take urgent measures to protect the deployed forces.

The Committee deplored the fact that the security incidents had merely led to a procedure for the withdrawal of a security clearance and that the service had not initiated any disciplinary procedure whatsoever. In addition, the Committee was forced to conclude that when GISS was confronted with an offence or a crime committed by its personnel, Article 29 BCCP was not applied and no report was made to the judicial authorities. Finally, the need for a comprehensive report to be prepared by GISS in the event of a security incident was once again brought to its attention.

I.11. REVIEW INVESTIGATIONS FOR WHICH THE INVESTIGATIVE STEPS WERE TAKEN IN 2020 AND INVESTIGATIONS OPENED IN 2020

I.11.1. THE APPLICATION OF NEW INTELLIGENCE METHODS, INCLUDING SPECIAL INTELLIGENCE METHODS

In 2010, the possibilities for intelligence-gathering by GISS and State Security were considerably extended. Since then, the services have been able to use ordinary, specific and exceptional methods – a classification intended to reflect the degree

19 For security reasons, the location has not been mentioned.

20 STANDING COMMITTEE I, *Activity Report 2018* (I.2. 'The activities of GISS in a foreign operations zone') and (IX.2.8. 'Un rapport circonstancié en cas d'incident de sécurité' ('A detailed report on a security incident').

of intrusiveness of the different measures.[21] The changes to the law that have taken place in the meantime have expanded the scope of several methods. As a result, some "special" methods have become "ordinary" and a number of new ordinary methods have been added.

The Committee has therefore been given a range of monitoring responsibilities with regard to certain "ordinary" methods, although this oversight is regulated in a different way for practically every method. The monitoring includes in particular checking the identity of the regular telecommunications user (Art. 16/2 of the Intelligence Services Act), the access to PNR data (Art. 16/3 of the Intelligence Services Act), the access to the images from cameras used by the police services (Art. 16/4 of the Intelligence Services Act), as well as the monitoring prior to interceptions, intrusions or recordings (Art. 44/3 of the Intelligence Services Act).

I.11.2. INFORMATION AND COMMUNICATION TECHNOLOGIES IN THE INTELLIGENCE PROCESS AT STATE SECURITY

As described above[22], the Standing Committee I initiated a 'Review investigation of the IT resources used by the Belgian intelligence services for the collection, processing, analysis and communication of information within the intelligence cycle'. The results of the investigation concerning GISS were finalised in 2020 (see I.6.). The section of the investigation relating to Security Service continued in 2020-2021, as did the section concerning GISS Cyber Directorate, for which, in view of its distinctive characteristics, a separate investigation report was drawn up.

I.11.3 MONITORING BY THE INTELLIGENCE SERVICES OF CURRENT AND FORMER PRISONERS CONVICTED FOR TERRORISM OR IDENTIFIED AS RADICALISED

Between 2015 and 2020, the Belgian courts handed down a total of 464 convictions for offences relating to terrorist activities.[23] Some of the individuals concerned were convicted *in absentia* and therefore could not be imprisoned. Others have obtained a temporary release from prison, have now served their prison sentence or have

---

21 The Committee organised a symposium at the Chamber to mark the tenth anniversary of the "SIM Act" (see below). On this subject see: J. VANDERBORGHT, (ed.), *Les méthodes particulières de renseignement : de l'ombre à la lumière*, Antwerp, Intersentia, 2020, 70 ff.

22 See I.6. 'Information and communication technologies in the intelligence process at GISS'.

23 M. VANDERSMISSEN, *Knack*, 19 January 2021 ('Belgische rechtbanken veroordeelden de voorbije vijf jaar 464 terroristen'). In addition to the nearly 500 individuals convicted, there are 200 jihadists who were or still are in Syria and Iraq. The exact number of these individuals who are still alive is unknown.

been released on parole (before the end of their sentence) following a decision by the Sentence Enforcement Court.

Given the potential danger of recidivism, the Committee decided in mid-2019 to open a review investigation into 'The monitoring by the Belgian intelligence and security services, first, of those charged in Belgium for terrorist offences committed in Belgium or elsewhere and benefiting from an arrangement under the Act of 20 July 1990, and second, of those convicted in Belgium for terrorist offences who leave Belgian prisons, either under one of the arrangements referred to in the Act of 17 May 2006, or after being permanently released (Art. 71 of the Act)'.

The Committee examined the way in which the two intelligence services monitor these individuals, what resources and methods are used, how cooperation with partners takes place and within what structures. Finally, through benchmarking, the French and British approaches were analysed. The investigation continued in 2021.

I.11.4. THE RISK OF INFILTRATION WITHIN THE TWO INTELLIGENCE SERVICES

The international world of intelligence has been shaken in recent years by a series of cases of infiltration (and "insider threat"). In 2019, the Committee took the initiative of launching a review investigation into how the two intelligence services manage the risk of infiltration: what risks have been identified? What measures have been taken to control them and to react if these risks materialise?

I.11.5. POSSIBLE THREATS TO ECONOMIC AND SCIENTIFIC POTENTIAL (PRISM/PES): FOLLOW-UP INVESTIGATION

In 2016, a review investigation relating to the protection of the economic and scientific potential was finalised in the wake of the Snowden revelations about, among other things, the PRISM programme through which the NSA collected telecommunications data and metadata. Intelligence operations conducted by both the American and the British services against different international institutions and cooperation structures (UN, EU and G20) were also revealed; with "friendly" countries being targeted. The Committee's investigation focused on the possible implications of foreign programmes for the protection of the country's economic and scientific potential. The goal was to investigate whether the Belgian intelligence services were attentive to this phenomenon; whether they had detected a real or potential threat to the Belgian economic and scientific potential; whether they had informed the competent authorities and suggested protective measures to them; and finally, whether they had sufficient and appropriate resources to monitor this

issue. The Committee also examined the effects of the PRISM programme and/or similar systems on the economic and scientific potential of the country.

At the end of November 2019, the Parliamentary Monitoring Committee asked the Standing Committee I to resume and update the review investigation.

I.11.6. ESPIONAGE VIA ENCRYPTION EQUIPMENT: OPERATION BUBICON

In mid-February 2020, revelations were made about Operation Rubicon, in which American and German intelligence services listened for decades to the encrypted communications of the authorities in dozens of countries, using the Swiss company Crypto AG as a cover. The Netherlands, France, Sweden and Denmark (the "Maximator countries") were among the *cognoscenti*, i.e. countries that had been informed of the cryptological details of certain devices. Belgium, which 'was invaluable for the clarifications that its reports provided on diplomatic events' (free translation) and above all of interest as a diplomatic centre for NATO and the then European Economic Community, was said to have been targeted.

The Committee opened a review investigation in an attempt to answering several questions arising from this affair: to what extent were the Belgian intelligence services aware (or to what extent should they have been aware) of these operations in view of their statutory roles? Was intelligence collected on these operations, or was this not considered desirable? And more importantly: do the services offer sufficient protection in this respect now? Have risk assessments been carried out? Where the use of encryption equipment was found, what precautionary measures were taken? How is this encryption problem managed today?

I.11.7. OFFENSIVE INTELLIGENCE RESOURCES FOR THE INTELLIGENCE SERVICES?

Given the intelligence mission described by the law, information relevant to the intelligence services can be found both in Belgium and abroad. A review investigation was therefore opened in 2019 on the (additional) offensive intelligence resources potentially required by the Belgian intelligence services. This investigation has several objectives:

- To check whether State Security and GISS currently engage in operational intelligence-gathering abroad, and if so, in what form and through what intelligence activities;
- To examine the activities carried out abroad in light of the current regulatory framework;

- To check whether the services need additional resources, including legal resources (in other words, investigative powers) to be able to collect intelligence abroad.

I.11.8. CUTA AND THE SUPPORTING SERVICES (FOLLOW-UP)

In June 2020, the Standing Committee I, together with the Standing Committee P, conducted a review investigation of the supporting services of the Coordination Unit for Threat Assessment (CUTA). This investigation focused on four supporting services: the FPS Interior (Immigration Office), the FPS Foreign Affairs, the FPS Mobility and Transport and the FPS Finances (Customs and Excise).[24]

In order to be able to answer the questions asked by the Parliamentary Monitoring Committee concerning progress in the implementation of the recommendations made in the context of this investigation, the Standing Committees I and P opened a follow-up investigation in early June 2020.

I.11.9. CUTA AND "ADDITIONAL" SUPPORTING SERVICES

As mentioned above, CUTA is able to make use of various supporting services. The Royal Decree of 17 August 2018 extended the list of CUTA's supporting services to four other services, namely the Governmental Coordination and Crisis Centre, the General Administration of the Treasury, the Directorate-General of Penal Institutions and the Department of Worships and Secularism of the Directorate-General of Legislation and Fundamental Freedoms and Rights of FPS Justice. Although this decision dates back to August 2018, the investigation of the CUTA's supporting services did not cover these new services, as it was too early to perform an analysis of the flow of information and processes implemented in this context. A new review investigation, carried out jointly with the Standing Committee P, was necessary.

I.11.10. THE EXCHANGE OF INFORMATION ABOUT AN EMPLOYEE BETWEEN THE INTELLIGENCE SERVICES AND A PRIVATE- OR PUBLIC-SECTOR EMPLOYER

In August 2019, the Standing Committee I received a complaint from an employee of a public institution. They complained that their employer had requested

[24] See I.1. 'Supporting services of CUTA'.

information about them from an intelligence service and intended to take disciplinary action on this basis.

The Committee began its processing of the complaint by carrying out a legal analysis of the more general question of the circumstances and conditions under which a private or public organisation can address a request about an employee (or a job candidate) to one of the two intelligence services. The Committee also considered in what circumstances the intelligence service concerned can or must respond to such a request, and what requirements this response must meet.

I.11.11. MONITORING OF SPECIAL FUNDS: FOLLOW-UP INVESTIGATION

Like any public service, the intelligence services are allocated public funds for the performance of their statutory missions. The normal rule for the use of these funds is complete transparency and total control. However, as some missions of State Security and GISS are unpredictable or must be kept secret, part of their budget falls outside this normal rule. This part is better known as "special funds". Although the amount of these funds is included in the budget allocated to the services, special rules apply to their management, use and control. In 2015, the Committee focused in particular on determining the nature of these special funds, their amount and their distribution. It also investigated the use of resources and the interactions between these special funds and the normal budgets. Finally, the Committee looked at the regulatory framework and examined the control mechanisms, both internally (within the services) and externally (the Court of Audit, the Finance Inspectorate, the Standing Committee I, etc.). Various recommendations were made.

Since 2018 (State Security) and 2020 (GISS), the Court of Audit has expressed its intention of conducting a periodic audit of these funds. In this context, the Court of Audit has been able to use technical assistance offered by the Standing Committee I. The Committee in turn has been able to '*perform its role with more attention to the use of these funds*'. A follow-up investigation was opened in 2020 on the management, use and control of special funds.

I.11.12. INVESTIGATION ON THE MONITORING OF POLITICAL REPRESENTATIVES

The question has frequently been raised during parliamentary debates whether and to what extent the Belgian intelligence services monitor (or are allowed to monitor) political representatives, and what rules have to be observed in this respect. Since the beginning of January 2018, a new memorandum classified as "confidential",

has been applicable within State Security. This service sends two types of reports to the Minister of Justice and the Prime Minister, with a copy to the Standing Committee I: occasional reports on political representatives who contribute to the emergence of a threat and a quarterly overview of all documents in which political representatives are mentioned.[25] The Minister of Justice previously agreed to the 'principle of verifications by the Committee I which prove to be necessary under the terms of the Act of 18 July 1991'.

Without any guidelines on what it is expected to do with the aforementioned information, the Standing Committee I took the initiative of developing a methodology relating to the 'issue of the monitoring of political representatives by the intelligence services and the role of the Standing Committee I'. This methodology was approved by the Parliamentary Monitoring Committee in 2020. Based on this methodology, a (periodic) review investigation was initiated in 2020.

[25] The political representatives concerned are the ministers of the various governments, the Belgian Commissioner at the European Commission and the members of the various parliaments and assemblies, including Belgian members of the European Parliament. Other elected officials or appointed representatives are not involved (e.g. aldermen and -women at municipal level or governors at provincial level).

CHAPTER II.

CONTROL OF SPECIAL AND CERTAIN ORDINARY INTELLIGENCE METHODS

The year 2020 marked the tenth anniversary of the Act of 4 February 2010 governing the intelligence collection methods used by the intelligence and security services (SIM Act[73]). This event was worthy of celebration. On 31 January 2020, the Committee therefore held a symposium entitled "Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière" (Special intelligence methods: from shadow to light) under the auspices of the Chamber of Representatives.

The entry into force of this law, which was profoundly modified by the Act of 30 March 2017[74] (the "SIM Update Act"), considerably expanded the possibilities for intelligence-gathering by the two intelligence services.

When the legislators finally decided in 2010 to give the intelligence services new powers, a significant task was entrusted to the Standing Committee I at the same time. Together with the SIM Commission, the Committee was to monitor the use of these data collection methods, which by definition intrude greatly on individual rights and freedoms. Article 35 of the Review Act requires the Committee to maintain transparency in the activities it performs in this context.

This chapter therefore includes detailed figures on the use by State Security and GISS of specific and exceptional methods (grouped together as "special intelligence methods") and certain ordinary methods for which the Committee has been given an additional oversight role. In addition, it reports on the way in which the Committee carries out its judicial oversight role with regard to these methods (by presenting the number of decisions and the way in which requests were submitted to the Committee). For details on the case law relating to the Standing Committee I, see the Activity Report 2020 available in French and Dutch on the Committee's website.

---

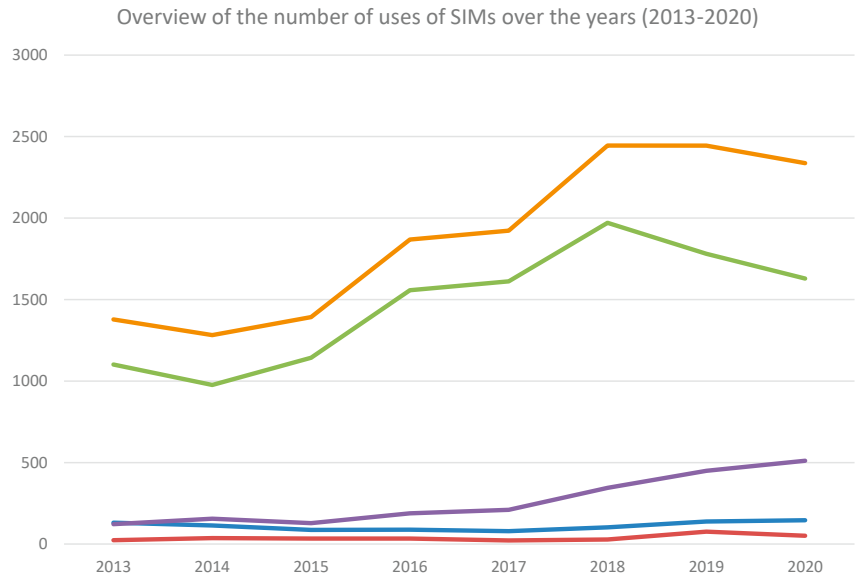
73 *Belgian Official Journal*, 10 March 2010.

74 *Belgian Official Journal*, 28 April 2017.

II.1. FIGURES ON SPECIAL METHODS AND CERTAIN ORDINARY METHODS

Between 1 January and 31 December 2020, a combined total of 2337 authorisations were granted by the two intelligence services for the use of special intelligence methods: 2140 by State Security (1629 for specific methods and 511 for exceptional methods) and 197 by GISS (146 for specific methods and 51 for exceptional methods). According to the officials responsible for data collection methods at State Security and GISS, the COVID pandemic had no impact on the number of special intelligence methods used.

The graph below provides a comparison with the figures of previous years.



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

The number of SIMs used increased steadily in recent years until it reached a plateau in 2019; in 2020 a negligible decrease can be noticed for the first time, with the total number of uses of these methods remaining more or less stable. However, it should be noted that the same authorisation may cover several targets (people, organisations, places, objects, means of communication, etc.).

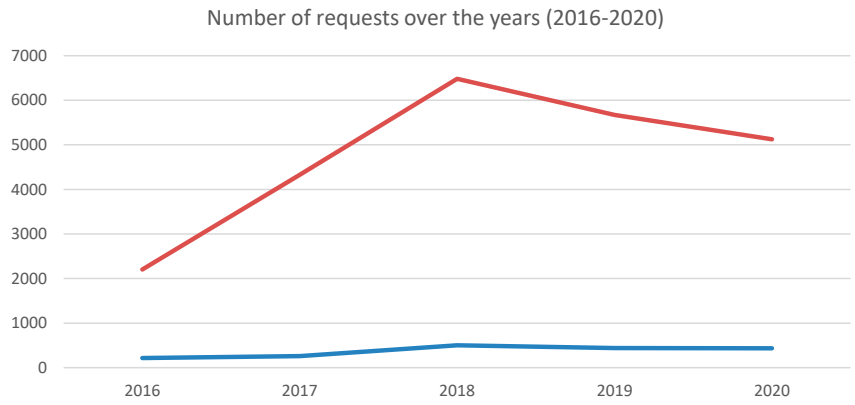
State Security is responsible for by far the largest share (91.5%) of the methods used.

A breakdown of the figures shows that the use of specific methods by GISS continued to increase, from 138 to 146 instances. However, the number of exceptional methods used dropped by around a third, from 76 to 51.[75]

At State Security, the opposite trend is observed, namely a striking decrease in the use of specific methods (from 1781 in 2019 to 1629 in 2020) and a further significant increase in the use of exceptional methods (from 449 in 2019 to 511 in 2020, an increase of around 14%). The Committee confines itself here to presenting raw statistics.

There was a further decrease (of about 10%) in the use of ordinary methods involving requests made to telecom operators and providers in order to identify certain means of communication (cf. Art. 16/2 of the Intelligence Services Act). About 10 fewer requests were made by GISS than in 2019, compared to over 550 fewer requests made by State Security.

The graph below shows the changing number of requests over the years:



The blue line refers to the requests made by GISS, whereas the red line refers to the requests made by State Security.

The Committee stated that '[it could] not ignore the finding that the number of identifications has increased considerably since the introduction of the streamlined procedure under Article 16/2 of the Intelligence Services Act'.[76] The number of requests continued to fall in 2020, but remains quite high.

75 It is important to note in this context that GISS also has specific powers for intelligence-gathering, as regulated in Articles 44 ff. of the Intelligence Services Act. On this matter, see Chapter III. Monitoring of foreign interceptions, image recordings and IT intrusions.

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

II.1.1. METHODS USED BY GISS

II.1.1.1. Ordinary "plus" methods

Identification of a telecommunicationuser

Identifying a telecommunication subscriber/ user (e.g. a mobile phone number or IP address) or a used means of communication is regarded as an ordinary method if it happens through a request to the telecom operators and providers or through a direct access to the customer database.[77] The regulation requires the intelligence services to keep a register of all requested identifications and all identifications made through direct access.[78] Under these regulations, the Committee must receive a monthly list of the requested identifications and of each instance of access. In 2020, GISS recorded a slight decrease in the number of requests, from 442 in 2019 to 433. This topic was also the subject of a review investigation opened in 2019 (see above).

Access to PNR data

In early 2017,[79] the possibility for the intelligence services of accessing the information held by the Passenger Information Unit by means of targeted searches was introduced (Art. 16/3 of the Intelligence Services Act and Art. 27 of the PNR Act of 25 December 2016). The Committee is informed of the use of this method and can prohibit it, where appropriate.[80]
The PNR rules also allow a so-called "prior assessment" to be carried out in which the entered PNR data is automatically checked against the intelligence services' lists of names or databases and in which information based on validated hits is forwarded (Article 24 of the PNR Act). The number of searches performed on PNR data fell from 38 in 2019 to 28 in 2020.

---

77 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).

78 The possibility for the intelligence services to request such identification data through direct access to the customer database of telecommunications operators and providers, created by Article 16/2, § 1, last paragraph of the Intelligence Services Act, has not been used so far.

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

80 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.

Use of police camera images

The Act of 21 March 2018 (*Belgian Official* , 16 April 2018) amended the Act of 30 November 1998 governing the intelligence and security services to allow the intelligence services to use police camera images. A new ordinary method was introduced for this purpose (Art. 16/4 § 2 of the Intelligence Services Act).[81] [82]

Figures

Ordinary methods (GISS)	Number of authorisations
Identification of a telecommunication user	433
Targeted PNR data searches	28
Referral of PNR data on basis of hits	Not disclosed
Use of police camera images	Not in force[83]

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)[84]	6
Searching 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

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

82 At the beginning of 2019, the Council of Ministers approved a draft Royal Decree implementing Art. 16 § 4 of the Intelligence Services Act, which was submitted to the Standing Committee I for an opinion. This opinion 002/CPR-ACC/2019 of 9 April 2019 can be consulted on the Committee's website (www.comiteri.be).

83 The scope of application of Article 16/4 of the Intelligence Services Act (for example with regard to consultations of the Directorate of Police Information and ICT Resources (DRI) of the Federal Police) is the subject of a legal analysis by the Standing Committee I (2021).

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

Specific methods (GISS)	Number of authorisations
Requesting transport and travel information from private transport and travel services (Art. 18/6/1 of the Intelligence Services Act)	2
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 (Art. 18/7 § 1, 1 of the Intelligence Services Act)	2
Requesting the assistance of the operator of an electronic communications network to obtain payment method data and identify the payment method and time of payment for the subscription to or use of the electronic communications service (Art. 18/7 § 1, 2 of the Intelligence Services Act)	0
Tracing call-associated data of electronic means of communication and requesting the cooperation of an operator (Art. 18/8 § 1, 1 of the Intelligence Services Act)	69
Monitoring localisation data for electronic communications and requesting the cooperation of an operator (Art. 18/8 § 1, 2 of the Intelligence Services Act)	67
TOTAL	**146**

In terms of the execution of specific methods, the tracing of call-associated data of electronic means of communication (Art. 18/8 of the Intelligence Services Act) and obtaining localisation data (Art. 18/8 of the Intelligence Services Act), both accompanied by a request for the cooperation of an operator in each case, are easily top of the ranking (136 of the 146 used specific methods). Instances of searching places accessible to the public using technical means halved, from 12 in 2019 to 6 in 2020.

II.1.1.3. Exceptional methods

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

Exceptional methods (GISS)	Number of authorisations
Surveillance, whether or not using technical means, in places that are inaccessible to the public and hidden from view and entering places that are inaccessible to the public, whether or not hidden from view for surveillance, installing technical means, opening or removing an object (Art. 18/11 of the Intelligence Services Act)[85]	2

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

Exceptional methods (GISS)	Number of authorisations
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)	0
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)	0
Collecting data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act)	6
Penetrating a computer system (Art. 18/16 of the Intelligence Services Act)	4
Tapping, intercepting and recording communications (Art. 18/17 of the Intelligence Services Act)	39
TOTAL	**51**

The sharp percentage decrease (more than 30%) in the number of authorised exceptional methods by GISS mainly relates to the collection of data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act): this method was used 20 times in 2019, but only 6 times in 2020. The same downward trend is observed for the penetration of a computer system (Art. 18/16 of the Intelligence Services Act): uses of this method halved relative to 2019 (from 8 to 4).

II.1.1.4. Interests and threats justifying the use of ordinary and special methods[86]

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

- Intelligence assignment (Art. 11/1 of the Intelligence Services Act);
- Ensuring military security (Art. 11/2 of the Intelligence Services Act);
- Protecting secrets (Art. 11/3 of the Intelligence Services Act);
- 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 therefore cannot be used for security investigations or other roles entrusted to GISS by or in accordance with 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).

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

About two-thirds of the specific and exceptional methods used by GISS relate to the role of collecting, analysing and processing intelligence about the activities of foreign intelligence services on Belgian territory (Article 11/5 of the Intelligence Services Act).[87] 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 countering espionage. It is also worth noting that the number of special methods used in the context of the threats of terrorism and extremism has increased significantly, whereas those relating to the threat of interference have halved.

NATURE OF THREAT	NUMBER IN 2020
Espionage	139
Interference	19
Extremism	20
Terrorism	19
Criminal organisations	-
Other	-
Total	**197**

Unlike for the use of special methods, the Committee does not have any figures on the perceived threat and the interests to be defended for ordinary methods referred to in this chapter. In a previous activity report, the Committee recommended that the services also record this data and make it available.[88] This has not happened so far; the Committee repeats its earlier recommendation in this regard.

II.1.2. METHODS USED BY STATE SECURITY

II.1.2.1. Ordinary "plus" methods

Ordinary methods (State Security)	Number of authorisations
Identification of a telecommunication user	5123
Identification of a prepaid card holder	0
Targeted PNR data searches	30
Referral of PNR data on basis of hits	Not disclosed
Use of police camera images	Not in force[89]

87 There were no uses of special intelligence methods outside Belgium by GISS in 2020.

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

89 The scope of application of Article 16/4 of the Intelligence Services Act (for example with regard to consultations of the Directorate of Police Information and ICT Resources (DRI) of the Federal Police) is the subject of a legal analysis (2021).

As stated, the Committee is examining in more detail the way in which this method is used in a review investigation initiated in 2019.

II.1.2.2. Specific methods

Specific methods (State Security)	Number of authorisations
Surveillance in places accessible to the public using technical means or surveillance in a place that is inaccessible to the public and not hidden from view whether or not using technical means (Art. 18/4 of the Intelligence Services Act)	245
Searching 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)	1
Requesting transport and travel information from private transport and travel services (Art. 18/6/1 of the Intelligence Services Act)	70
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 (Art. 18/7 § 1, 1 of the Intelligence Services Act)	46
Requesting the cooperation of the operator of an electronic communications network to obtain payment method data and identify the payment method and time of payment for the subscription to or use of the electronic communications service (Art. 18/7 § 1, 2 of the Intelligence Services Act)	0
Tracing call-associated data of electronic means of communication and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act)	650
Monitoring localisation data for electronic communications and requesting the cooperation of an operator (Art. 18/8 of the Intelligence Services Act)	617
TOTAL	**1629**

As mentioned earlier, the number of the specific methods used saw a clear decrease in 2020 compared to 2019, from 1781 to 1629. There was a gradual decrease for practically all the specific methods; with the exception of requests for transport and travel information from private transport and travel services, the number of which increased considerably from 48 in 2019 to 70 in 2020.

II.1.2.3. Exceptional methods

Exceptional methods (State Security)	Number of authorisations
Surveillance, whether or not using technical means, in places that are inaccessible to the public and hidden from view and entering places that are inaccessible to the public, whether or not hidden from view for surveillance, installing technical means, opening or removing an object (Art. 18/11 of the Intelligence Services Act)	9
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)	8
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)	11
Collecting data on bank accounts and banking transactions (Art. 18/15 of the Intelligence Services Act)	186
Penetrating a computer system (Art. 18/16 of the Intelligence Services Act)	74
Tapping, intercepting and recording communications (Art. 18/17 of the Intelligence Services Act)	223
TOTAL	**511**

Unlike the used specific methods, the number of used exceptional methods by State Security is constantly increasing (+14% compared to 2019). This increase is entirely explained by the use of the method 'Collecting data on bank accounts and banking transactions' (Art. 18/15 of the Intelligence Services Act), which more than doubled (from 95 in 2019 to 186 in 2020) and of 'Penetrating a computer system' (Art. 18/16 of the Intelligence Services Act), for which the numbers rose from 48 in 2019 to 74 in 2020. Less use was made of the other exceptional methods compared to 2019.

II.1.2.4. Interests and threats justifying the use of special methods

The following table lists the threats (and potential threats) for which State Security issued authorisations for specific and exceptional methods. Of course, a single method may be directed against multiple threats. State Security may use specific methods in the context of all threats within its competence (Article 8 of the Intelligence Services Act), namely espionage, terrorism (including the radicalisation process), extremism, proliferation, harmful sectarian organisations, interference and criminal organisations.

Since the entry into force of the Act of 30 March 2017, the special intelligence 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 THREAT	NUMBER IN 2020
Espionage	816
Interference	27
Extremism	296
Proliferation	3
Harmful sectarian organisations	0
Terrorism	998
Criminal organisations	0
Monitoring the activities of foreign services in Belgium	(included in the figures above)
TOTAL	2140

The figures above show that while the threat of terrorism certainly accounted for fewer uses of special intelligence methods in 2020 (decreasing from 1118 to 998), it remained the top priority for State Security in 2020, followed closely by espionage (816). Like GISS, State Security recorded a sharp drop in the number of requests relating to interference (from 87 in 2019 to 27 in 2020). Given that harmful sectarian organisations and criminal organisations have not been actively monitored since 2015, it is not surprising that these threats do not feature in the figures.

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

II.2.1.1. General

The control of certain ordinary methods is regulated differently in the case of each method.

Regarding the identification of a telecommunication 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. However, the

Committee decided to carry out random checks on a number of requests every year.[90] This control started in 2020.

With regard to access to PNR data held by the Passenger Information Unit, Article 16/3 of the Intelligence Services Act states that the head of service must decide on any such access, 'in a duly justified manner'. 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 translations). The Committee issued only one such prohibition in 2020 (see below).

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 and an *a posteriori* check.

II.2.1.2. Corrective decisions

Regarding the corrective decisions taken by the Committee in the context of the monitoring of the use of the ordinary methods mentioned above, concerning State Security, additional information was requested in two cases and no orders prohibiting the use of data were issued.

Concerning GISS, four decisions were taken in 2020 in this context: additional information was requested in three cases and one prohibition order was issued. In this connection, the Standing Committee I wishes to point out that although Article 16/3 makes provision for it, issuing an order prohibiting the use of data without ordering the destruction of that data makes little sense. However, a destruction order is always possible on the basis of the Data Protection Act. It therefore seems appropriate to combine Article 16 of the Intelligence Services Act and Article 51/3 of the Review Act.

II.2.2. Control of special methods

II.2.2.1. Figures

This section deals with the activities of the Standing Committee I in relation to specific and exceptional intelligence methods. Attention will only be paid to the jurisdictional decisions made in this regard and not to the operational data. 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 also attends the fortnightly meetings at which State Security informs the SIM Commission about

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

the implementation of the exceptional methods. A report on this subject is prepared for the Committee, giving it a better insight into the use of these methods.[91]

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

1. At its own initiative;
2. At the request of the Data Protection Authority (DPA);
3. As a result of a complaint from a citizen;
4. By operation of law, whenever the SIM Commission has suspended a specific or 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 (Articles 131*bis*, 189*quater* and 279*bis* BCCP). In that case, the Committee gives its opinion on the lawfulness of the specific or exceptional methods that have produced intelligence used in a criminal case. Requests for an opinion are made by the investigating or criminal courts. Strictly speaking, the Committee does not act as a jurisdictional body in this matter.

METHOD OF REFERRAL	2013	2014	2015	2016	2017	2018	2019	2020
1. At its own initiative	16	12	16	3	1	1	4	2
2. Data Protection Authority	0	0	0	0	0	0	0	0
3. Complaint	0	0	0	1	0	0	0	0
4. Suspension by SIM Commission[92]	5	5	11	19	15	10	12	9
5. Authorisation by Minister	2	1	0	0	0	0	0	0
6. Pre-judicial consulting body	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**

The number of decisions taken by the Committee continued to fall. In addition, all but two referrals resulted from a suspension by the SIM Commission.

91 In 2017, the Committee recommended that GISS also hold such fortnightly meetings, considering its statutory obligation to do so (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 special intelligence methods – there have been monthly meetings and (in principle) fortnightly reports.

92 Arising, for example, from recording problems or problems with the removal of equipment.

Once the referral has been made, the Committee may make various kinds of decisions and at various stages (preliminary[93], interim[94] or final[95]).

In 2020, all ten of the final decisions taken by the Committee consisted of putting a stop to the use of the intelligence method concerned.

II.2.2.2. Decisions

The main illegalities identified by the Committee were lack of sufficient justification, late notification of the SIM Commission, and lack of a precise purpose.

For a more complete summary of the case law, see the Activity report 2020, available in French and Dutch on the Committee's website. This report details the substance of the decisions taken in 2020 by the Standing Committee I in its jurisdictional role – stripped from all operational data and only mentioning the elements of legal relevance.

The decisions are divided under three headings:

- 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.

II.3. CONCLUSIONS

The Standing Committee I draws the following general conclusions:

- Between 1 January and 31 December 2020, a combined total of 2337 authorisations were granted by the two intelligence services for the use of special intelligence methods: 2140 by State Security (1629 for specific methods and 511 for exceptional methods) and 197 by GISS (146 for specific methods and 51 for exceptional methods). The number of uses of SIMs increased steadily in recent years until it reached a plateau in 2019; in 2020 it fell slightly for the first time. According to the officials responsible for data collection methods at State Security and GISS, the COVID pandemic had no impact on the use of special intelligence methods.
- State Security remains responsible for the largest share by far (91.5%) of uses of these methods. In other words, GISS accounts for less than 1 in 10 uses.

---

93 Finding that a complaint is manifestly unfounded or null and void.

94 Such as suspending the use of the method concerned, ordering an investigation by the Investigations Service, etc.

95 Such as putting a stop to the use of the method concerned, banning the use of the data collected by this method and ordering its destruction, totally or partially lifting the suspension and the ban decided on by the SIM Commission, etc.

- A breakdown of the figures shows that the use of specific methods by GISS continued to increase, from 138 to 146 instances. However, the number of exceptional methods used dropped by around a third, from 76 to 51. At State Security, the opposite trend is observed, namely a striking decrease in the use of specific methods (from 1781 in 2019 to 1629 in 2020) and a further significant increase in the use of exceptional methods of 14% relative to 2019.
- With regard to the ordinary method of sending a request to operators in order to identify certain means of communication, a decrease in their use can again be observed, of approximately 9% for both State Security and GISS.
- It is also worth noting that the number of special methods used in relation to the threats of terrorism and extremism has increased significantly, whereas those relating to the threat of interference have halved.
- In its use of specific intelligence methods, GISS mainly focused on the threats of terrorism and extremism; its uses of such methods in response to the threat of interference have halved. The main threat State Security focused on in this context was terrorism, followed by espionage.
- A total of 11 cases were referred to the Committee: there were 2 referrals at its own initiative and 9 automatic referrals following a suspension by the SIM Commission on the grounds of illegality (Art. 43/4 of the Intelligence Services Act). The main illegalities identified were lack of sufficient justification, late notification of the SIM Commission, and lack of a precise purpose.
- In 2020, for the first time since the entry into force of the SIM Act of 4 February 2010, the Standing Committee I submitted a preliminary question to the Constitutional Court concerning the SIM legislation.

CHAPTER III.

MONITORING OF FOREIGN INTERCEPTIONS, IMAGE RECORDINGS AND IT INTRUSIONS

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

The review *prior* to interceptions, intrusions or image recordings is done on the basis of a list drawn up annually.[89] This means that in addition to an annual interception plan, an intrusion and image plan must also be drawn by GISS.[90] 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, which in turn sends the lists, with the minister's authorisation, to the Standing Committee I.[91]

In the plan received for the year 2020, only minor remarks were made about the listed interceptions. The Standing Committee I stressed that future plans relating to recordings and intrusions must comply with legal requirements and suggested that the relevant sections should be based on the interceptions plan.

---

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

90 In these plans, GISS draws up a list of '*organisations and 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 shall justify why each organisation or institution will be subject to an interception, intrusion or capture of fixed or moving images, with reference to the roles mentioned in Article 11, § 1, 1 to 3 and 5, and shall state the anticipated duration*' (Art. 44/3 of the Intelligence Services Act).

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

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

In 2020, the Committee visited the facilities from which the interceptions are carried out. During the visit, the logbook's compliance with the relevant laws and directives was checked. The Standing Committee I noted on this occasion that GISS had opened a new register which no longer corresponded to the Committee's recommendations.

The Standing Committee I also observed that GISS was still implementing projects relating to the application of Article 44 of the Intelligence Services Act.

In 2020, despite the restrictions imposed by the public health crisis, the Standing Committee I continued its procedures with GISS in connection with its control of the activities relating to Article 44 of the Intelligence Services Act. At the end of the year, a working meeting was organised at GISS with all those involved in the implementation of Article 44, at which certain points for attention were clarified and steps were taken towards the standardisation of the various plans.

The review *after* the use of the method is carried out '*using monthly lists of countries or of organisations or institutions that have actually been the subject of interception, intrusion or image capture during the previous month*'; these lists '*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 submitted 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.

The Standing Committee I received all the legally required lists for 2020.

What can the Standing Committee I do in case of irregularity? Article 44/4 of the Intelligence Services Act states that '*the Standing Intelligence Agencies Review 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] authorisation. 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). Despite the Committee's urgent recommendation, such a decree on the subject of interception has still not been issued. The Committee therefore once again recommends that this be done as soon as possible.

CHAPTER IV.
PARTICULAR ASSIGNMENTS

Over the years, the Standing Committee I has been assigned a number of particular roles 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. They relate to the control of the activities of the ISTAR (Intelligence Surveillance Target Acquisition and Reconnaissance) battalion, the monitoring of special funds, and the oversight of the monitoring of political representatives.

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

The creation of the ISTAR battalion responded to an ever-growing need for battlefield intelligence capabilities during operations abroad. The question of which body would oversee the activities of this battalion arose.

A protocol agreement was signed in 2018 between GISS and the CHOD which has temporarily settled the issue.[100] The organisation of technical and legal oversight[101] lies with GISS, with additional monitoring – albeit indirectly – by the Standing Committee I.

In accordance with the protocol, the Committee received several GISS monitoring reports in 2020, which showed that the ISTAR battalion was engaged in few activities falling within the scope of the protocol. According to GISS, the intelligence activities conducted by the ISTAR battalion complied with the relevant regulations and guidelines.

---

100 Protocol agreement of 24 May 2018 between the CHOD and GISS regarding the HUMINT and analysis capabilities of the ISTAR battalion. A two-year extension of this protocol agreement was signed on 19 May 2020.

101 By technical oversight is meant the monitoring of the correct application of the analysis guidelines, the HUMINT guidelines and the specific agreements between the CHOD and GISS. By legal oversight is meant checks that the protocol is being applied correctly.

IV.2. MONITORING OF SPECIAL FUNDS

The Court of Audit checks the legality, legitimacy and effectiveness of all expenditure of government agencies. In principle, this also applies to all expenditure of the intelligence services. However, due to the sensitivity of this matter, part of the budget of State Security and GISS (i.e. the "special funds", including spending on operations and informants, for example) is not examined by the Court of Audit. For State Security, this expenditure was only audited by the General Policy Director of the Minister of Justice. Midway through 2018, the Court of Audit expressed its intention of conducting a periodic audit of these funds starting from the closure of the 2018 account.

Since 2020, the formal audit of GISS accounts has also been carried out by the Court of Audit, which can request technical support from the Standing Committee I.

The Committee has thus been able to '*perform its role with more attention to the use of these funds*' (free translation). It was decided to initiate a follow-up investigation into the management, use and control of special funds (cf. Chapter I.11.11).

IV.3. OVERSIGHT OF THE MONITORING OF POLITICAL REPRESENTATIVES

The question whether and to what extent the Belgian intelligence services (may) monitor political representatives, and according to what rules, remains highly topical.

In accordance with an internal directive, State Security sends since 2018 occasional reports to the Minister of Justice and the Prime Minister, with a copy to the Standing Committee I, on political representatives who contribute to the creation of a threat, as well as a quarterly overview of all documents in which political representatives are mentioned.

To ensure oversight, the Committee has developed a methodology relating to the '*issue of the monitoring of political representatives by the intelligence services and the role of the Standing Committee I*', which was approved by the Parliamentary Monitoring Committee in 2020. The monitoring of political representatives was also the subject of a (periodic) review investigation in 2020 (see Chapter I.11.12).

Like State Security, GISS was urged to adopt a uniform directive with clear and unequivocal rules regarding the collection, processing, consultation, storage and archiving of information relating to political representatives. In 2020, the Committee still did not receive any indication that it had done so in 2020. Despite repeated requests, GISS has no standard operating procedure to deal with this information, nor has it determined how to inform the Standing Committee I.

CHAPTER V.

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

V.1. INTRODUCTION

The General Data Protection Regulation 2016/679 (GDPR)[115] and Directive 2016/680 (the Directive)[116] regulate how public and private actors must act when collecting, storing, retaining and transferring personal data. Both European instruments resulted in important legislative changes at national level: the Data Protection Authority (DPA)[117] – which succeeded the Privacy Commission – was established in December 2017, and a new Data Protection Act was voted on in July 2018.[118] This Act, in turn, amended the Review Act of 18 July 1991, with the Standing Committee I being designated as the data protection authority for the processing of personal data in the context of "national security".

The Committee's role in this regard is described in the Act establishing the Data Protection Authority (DPA Act), in the Data Protection Act (DP Act) and in the Review Act.

In 2019-2020, the Committee developed various activities in order to be able to observe these additional duties and obligations. As of 2018, a Data Protection Officer (DPO) was appointed for all processing operations carried out by the Committee that fall outside "national security" (e.g. processing in the context of

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

116 Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *Official Journal of the European Union*, 4 May 2016, No. 119/89.

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

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

personnel management and logistics). In addition, various meetings were held with the three other competent supervisory authorities (see below, V.2.). The Standing Committees I and P agreed to draw up a proposal for the amendment of the Review Act, as some of its provisions do not reflect the new powers of the two Committees. The Committee also continued its internal discussions, which gave rise to an initial general commentary that will contribute to the next assessment of the DP Act[119] (see below, V.7).

V.2. COOPERATION BETWEEN THE COMPETENT SUPERVISORY AUTHORITIES

Belgium has no fewer than four competent supervisory authorities (CSAs) at federal level. In addition to the Standing Committee I, the Data Protection Authority (DPA), has a general and residual competence, the Supervisory Body for Police Information (C.O.C.) mainly controls processing activities that fall within the scope of Title 2 of the Data Protection Act, and the Standing Committee P, controls, together with the Standing Committee I, the processing activities of CUTA (Art. 161 DP Act). The C.O.C. and the Standing Committee I are also jointly responsible for the common databases referred to in Article 44/11/3*bis* of the Policing Act (Article 44/11/3*quinquies*).

The competent supervisory authorities are required 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). In 2019, the various services prepared and negotiated a cooperation protocol, which was adopted and published in 2020.[120]

V.3. MONITORING OF PERSONAL DATA PROCESSING PERFORMED BY BELPIU

V.3.1. THE FRAMEWORK FOR BELPIU'S MONITORING

The Act of 25 December 2016 on the processing of passenger name records (PNR Act) implements the European objectives of simultaneously preventing and combating terrorism and serious crime. A "Passenger Information Unit" (PIU) was set up for this purpose within the FPS Home Affairs FPS, namely the

119 See Article 286 of the DP Act.

120 See:
https://www.comiteri.be/images/pdf/publicaties/samenwerkingsprotocol_DPAS_FR_2020_11_24.pdf.

Belgian Passenger Information Unit (BELPIU). This unit stores passenger data in a database with a view to preventing and combating the crimes or threats specified in the PNR Act.

Under subtitle 5 of Title 3 of the DP Act, the Standing Committee I is the competent supervisory authority with regard to '*any processing of personal data by the PIU carried out for the purposes referred to in Article 8, § 1, 4, of the Act of 25 December 2016*' (Art. 169 DP Act) or, in other words, the processing 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 intelligence and security services*' (Art. 8, § 1, 4 DP Act) (free translations). This refers to the processing by State Security and GISS as part of their regular intelligence assignment. The Committee is competent to monitor the functioning of the PIU only to the extent that it cooperates with requests for information and intelligence from one of the two intelligence services, whether in the form of targeted searches, watch lists or profiles.

V.3.2. RESULT OF JOINT MONITORING

Given their respective powers as competent supervisory authorities for data processing by the Passenger Information Unit, the Supervisory Body for Police Information (C.O.C.) and the Standing Committee I decided, on their own initiative, to conduct a joint inspection of this service. The inspection focused on ICT security and information safety and on the proportionality of data processing. The investigation report was finalised in June 2020 and presented to the Parliamentary Monitoring Committee.

In essence, the Committee and the C.O.C. generally approved of the structured approach to data protection and information security, in particular with regard to the initiatives and advice of the Data Protection Officer. However, the Committee and the C.O.C. identified a series of points for attention relating to the organisation of information security. Special attention was also paid to an incident relating to the creation and use of privileged users, which requires further investigation. The Committee and the C.O.C. also highlighted a problem relating to compliance with the "closed box" principle[121], although the legal requirements concerning this principle have not been breached by BELPIU.

[121] This principle refers to the Operational Travel Intelligence Room (OTIR), a confined space at FPS Home Affairs where seconded members of the PIU have access to the passenger database. It is a space which is hermetically sealed off from third parties and unauthorised persons, and only accessible to a limited number of specifically designated persons. Access to the passenger database is linked to the performance of a specific assignment by the seconded PIU member. This person only has access to passenger data relating to the assignment or assignments of his or her service, on the basis of individual access profiles.

V.4. OPINIONS

The Committee may provide an opinion '*on a draft of a bill, royal decree, circular or any other document setting out the policies of the competent ministers*' (free translation) in two cases: if the law requires it to give an opinion or at the request of the Chamber of Representatives or the competent minister (Art. 33, paragraph 8 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 (cf. Chapter VII). This general advisory competence is broader in that sense, but it is also narrower since it is limited to the operation of the intelligence services and CUTA.

In 2020, the Committee issued four opinions in this capacity, either as an exclusively competent supervisory authority or as an authority jointly competent with the Standing Committee P. Two of these opinions relate to the exchange of classified information and two others to the administrative approach and the creation of a Directorate responsible for assessing the integrity of the public authorities.[122]

V.5. INFORMATION FROM THE MONITORED SERVICES

The services monitored by the Standing Committee I must keep or make certain information available to it. The data controller must, for example, give notification of any security breach likely to create a high risk to the rights and freedoms of natural persons as soon as possible and preferably within 72 hours of becoming aware of it (Articles 89, 122, 155 and 180 DP Act). No data breaches[123] were reported to the Committee in 2020.

On its website, the Committee has made available a form that can be used to notify it of data breaches with the required precision.[124]

V.6. HANDLING OF INDIVIDUAL DPA COMPLAINTS

The Standing Committee I also handles individual requests with regard to the processing of personal data by the aforementioned persons and services as well

---

122 Opinions can be found on the Standing Committee I's website.

123 Article 26, 11 DP Act: '*data breach: a security breach resulting in the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of transmitted, stored or otherwise processed personal data, or unauthorised access to such data*' (free translation).

124 https://www.comiteri.be/images/pdf/FormDB_fr.pdf.

as their subcontractors (Art. 34 Review Act and Articles 79, 113, 145 and 173 DP Act). The requesting party is entitled to ask for their inaccurate personal data to be corrected or erased. They may also ask for a check to be conducted on the compliance with the applicable data protection rules . In addition, they can complain about the failure to comply with data protection rules of a data controller under the jurisdiction of the Committee.

In order to be admissible, the request must be written, dated, signed and duly motivated (Art. 51/2 Review Act). If the request is manifestly unfounded, the Committee may decide not to comply with it. This decision must be duly motivated and communicated in writing to the requesting party.

The following table gives an overview of the requests processed (opened and/or closed) in 2020. The columns provide a breakdown of the requests according to whether the competence of the Standing Committee I is exclusive or joint with other supervisory authorities.

Processing of individual requests[125]

2020	Standing Committee I	Standing Committees I and P	Standing Committees I and P and the C.O.C.	Total
1. Case opened in 2018	1	0	0	**1**
2. Cases opened in 2019	4	0	0	**4**
3. Cases opened in 2020	17	1	3	**21**
4. Alleged interference with rights and freedoms	15	1	2	**17**
5. No interference alleged with rights and freedoms	7	0	1	**8**
6. Cases in progress	7	1	3	**11**
7. Closed cases	15	0	0	**15**
8. Request inadmissible	1	0	0	**1**
9. Processing compliant with DP Act	14	-	-	**14**
10. Processing not compliant with DP Act	-	-	-	**0**
11. Total number of requests	22	1	3	**26**

125 Rows 1 to 3 show the number of cases according to the year in which they were opened. Rows 4 and 5 divide them up according to whether or not the data subject alleges specific interference with his or her rights and freedoms in connection with the processing of data by the data controller. Rows 6 and 7 specify the state of progress of the cases in 2020 (closed or still in progress). Finally, Rows 8 to 10 arrange the closed cases according to their outcome (a finding of compliance or lack of compliance with the DP Act – N.B.: the failure to process personal data is counted as data processing in accordance with the DP Act).

To summarise, the table covers a total of 26 cases. Of these, 11 were still in progress at the end of 2020 and 15 had been closed. One of these cases was considered inadmissible and in the other 14 it was found that the data processing had been carried out in accordance with the DP Act. In the cases which were admissible and closed, the requesting parties were systematically informed that the required checks had been carried out.

It is worth noting that in 70% of the requests, the data subjects alleged a specific interference with their rights and freedoms caused by or linked to the processing of data by a data controller falling under the competence of the Standing Committee I. Such interference would exist, for example, in the context of a nationality declaration procedure during which an intelligence service communicates information to the Public Prosecutor's Office, if the data subject claims to be the subject of regular police checks or has been refused access to a territory, if data from an intelligence service has been used in criminal legal proceedings, etc.

The remaining 30% of requests consisted in the indirect exercise of rights, without any particular details being provided or any specific grievance. Typically, the data subject wonders if their personal data is being processed and if its processing complies with the applicable regulations (indirect access).

This finding is not surprising, as the answer provided to a data subject who exercises his or her rights does not give any information about any processing of personal data about him or her by the services under the competence of the Committee. It is only when the data subject suspects or actually experiences the effect of such data processing that he or she has a reason to ask the Standing Committee I to carry out the necessary checks.

V.7. ASSESSMENT OF THE DATA PROTECTION ACT

Article 286 of the DP Act states that the Act will be subject to a joint assessment by the competent ministers during the third year after its entry into force. In this context, and taking account of its newly acquired experience as a supervisory authority, the Committee has made several recommendations to the legislators – summarised below – to ensure the effectiveness of the data protection rules.

V.7.1. HELPFUL COMMUNICATION WITH DATA SUBJECTS

Whatever the extent and outcome of the checks performed by the Committee, a data subject who submits a complaint or exercises his or her rights indirectly through the Committee is invariably presented with the same enigmatic response:

'The necessary verifications have been performed'.[126] However, the possibility cannot be ruled out *a priori* and for all scenarios that it may be legitimate and appropriate to communicate certain information to the data subject.[127]

The Standing Committee I recommends that the legislators should make provision in certain cases for the possibility of communicating (pieces of) information to the data subject under Title 3 of the DP Act.

V.7.2. CHECKING THE APPLICATION OF THE DATA PROTECTION RULES AT THE RIGHT TIME

The Standing Committee I points out that it could be consulted by persons already involved or in the process of becoming involved in civil, judicial or administrative proceedings (e.g. naturalisation processes, mandatory measures, etc.), the resolution of which may depend on analyses or data from an intelligence service or CUTA.

The Committee takes the view that in such cases, when the dispute enters a contentious phase, the legislators could stipulate that the competent judge, if faced with a serious challenge to the data being used, could, if they deem it necessary (and where applicable, exclusively at the request of the data subject), suspend the case in order to question the Standing Committee I so that it can carry out the necessary checks and submit an opinion to the judge.

V.7.3. BETTER COORDINATION OF JOINT OR CONCOMITANT COMPETENCE BETWEEN CSAS

The legislators defined the scope of Belgian data protection rules on the basis of the organic criterion.[128] They have also made provision, with regard to the Standing Committee I, for scenarios where there is joint competence: in relation to CUTA (joint competence with the Standing Committee P),[129] and in relation to the common databases (joint competence with the C.O.C.).[130] This sometimes leads to the same request from a citizen concerning the operation of CUTA giving rise

126 Article 80, para. 2 DP Act; Article 34, para. 6 Review Act.

127 The legislators had in fact already made a pronouncement along these lines when defining the Committee's original field of competence: in the context of handling complaints and reports, the Committee can (and indeed must) communicate the outcome of an investigation 'in general terms' when it has been completed (Article 34, para. 6 Review Act).

128 Put simply, the Supervisory Body for Police Information is responsible for integrated police, the DPA for the private sector and the Standing Committee I for State Security and GISS.

129 See Article 161 DP Act as well as Subtitle 4 of Title 3 DP Act.

130 See Articles 44/11/3*bis* to 44/11/3*quinquies*/2 Policing Act.

to two separate verifications.[131] Competences can also be concomitant, meaning that the competence of each supervisory authority separately is legally exclusive but, in practice, is exercised at least partly concomitantly, so that it would scarcely be possible for one to act without the other (in particular because of the risk of subjecting a data controller to contradictory instructions).
This situation illustrates that an 'organic logic' for the applicability of data protection rules can bring with it complexity and, consequently, potential administrative burdens that may lead to inefficiency.
For the sake of efficiency, the Standing Committee I recommends that the legislators only assign clear and consistent exclusive powers to the competent supervisory authorities.

V.7.4. CLARIFYING THE DATA PROTECTION RULES APPLICABLE TO THE COMPETENT CSAS IN THE NATIONAL SECURITY SECTOR

The Standing Committee I recommends that the legislators clearly define the data protection regime applicable to the Committee and the SIM Commission in the exercise of their functions in the field of national security, as the current legal framework has too many omissions. This legal regime should be founded on Title 3 of the DP Act and adapted to the specific characteristics of the aforementioned institutions.

V.7.5. ALLOWING THE STANDING COMMITTEE I TO PROVIDE OPINIONS AT ITS OWN INITIATIVE

The possibility cannot be ruled out that, in the exercise of its powers, the Standing Committee I may identify outdated texts or practices to which it would like to be able to draw attention by means of an opinion, whether in connection with a particular legislative process or otherwise. However, unless it is legally required to do so, the Standing Committee I can only issue an opinion when requested by the Chamber of Representatives or the competent Minister.
The Committee recommends that the legislators allow the Committee to provide opinions at its own initiative, along the same lines as the possibilities open to the DPA and the C.O.C.[132]

---

131 A first verification jointly with the C.O.C. on the role of CUTA in the context of the common databases, and a second jointly with the Standing Committee P on the other aspects of the operation of CUTA.

132 See Article 23, § 1 DPA Act and Article 236, § 2 DP Act.

V.7.6. IMPROVING LEGAL CERTAINTY IN THE DATA PROTECTION REGIME APPLICABLE TO THE FIELD OF NATIONAL SECURITY

The wording of the Belgian law on the protection of personal data is complex and difficult to comprehend. However, in this area, the clarity of the text is a constitutional and conventional requirement.

The Standing Committee I first wishes to point out that the purpose of data processing could be made decisive in determining the applicable data protection rules. In positive law, at least in part, the legislators govern the competence of the supervisory authorities on the basis of an organic criterion. However, it is the purpose of a data processing operation that should determine whether or not it falls within the scope of a complete Title 3, as far as national security is concerned.

With the same objective of clarity and legal certainty, the Standing Committee I further notes that the criteria defined for identifying the data controller give rise to legal uncertainty. With regard to the field of national security, the legislators could, in the DP Act, identify the (joint) controller(s)on the basis of their concrete responsibilities with regard to these roles and their relative autonomy, or even their independence.

V.7.7. THE INTERNATIONAL DIMENSION OF DATA PROCESSING

In the Bern joint declaration,[133] the Standing Committee I and some of its counterparts underlined the limits of their respective *national* oversight mandates. This led to the adoption of a Charter of the Intelligence Oversight Working Group and the creation of an Oversight Working Group.[134]

Mutatis mutandis, such limits also exist in the context of the protection of individuals with regard to the processing of personal data.

In this context, the Standing Committee I draws the legislators' attention to the forthcoming ratification of Convention 108+, which introduces a mechanism for cooperation and mutual assistance between Parties. Unlike cooperation mechanisms under EU law, this international instrument will cover processing for national security purposes. In order to implement this mechanism, Article 16, 2., a) states that each Party should designate one or more supervisory authorities within the meaning of Article 15 of the Convention.

---

133 Strengthening oversight of international data exchange between intelligence and security services (free translation), 22 October 2018.

134 See https://www.comiteri.be/images/pdf/publicaties/Charter_Intelligence_Oversight_Working_Group_signed_12_December_2019.pdf.

However, as the law stands, Article 55, § 1, of the DPA Act states that '*the Data Protection Authority may cooperate with any body or other data protection authority of another State, making use of the powers conferred on it either under Regulation 2016/679 or by national legislation*' (free translation).

Given the independence of the DPA and the Standing Committee I as competent supervisory authorities, the Committee recommends that the legislators assign to the Committee, taking into account the rules governing its activities (including the Classification and Security Clearances Act), exclusive and specific competence in matters of international cooperation in the field of data protection in the intelligence sector.

Beyond the question of international cooperation, the international dimension of data flows also entails a loss of control *at the level of the Belgian services* of data leaving Belgian jurisdiction as a result of cross-border data flows. On this point, although the legislators have not chosen to make the principle of accountability binding on the intelligence services,[135] the Standing Committee I takes the view that certain modifications to the rules relating to cross-border data flows in the direction of greater accountability for the services could strengthen the effectiveness of data protection. The Committee stresses the importance of this part of the data protection rules. It is indeed important to avoid personal data, once transferred by the Belgian intelligence services, completely escaping their control, with unjustified (or no longer justified) effects on the rights and freedoms of the data subjects abroad.

135 On this principle, see in particular Articles 5, 2. and 24, 1. GDPR, as well as Article 10, 1. Convention 108+.

CHAPTER VI.
MONITORING OF COMMON DATABASES

In 2016, the Ministers of Home Affairs and Justice set up the common database of foreign terrorist fighters (CDB FTF). Its purpose was to contribute to the analysis, evaluation and monitoring of individuals with links to this issue. This common database (CDB) was modified in 2018 to create the common database of terrorist fighters (CDB TF). This includes, in addition to the existing category of "foreign terrorist fighters", a category of "homegrown terrorist fighters". The year 2018 also saw the creation of a new, separate common database for "hate propagandists" (CDB HP).[134]

By a Royal Decree issued at the end of December 2019,[135] two new categories were added to the CDB TF: "potentially violent extremists" (PVE) and "terrorism convicts" (TC).

VI.1. THE MAIN REGULATORY CHANGES

The Royal Decree of 20 December 2019, published in January 2020, has a threefold objective. First, new categories are added to the common database of terrorist fighters (CDB TF), namely 'potentially violent extremists' and 'terrorism convicts'. Secondly, several 'technical amendments' are made to the Royal Decrees TF and HP following the amendment of the Act of 5 August 1992 by the Act of 22 May 2019. Lastly, the intention was to grant the FPS Finance's General Administration of the Treasury direct access to the CDB TF and HP.

134 Article 44/6 of the Policing Act assigns oversight over the processing of information and personal data contained in the CDBs to the Supervisory Body for Police Information (C.O.C.) and to the Standing Committee I ("the supervisory authorities").

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

VI.1.1 ADDING POTENTIALLY VIOLENT EXTREMISTS (PVE) TO THE CDB TF

A potentially violent extremist is defined as any individual with a connection to Belgium who meets the following cumulative criteria:

a) they have extremist ideas that justify the use of violence or coercion as a course of action in Belgium;
b) there are reliable indications that they intend to resort to violence in relation to the extremist views mentioned in a);
c) in addition, the PVE must meet at least one of the following three conditions which are considered to be risk factors for the use of violence:
   - they systematically maintain social contacts within extremist circles;
   - they have been found by a competent professional to have psychological problems;
   - they have committed acts or have a record that can be regarded as a) a crime or offence against the physical or mental integrity of third parties; or b) instruction or training in the manufacture or use of explosives, firearms or other weapons or noxious or hazardous substances, or in other specific methods and techniques useful for committing terrorist offences; or c) deliberate acts that constitute material support for a terrorist/extremist organisation or network; or d) acts indicating a concerning level of vigilance on the part of the individual with regard to security.

VI.1.2. ADDING TERRORISM CONVICTS (TC) TO THE CDB TF

Terrorism convicts must meet the following cumulative conditions:

- they have a connection with Belgium;
- they have been convicted or been a subject of a court decision for internment, or in the case of minors, of a protection measure for terrorist offences as stipulated in Book 2, Part I*ter* of the Penal Code (in Belgium), or for similar offences abroad; and
- whose level of threat is evaluated by CUTA as medium (level 2), serious (level 3) or very serious (level 4).

Introducing this new category in the CDB TF ensures that all parties who must monitor TC (such as the Directorate general of Penitentiaries, law centres, police, closed asylum centres, State Security, the local taskforces, etc.) are promptly and fully informed about the persons concerned.

VI.1.3. DIRECT ACCESS TO THE CDB TF AND HP FOR A NEW SERVICE

The General Administration of the Treasury was also granted direct access to the CDBs TF and HP. It is the competent authority imposing financial sanctions including freezing funds and economic resources of persons or organisations that commit or attempt to commit, facilitate or participate in terrorist offences.

VI.2. MONITORING ROLE AND OBJECT OF MONITORING

For 2020, the Standing Committee I and the C.O.C. decided to focus their joint monitoring on verifying the direct access granted to the National Security Authority (NSA) and on following up certain recommendations formulated in previous years' reports.

In addition, the monitoring bodies carried out an in-depth examination of the coordination of information processing in the CDB TF and HP, with particular attention to the role of the data protection officer (DPO). In this regard, the growing number of services with access to the CDB TF and HP was also taken into account.

From a methodological point of view, given the coronavirus crisis and in order to allow the services sufficient opportunity to implement the recommendations formulated at the end of the 2019 report, arrangements were made to carry out the survey during the fourth quarter of 2020. Several services were questioned, including the NSA, CUTA (the operational manager of the common databases), the Federal Police (the technical manager) and the data protection officer (DPO). The investigation ended with a meeting with the acting Director of CUTA and the DPO of the common databases. The report is due for the first half of 2021.

VI.3. THE COMMITTEE'S ADVISORY ROLE

The Policing Act requires the joint opinion of the Standing Committee I and the C.O.C. to be sought in various circumstances.

Thus, prior to its creation, the Ministers of Home Affairs and Justice must declare a common database to the Standing Committee I and the C.O.C., as well as its processing methods (including those relating to the recording of data) and the different categories and types of personal data and information processed. In turn, the Committee and the C.O.C. must jointly issue an opinion within 30 days (Art. 44/11/3*bis* § 3 Policing Act). Following consultation with these two bodies, a royal decree deliberated in the Council of Ministers determines the rules for each common database with regard to the protection of personal data and the rules

on the secure processing, use, storage and deletion of data (Art. 44/11/3*bis* § 4 Policing Act). Additional management procedures for common databases may also be determined by a royal decree deliberated by the Council of Ministers, after seeking the opinion of the Standing Committee I and the C.O.C. (Art. 44/11/3*bis* § 8 Policing Act). Finally, the advisory role is also exercised with regard to any draft royal decree establishing or modifying access to common databases (Art. 44/11/3*ter* §§ 2 to 4 Policing Act).

The opinion of the Standing Committee I and the C.O.C. was not sought in this context in 2020.[136]

136 A joint opinion was issued in 2019 concerning the Royal Decree of 20 December 2019, published in the *Belgian Official Journal* on 27 January 2020 (www.comiteri.be).

CHAPTER VII.
OPINIONS

Article 33, seventh paragraph, of the Review Act states that the Standing Committee I '*may only advise on a draft of bill, royal decree, circular letter, or any other document setting out the policies of the competent ministers at the request of the Chamber of Representatives or the competent minister*' (free translation). The Committee issued four opinions on this basis in 2020. These concerned:

- the automatic declassification and transfer of documents to the archives of the Kingdom;
- the creation of a Crossroads Bank for Security;
- evaluation notes in the context of cooperation with foreign intelligence and security services;
- access to the Terrorist Fighters database for Brussels Prevention and Security.

For a summary of the opinions, see the activity report 2020, available in French and Dutch on the Committee's website. The opinions are also available in full on the Committee's website.

CHAPTER VIII.

CRIMINAL INVESTIGATIONS AND JUDICIAL INQUIRIES

As well as contributing to review investigations, the Investigation Service of the Standing Committee I (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 governing review 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 CUTA.

In the cases in which the Investigation Service I conducts a criminal investigation, the director must report to the Standing Committee I after its completion although '*the report shall be limited to the information necessary for the Standing Committee I to perform its roles*' (free translation) (Art. 43, third paragraph of the Review Act).

In 2020, the Investigation Service I carried out investigative actions in the context of its judicial role, concerning three law enforcement cases. A total of 25 official reports were drawn up.

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 must draw up an information report and send it to the Head of the Investigation Service I within a period of fifteen days*' (free translation). The Investigation Service received no such report in 2020.

CHAPTER IX.
EXPERTISE AND EXTERNAL CONTACTS

IX.1. SYMPOSIUM FOR THE TENTH ANNIVERSARY OF THE SIM ACT

The year 2020 marked the tenth anniversary of the SIM Act, and it was felt that this should not go unnoticed. Since the entry into force of the Act of 4 February 2010 governing the intelligence collection methods used by the intelligence and security services, State Security and GISS have used what are termed "special intelligence methods" (SIM). When the legislators decided in 2010 to give the intelligence services new powers, an important task was entrusted to the Standing Committee I at the same time. Together with the SIM Commission, the Committee was to monitor the use of these intelligence-gathering methods, which by definition intrude greatly on individual rights and freedoms.

A decade after the entry into force of the SIM Act, the Standing Committee I considered it appropriate to perform a critical evaluation and discuss the future together with specialists in the field.

On 31 January 2020, the Committee therefore held a symposium entitled "Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière" (Special intelligence methods: from shadow to light) under the auspices of the Chamber of Representatives, intended for the world of intelligence in the broad sense.

The report on the symposium, published in the form of a book,[164] includes the papers presented on this occasion, including international contributions from the Netherlands, Switzerland and France.

[164] J. VANDERBORGHT (ed.), *Bijzondere inlichtingenmethoden in de schijnwerpers – Les méthodes particulières de renseignement : de l'ombre à la lumière*, Lefebvre Sarrut Belgium, Brussels, 2020, 151 p.

IX.2. COOPERATION PROTOCOL BETWEEN HUMAN RIGHTS INSTITUTES

The Act of 12 May 2019 created the Federal Institute for the Protection and Promotion of Human Rights (FIRM/IFDH).[165] The creation of a national institute for human rights, to which Belgium committed when signing the Protocol to the United Nations Convention against Torture, was long overdue.

Meetings – and, given the strict measures dictated by the public health crisis, videoconferences – were organised at regular intervals, bringing together different institutions with a human rights mandate.[166] In a cooperation protocol,[167] all participating institutions agreed to exchange practices and methods, discuss common issues and promote mutual cooperation.

The newly created institute has already been assigned a number of roles: to issue opinions and recommendations, on request or at its own initiative, on questions relating to the promotion and protection of fundamental rights, to monitor the implementation of the international commitments entered into by the Belgian authorities and to encourage the ratification of new international human rights instruments. In 2020, the Chamber of Representatives established a board of directors, appointing twelve independent experts from academia, the judiciary, civil society and the social partners.

IX.3. A MULTINATIONAL INITIATIVE ON INTERNATIONAL INFORMATION SHARING

The inevitable increase in data exchange at the international level between intelligence and security services entails a number of challenges for national oversight bodies. Oversight bodies from (initially) five European countries (Belgium, Denmark, the Netherlands, Norway and Switzerland) have been working together for some years to address these challenges and find ways to reduce the risks of a supervisory gap. After some time, a new partner became involved in this project, namely the United Kingdom's Investigatory Powers Commissioner's Office (IPCO). The group was renamed the "Intelligence Oversight Working Group" (IOWG) and in 2019 was expanded to include three observers: the Swedish Foreign Intelligence Inspectorate

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

166 These institutions include Unia, the Federal Migration Centre, the Institute for the Equality of Women and Men, the Data Protection Authority, the Federal Ombudsman, the High Council of Justice, and the Standing Committees I and P. In 2021, the Combat Poverty, Insecurity and Social Exclusion Service took over the presidency from Unia.

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

(*Statens inspektion av försvarunderättelse-verksamhet* (SIUN)), the Swedish Board of Inventions (*Statens uppfinnarnämnd*, (SUN)) and the German G10 Commission.

Due to restrictions linked to the public health crisis, international activities remained very limited in 2020.

In mid-January 2020 – before the outbreak of the COVID-19 pandemic – representatives of the various oversight bodies held an expert meeting in Oslo, Norway, in order to exchange experiences and discuss methods, best practices and the legal pitfalls they face. The topics discussed at this meeting included the tools for log analysis, the organisation of oversight over bulk collection and the possibility of sharing information between the various participating oversight bodies. In addition, the Standing Committee I explained its intention of exchanging personnel with the Swiss Independent Oversight Authority for Intelligence Activities (OA-IA) within the framework of an internship, even if only for a short period. Having been suspended due to the public health crisis, this exchange was scheduled for the fourth quarter of 2021.

The next meeting, which would be held in Bern, Switzerland, was also postponed indefinitely for the reasons already mentioned.

The Dutch *Commissie van Toezicht op de inlichtingen- en Veiligheidsdiensten* (CTIVD) also took the initiative of studying the rules established on the basis of the international standard constituted by Convention No. 108 of the Council of Europe for the protection of citizens with regard to automatic processing of personal data and its additional protocol, recently updated in Convention 108+ (signed by Belgium on 10 October 2018 but not yet ratified);[168] it requested input from other oversight authorities.

IX.4. CONTACTS WITH FOREIGN OVERSIGHT BODIES

The conferences organised annually by and for the national oversight bodies have resumed since 2018. After the first conference in Paris in 2018, jointly organised by the French *Commission nationale de contrôle des techniques de renseignement* (CNCTR) and the Standing Committee I, a second conference was held in December 2019. In 2020, the Italian oversight body, the *Procura Generale della Corte di Cassazione*, was due to host the European Intelligence Oversight Conference in Rome. The conference, which had to be cancelled, should finally be held in October 2021. In July 2020, delegations from the CTIVD, the CNCTR and IPCO met with the Italian oversight body in Rome to plan this conference and discuss the programme.

168 On this subject see: https://www.coe.int/fr/web/data-protection/convention108-and-protocol. Updated Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 128th Session of the Committee of Ministers, Helsingør, Denmark, 17-18 May 2018.

As a follow-up to the European Intelligence Oversight Conference 2019 in The Hague, the CNCTR prepared a questionnaire on *ex ante* oversight, to which the oversight bodies of all participating countries were invited to respond. The questionnaire was designed to serve as a basis for discussion and exchange of experiences at the next meeting. The Standing Committee I completed this questionnaire in close consultation with the SIM Commission. In July 2020, the Dutch oversight body CTIVD launched a similar initiative. This was a questionnaire on complaint handling. The aim was similar: to collect and analyse best practices on handling complaints in Europe, with a view to improvements. However, these initiatives had to be put on hold.

Finally, in March 2020, the Bulgarian National Special Intelligence Devices Control Bureau set up a project '*for strengthening the capacities of the oversight bodies to protect the rights and freedoms of citizens against unlawful use of special intelligence devices*'. So far, no steps have been taken in this context.

CHAPTER X.

THE APPEAL BODY FOR SECURITY CLEARANCES, CERTIFICATES AND ADVICE

X.1. INTRODUCTION

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.

The Appeal Body is composed of the chairs of the Standing Committee I, of the Standing Committee P and of the Dispute Chamber of the Data Protection Authority. If the three chairs are unable to attend, they can be replaced by a full member of the institution to which the chair concerned belongs.

The chair of the Standing Committee I chairs the Appeal Body. The registry role is performed by the registrar of the Standing Committee I; the registry's personnel are appointed by the Committee I. For more than twenty years, the Appeal Body's activities have been a perfect example of synergy within certain satellite institutions of the Parliament. The collegiate composition of the Appeal Body also ensures that each case is deliberated on with multidisciplinary expertise.

The functioning of the Appeal Body is entirely supported by the Standing Committee I. This involves providing the chair and deputies, the registrar, legal specialists as additional registrars and the administrative personnel who form the registry of this administrative body. In addition, the Standing Committee I covers the costs of the premises and of the functioning of the Appeal Body from its budget. Unlike the Standing Committee I and the Standing Committee P, the Appeal Body does not benefit from free postage, despite all its dispatches being made by registered letter with confirmation of receipt.

Decisions are deliberated on a collegiate basis.

Applications submitted to this jurisdictional body are completely free of charge, unlike most other administrative bodies or courts. In addition, by law, the losing party is not ordered to pay any costs.

Finally, in 2020, a specific website was created for the Appeal Body: www.organederecours.be. This is designed to offer citizens, litigants and lawyers useful information to enable them to submit an appeal and conduct proceedings before the collegiate jurisdictional body.

X.2. THE FUNCTIONING OF THE JURISDICTIONAL BODY DURING THE PANDEMIC

The functioning of the Appeal Body was affected by the COVID-19 pandemic. In addition to the lockdown imposed from March 2020 onwards, the registry no longer received registered post from applicants or certain files due to postal problems. The Appeal Body had to cancel some hearings between 13 March and 27 May 2020 due to the lockdown and the closure of the Chamber of Representatives buildings, where hearings are usually held.

However, in order to ensure the proper functioning of the jurisdictional body and prevent a backlog, the Appeal Body increased the number of hearings post-lockdown. It held an average of more than three hearings per month in June, July, September and October 2020 instead of the usual two.

X.3. A SOMETIMES CUMBERSOME AND COMPLEX PROCEDURE

Despite the decrease in appeals submitted in 2020 (down from 196 in 2019 to 144 in 2020), the number of decisions issued in 2020 increased (from 166 in 2019 to 176 in 2020) (see below). The Appeal Body once again recorded an increase in its workload, due to the administrative management of cases, hearings and decisions becoming increasingly complex. The Appeal Body currently lacks sufficient capacity to prepare for its cases. Assistance in carrying out certain tasks in the future is needed in order to improve the jurisdictional body's functioning.

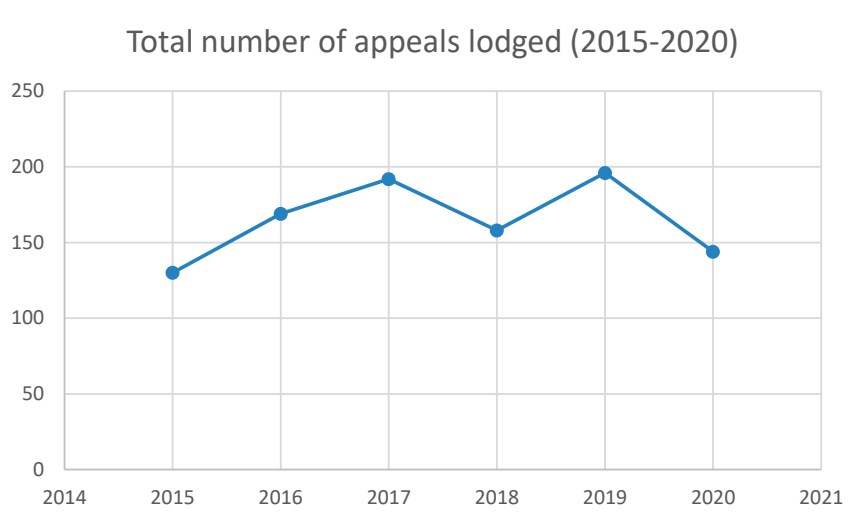
X.4. NO CHANGE TO THE LEGAL FRAMEWORK

In 2018 and 2019, the legal framework evolved considerably, both as regards the Classification and Security Clearances Act and the Appeal Body Act; by contrast, there were no legislative or regulatory initiatives in 2020.

X.5. 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 and the nature of the decisions of the Appeal Body within the various appeal procedures. For comparison purposes, the figures for the past five years have also been included.

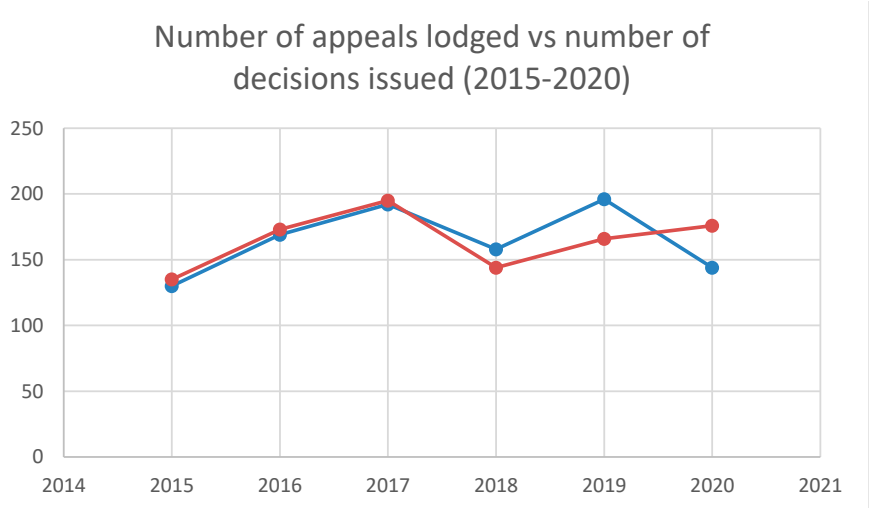
Table 1. Number of appeals lodged (2015-2020)



Overall, the number of appeals submitted to the Appeal Body has fallen in recent years. This overall decrease has three main explanations: first, the decline in appeals concerning security clearances (from 36 in 2018 to 51 in 2019 and to 32 in 2020). In addition, in contrast to the previous year, disputes relating to security advice have also decreased markedly (from 115 in 2019 to 99 in 2020). Finally, the number of appeals concerning the refusal of security certificates for the nuclear sector decreased from 17 in 2019 to 7 in 2020.

However, an important point should be made here: despite the decrease in appeals submitted in 2020, the number of decisions issued increased in 2020. The table below compares the number of appeals submitted and the number of decisions issued.

Table 2. Number of appeals lodged vs number of decisions issued (2015-2020)



The blue line refers to the number of appeals, whereas the red line refers to the number of decisions.

It is worth noting that for the first time the Appeal Body heard a case regarding the granting of a security certificate to an imam wishing to work in Belgian penal institutions on the basis of the provisions of the Royal Decree of 17 May 2019.[176]

A question was also brought before the Appeal Body concerning the granting of security advice for customs officers required to carry a weapon in the exercise of their duties, in accordance with the provisions of the Royal Decree of 15 December 2013.[177]

Similarly, for the first time, the Appeal Body deliberated on the granting of security advice for suppliers and subcontractors (and their staff) to the European institutions following a protocol concluded between the Foreign Affairs office and the European institutions.[178]

To the knowledge of the Appeal Body, the new security advice procedure described in the 2018 activity report has not been implemented yet. There has been

176 Royal Decree of 17 May 2019 on chaplains, religious service consultants and moral counsellors in prisons, *Belgian Official Journal*, 24 May 2019. (Article 3 § 3, 1°).

177 Royal Decree of 15 December 2013 identifying the services at the General Customs and Excise Administration where performing roles is subject to security verification, *Belgian Official Journal,* 19 December 2013.

178 On this subject, see the Royal Decree of 8 May 2018 determining the sectors of activity and the competent administrative authorities referred to in Article 22*quinquies*, § 7 of the Classification and Security Clearances Act which attributes to the official in charge of the FPS Foreign Affairs competence for the 'sector of activities' of the international institutions. A memorandum of understanding was concluded on 21 May 2019 between the FPS Foreign Affairs and the European institutions.

some talk of a desire for checks on the integrity and background of port personnel to be improved in the future. This new security advice procedure could be used in this connection.

Finally, 26 Appeal Body hearings were held in 2020.

Table 3. Security authorities concerned (2015-2020)

	2015	2016	2017	2018	2019	2020
National Security Authority	68	92	129	113	114	91
State Security	1	0	0	0	0	0
General Intelligence and Security Service	47	68	53	32	61	41
Federal Agency for Nuclear Control	10	8	7	10	17	7
Federal Police	3	1	3	3	3	4
Local Police	1	0	0	0	1	1
TOTAL	**130**	**169**	**192**	**158**	**196**	**144**

Table 4. Nature of the disputed decisions

	2015	2016	2017	2018	2019	2020
Security clearances (Art. 12 ff. Classification and Security Clearances Act)						
Confidential	9	5	1	2	5	0
Secret	35	38	33	31	39	27
Top secret	4	7	6	3	7	5
Refusal	36	28	30	26	39	23
Withdrawal	7	9	7	4	16	8
Refusal and withdrawal	0	0	0	0	0	0
Clearance for a limited period	3	4	1	1	3	0
Clearance for a lower level	0	1	0	0	0	0
No decision within time limit	2	7	2	5	0	0
No decision within extended time limit	0	1	0	0	0	0
Others						1[179]
SECURITY CLEARANCES SUBTOTAL	**48**	**50**	**40**	**36**	**51**	**32**

179 'Caution given to applicant'. One person had been granted security clearance for five years with a caution. He appealed against this caution.

	2015	2016	2017	2018	2019	2020
Security certificates for access to classified zones (Art. 22*bis*, para. 1 Classification and Security Clearances Act)						
Refusal	6	1	3	3	1	0
Withdrawal	0	0	0	0	0	0
No decision within time limit	0	0	0	0	0	0
Security certificates for a place or event (Art. 22*bis*, para. 2 Classification and Security Clearances Act)						
Refusal	12	9	20	15	12	6
Withdrawal	1	0	0	0	0	0
No decision within time limit	0	0	0	0	0	0
Security certificates for the nuclear sector (Art. 8*bis*, para. 2 Classification and Security Clearances Act)						
Refusal	-	7	7	11	17	7
Withdrawal	-	1	0	0	0	0
No decision within time limit	-	0	0	1	0	0
Security advice (art. 22*quinquies* Classification and Security Clearances Act)						
Negative advice	63	101	122	92	115	99
No advice	0	0	0	0	0	0
Retraction of positive advice	0	0	0	0	0	0
Normative legal acts of an administrative authority (Art. 12 Appeal Body Act)						
Decision by a public authority to request security certificates	0	0	0	0	0	0
Refusal by NSA to carry out verifications for security certificates	0	0	0	0	0	0
Decision by an administrative authority to request security advice	0	0	0	0	0	0
Refusal by NSA to carry out verifications for security advice	0	0	0	0	0	0
CERTIFICATES AND ADVICE SUBTOTAL	**82**	**119**	**152**	**122**	**145**	**112**
TOTAL DISPUTED DECISIONS	**130**	**169**	**192**	**158**	**196**	**144**

Table 5. Nature of the Appeal Body's decisions

	2015	2016	2017	2018	2019	2020
Security clearances (Art. 12 ff. Classification and Security Clearances Act)						
Appeal inadmissible	4	0	3	0	1	1
Appeal devoid of purpose	3	7	0	4	3	3
Appeal unfounded	19	18	13	12	12	16
Appeal well-founded (ful or partial adjudication)	24	24	24	12	25	14
Additional investigative actions by authority	0	2	0	1	1	2
Additional time for authority	1	2	1	1	0	3
Waiver of appeal granted	1	0	0	3	2	2
Security certificates for access to classified zones (Art. 22*bis*, para. 1 Classification and Security Clearances Act)						
Appeal inadmissible	0	0	1	0	0	0
Appeal devoid of purpose	0	0	1	0	0	0
Appeal unfounded	4	1	0	1	1	0
Appeal well-founded (adjudication)	2	1	1	0	3	0
Waiver of appeal granted	-	-	-	-	1	0
Security certificates for a place or event (Art. 22*bis*, para. 2 Classification and Security Clearances Act)						
Appeal inadmissible	0	0	1	2	4	2
Appeal devoid of purpose	0	0	1	0	0	0
Appeal unfounded	8	2	12	2	4	4
Appeal well-founded (adjudication)	10	4	7	3	4	1
Waiver of appeal granted	2	0	1	2	0	0

	2015	2016	2017	2018	2019	2020
Security certificates for the nuclear sector (Art. 8*bis*, para. 2 Classification and Security Clearances Act)						
Appeal inadmissible	-	1	1	0	1	0
Appeal devoid of purpose	-	1	0	1	0	0
Appeal unfounded	-	0	1	1	5	2
Appeal well-founded (adjudication)	-	7	5	6	7	4
Waiver of appeal granted	-	-	-	2	0	0
Security advice (art. 22*quinquies* Classification and Security Clearances Act)						
Appeal Body did not have jurisdiction	0	0	20[180]	12	0	0
Appeal inadmissible	6	15	10	3	7	8
Appeal devoid of purpose	0	0	1	3	1	6
Confirmation of negative advice	28	42	49	46	40	51
Conversion to positive advice	23	46	41	27	43	52
Waiver of appeal granted	0	0	1	0	1	5
Appeal against normative legal acts of an administrative authority (Art. 12 Appeal Body Act)	0	0	0	0	0	0
TOTAL	**135**[181]	**173**	**195**	**144**	**166**	**176**

180 The appeals in question had been lodged against (negative) security advice from the National Security Authority with regard to the personnel of subcontractors working at European institutions. The Appeal Body decided that there was no statutory basis for the advice formulated by the National Security Authority. 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.

181 There were two other specific decisions in which the waiver of an appeal was granted, bringing the total to 137 in 2015.

X.6. PROSPECTS

At the instigation of the chair, extensive reflections and actions were initiated to modernise the functioning of the Appeal Body. Several major objectives have been set: the simplification and standardisation of the procedure, the improvement of citizens' access to the jurisdictional body and the digitalised processing of files by the registry. Like other jurisdictional bodies, the Appeal Body is committed to simplifying its legal language.

On 24 November 2020, having first submitted it to the chairs of the Standing Committee P and of the Dispute Chamber of the Data Protection Authority, the Standing Committee I sent a legislative proposal to the Chamber of Representatives.

This draft is the outcome of the reflection process initiated years ago by the chair of the Appeal Body, and draws on the expertise of Mr Ivan Verougstraete, former President of the Court of Cassation. It suggests to set up a Council for Security Disputes by repealing the Act of 11 December 1998 establishing an Appeal Body for security clearances, certificates and advice. This jurisdictional body would replace the Appeal Body, and become a 'natural adjudicator' for security in matters concerning security clearances, certificates and advice as well as security guards and private detectives. This body's independence would be reinforced by the presence of three expert members: the Standing Committee I for matters relating to the 'Security Clearances Act' and 'Intelligence Act', the Standing Committee P for matters relating to the Policing Act and the Dispute Chamber of the Data Protection Authority for the protection of privacy. The text proposes a simplification of procedures and greater transparency, in particular by introducing the digitisation of files. The reform proposal should, if accepted, make it possible to lodge appeals electronically. In addition, the parties should be able to contact the registry through the same platform about their case. Approaches have been made to the bar to develop useful contacts to promote access for those wishing to take legal action. The new procedural rules will make the procedure smoother and more transparent by standardising the appeal time limits to a single time limit of thirty days: the current eight-day time limit (in relation to security certificates and advice) is too short to allow citizens to exercise their rights of defence properly. The interests of both the State and the citizens would be protected in this way. Finally, the proposal maintains the principle of free access for those wishing to take action.

The chair of the Appeal Body is examining the possibility of welcoming students or lawyers for internships.

It should also be noted that discussions are in progress concerning the publication of the decisions on the website. It is important for the case law of the Appeal Body to be accessible to all, as this marks an institution's transparent approach to the general public. Such publication would be anonymised, so as to consider the need to protect the major State interests, the secrecy of information or of a judicial investigation in progress, and the need to protect sources and the privacy of third parties. In addition, the Appeal Body is examining the idea of including a chronicle of case law on its website.

CHAPTER XI.

INTERNAL FUNCTIONING OF THE STANDING COMMITTEE I

XI.1. COMPOSITION OF THE STANDING COMMITTEE I

There were numerous changes of personnel in 2020. Serge Lipszyc (F), first substitute labour prosecutor at the Labour Court in Liège, who was sworn in in September 2018,[194] fulfilled his role as chair. Pieter-Alexander De Brock (N), whose first term expired in May 2019, was reappointed as counsellor in mid-January 2020.[195] At the end of November 2020, Laurent Van Doren, French-speaking counsellor to the Standing Committee I, informed the Chamber of Representatives of his resignation with effect from 31 December 2020.[196] Thibaut Vandamme (F), substitute public prosecutor for the district of Luxembourg, who had been appointed as first deputy member during the plenary session of 22 November 2018, agreed on 1 December 2020 to serve as a full member.[197]

At the beginning of January 2020, Registrar Wouter De Ridder exercised his pension rights. At the end of April 2020, the chair of the Committee sent a letter asking the Chamber to initiate the procedure for appointing a new registrar.[198] A call for applications for the appointment of the registrar of the Standing Committee I was published in the *Belgian Official Journal* in mid-May 2020.[199]

---

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

195 *C.R.I.* Chamber 2019-20, PLEN 020, 52.

196 *C.R.I.* Chamber 2020-21 PLEN 074, 47. On 24 September 2020, Linda Schweiger was appointed as first deputy member (*C.R.I.* Chamber 2019-20 PLEN055, 85) and on 29 October 2020, Wauter Van Laethem was appointed as second deputy member (*C.R.I.* Chamber 2019-20, PLEN 067, 16).

197 Under Article 30, paragraph 3 of the Review Act, if a deputy member's place falls vacant the Chamber must proceed without delay to the appointment of a new substitute member. The call for applications was published in the *Belgian Official Journal* on 18 December 2020. The first deputy member, Thierry Werts, was appointed during the plenary session of 20 May 2021 (*C.R.I.* Chamber, 2020-21, PLEN 105, 47). Michel Croquet remains the second deputy for the French-speaking member.

198 *C.R.I.* Chamber 2019-20, PLEN 038, 70.

199 At the time of finalisation of this activity report, the new registrar had not yet been appointed. On 21 June 2021, a bill was introduced with a view to broadening the conditions for the appointment of the registrars of the Standing Committees I and P (*Parl. doc.* Chamber 2021-21, 55-2064/001).

Changes also took place within the Investigation Service I: Frank Franceus left his position as director and was replaced by Fabian Poncelet (F), who also serves as security officer, and a new Dutch-speaking commissioner-auditor joined the service in September 2020.

Finally, the administrative staff of the Standing Committee I, under the direction of acting Registrar Wauter Van Laethem (N), also underwent some changes. In March 2020, a permanent Dutch-speaking legal specialist joined the Documentation and Legal Department, followed by a permanent French-speaking legal specialist in December 2020. The selection exams for the recruitment of a permanent Dutch-speaking secretary and a permanent French-speaking secretary were also held in 2020. At the end of 2020, the administrative staff had 18 employees.

XI.2. THE DATA PROTECTION OFFICER AT THE COMMITTEE

The Committee continued to use the services of the Data Protection Officer (DPO)[200], appointed for all processing of data that does not relate to 'national security'.

XI.3. MEETINGS WITH THE MONITORING COMMITTEE

In October 2019, the Chamber of Representatives amended the Chamber rules to change the composition of the Special Committee Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee. From now on, as many appointments as necessary are made so that each political group represented in the permanent committees has at least one member on the Monitoring Committee. Each political group that is not represented on the permanent committees appoints a non-voting member.[201] Following the federal elections of May 2019, the composition of the Monitoring Committee underwent some changes. The voting members were as follows: Peter Buysrogge (N-VA), Joy Donné (N-VA), Cécile Thibaut (Ecolo-Groen), Stefaan Van Hecke (Ecolo-Groen), André Flahaut (PS), Ahmed Laaouej (PS), Ortwin Depoortere (VB), Marijke Dillen (VB), Denis Ducarme (MR), Servais Verherstraeten (CD&V), Nabil Boukli (PVDA-PTB), Patrick Dewael (Open Vld)

200 The DPO is common to several institutions.

201 *Belgian Official Journal*, 25 October 2019. '*This modification of the regulations provides for a more restricted composition [of the monitoring commissions, i.e.] of the Committees P and I, which should increase their effectiveness*' (free translation), *C.R.I.* Chamber 2019-20, 17 October 2019, PLEN 009, 33.

and Bert Moyaers (Vooruit). In mid-October 2020, Eliane Tillieux (PS) succeeded Patrick Dewael (Open Vld) as President of the Chamber. Georges Dallemagne (cdH) participates as a non-voting member.

In the course of 2020, and despite the public health crisis, several meetings were held with the Monitoring Committee. On 2 March 2020, just before the outbreak of the public health crisis, the members of the Monitoring Committee attended a working meeting in the offices of the Standing Committee I. The objective of this meeting was to introduce the new members of the Monitoring Committee to the Committee's activities and to engage in a more in-depth exchange of views with familiar faces.

Several review investigations completed by the Standing Committee I were discussed at other Monitoring Committee meetings, behind closed doors. Were also discussed the annual report on the use of specific and exceptional methods by the intelligence services and on the Committee's oversight over the use of these methods (Art. 35 of the Review Act), as well as the report drawn up in the context of its supervisory competence – jointly with the Supervisory Body for Police Information (C.O.C.) – for databases (Art. 44/6 of the Policing Act). The Activity Report 2019 of the Standing Committee I was discussed on 16 December 2020.[202] The Monitoring Committee underlined '*the high quality of the annual report, which provides a complete picture of the activities of the Committee I*' (free translation). A series of themes particularly drew the attention of the MPs, such as the monitoring of sects, the shortage of personnel within the intelligence services, the challenges regarding security clearances, the activities of the Appeal Body, and the follow-up on recommendations. By way of conclusion, the Commission '*took note of the activity report 2019 of the Committee I and concurred with its recommendations*' (free translation).[203]

XI.4. FINANCIAL RESOURCES AND ADMINISTRATIVE ACTIVITIES

The Standing Committee I's 2020 budget was set at €4.615 million, up 9.5% on the 2019 budget.

In addition to normal cost increases (indexing, etc.), this increase was due to the Parliament's approval of two projects: first, the digitisation of work processes and means of communication (website), and second, an overhaul of the administrative

---

202 The Commission refers in this context to Article 66*bis*, § 2, of the Review Act, as amended by the Act of 6 January 2014 amending various institutional reform acts, *Belgian Official Journal*, 31 January 2014.

203 *Parl. doc.* Chamber 2020-21, 55-1689/001, 29 December 2020 (Activity Report 2019 of the Standing Intelligence Agencies Review Committee, produced on behalf of the Special Committee Entrusted with the Parliamentary Monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee).

staff with a view to adapting the profile of future employees to the changing nature of the Committee's roles, for which more operational staff and fewer support staff are required.

XI.5. IMPLEMENTATION OF THE RECOMMENDATIONS FROM THE COURT OF AUDIT

In 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. This included the Standing Committee I. The Court of Audit focused primarily on budgetary aspects (an analysis of income and expenditure) and on delineating the tasks of the various institutions. Ernst and Young's main assignment was to further analyse the processes, systems and organisational structure in each of these institutions. The audit report[204] formulated recommendations about the 'assignments' of the nine institutions entitled to appropriations covered by the audit was submitted at the end of March 2018. The common feature in the assignments of these institutions '*lies in the aim of achieving better legal protection for citizens by exercising various forms of oversight in specific policy areas*' (free translation).

In mid-November 2020, for the follow-up audit of the institutions by the Court of Audit, the Accounts Committee asked the services of the College of Quaestors to draw up a report on the implementation of these recommendations. A request was also made to look at how additional synergies could be implemented in order to achieve further savings and efficiencies.

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.[205] Given the strict measures dictated by the public health crisis, it was not possible to attend external training courses in 2020. A limited number of internal briefings were organised, however, at which experts briefed the Committee on current and important topics within the wider intelligence community.

---

204 *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.

205 The security briefings that employees are required to attend took place.

CHAPTER XII.
RECOMMENDATIONS

Based on the review investigations, controls and inspections concluded in 2020, the Standing Committee I has formulated the following recommendations. In 2020, these relate in particular to the coordination and efficiency of the intelligence services, CUTA and the supporting services, and the optimisation of the review capabilities of the Standing Committee I.

XII.1. RECOMMENDATIONS RELATED TO THE COORDINATION AND EFFICIENCY OF THE INTELLIGENCE SERVICES, CUTA AND THE SUPPORTING SERVICES

XII.1.1. VARIOUS RECOMMENDATIONS FOLLOWING THE JOINT REVIEW INVESTIGATION OF CUTA AND ITS SUPPORTING SERVICES[194]

XII.1.1.1. Better internal communication and information sessions for seconded experts

Better internal communication, in particular between the various departments of CUTA, would make it easier to know who does what, including for seconded experts. Similarly, a regularly updated list of staff members and their respective competencies would add value and should be circulated among staff.

During the investigation, it was noted that seconded experts (from the Punctual Analysis Department) rarely if ever visit their departments of origin, and some of them do not have much contact with these departments. A training or information session allowing them to update their knowledge of their original department and any (e.g. legislative or organisational) changes would also add value.

194 See Chapter I.1. 'Supporting services of the CUTA'.

XII.1.1.2. Optimisation of contacts between CUTA and its supporting services

When direct contact is established between the supporting service and CUTA, the official point of contact of the supporting service has to be informed via their functional mailbox, copying them in to any exchange of information. The aim is to minimise any loss of information.

In case of bilateral contacts between staff members of CUTA and of the supporting service, it is important to ensure continuity if one of the last mentioned leaves or is absent, to avoid a loss of (quality in the flow of) information.

Regarding the supporting services where the flow of information is limited, synergy should be developed between CUTA and the point of contact to raise staff awareness of CUTA' s roles across, as far as possible, the various departments of the service (by means of information sessions, for example). It is up to the supporting services to take initiatives to raise the awareness among their staff.

XII.1.1.3. Compliance with legal obligations by the Customs and Excise Administration

Although the Customs and Excise Administration – Investigations and Research Section (FPS Finances) considers its collaboration with CUTA to be of little value and does not see what information it could provide, this administration is a legally designated point of contact for CUTA. It is therefore up to this service to perform an internal analysis to establish what kinds of collected information could prove useful for CUTA. On this basis, another point of contact may possibly be designated within Customs and Excise.

In addition, the FPS Customs and Excise Administration – Investigations and Research Section must take the appropriate measures to comply with the legal required minimum standards for the storage and consultation of classified documents.

XII.1.2. VARIOUS RECOMMENDATIONS RELATED TO THE REVIEW INVESTIGATION OF THE MONITORING OF THE FAR-RIGHT[195]

XII.1.2.1. Recommendations regarding the political definition of the intelligence objective

The various services responsible for monitoring the far-right/right-wing extremism should aim to use a common and uniform terminology. This would have a positive impact on data exchange and cooperation. They should also define the most objective possible criteria for determining which individuals and/or groups need to be monitored by them.

Several options are available to the legislative and executive branches:

- legislators could consider providing a better description[196] of the concept of 'extremism' in the Act of 30 November 1998 governing the intelligence and security services (Intelligence Services Act) and a precise definition of the term 'right-wing extremism' (and by extension 'left-wing extremism'). Other concepts such as 'nationalism' could also be included;
- or the National Security Council (NSC) could take the lead, as stipulated in the Royal Decree establishing this body;
- or the competent ministers could take the lead and give clear instructions on how to regard the threat.

In all these cases, the services participating in the Far-Right Working Group could be asked to adopt a common approach. Moreover, a theoretical paradigm already exists in this connection. CUTA is well-positioned to work together with the services to reach a conclusion, which could then be formalised at a higher level.

It is also necessary to measure the extent of the threat. The intelligence services are not alone in collecting or being able to collect information on this subject. Compiling statistics in this area is not the sole responsibility of the intelligence services. For example, collaboration and coordination with the police services and public prosecutors' offices is necessary to collect figures on politically and ideologically motivated offences. The Far Right Working Group of the Radicalism Action Plan can play, under the direction of the NSC, a key role in determining the contribution of each party.

---

195 See Chapter I.7., 'Monitoring of the far-right by the Belgian intelligence services'.

196 In this regard, State Security rightly points out that a clear definition has both advantages and disadvantages: it creates a good, up-to-date framework, but the definition needs to be flexible enough to encompass existing and future phenomena.

XII.1.2.2. Recommendations regarding organisation and planning

The Standing Committee I recommends that the intelligence services assess whether their internal planning (operational and tactical) is adequate for achieving their strategic objectives and whether the resources available are proportionate to the threat. However, a clear description of the phenomenon and its extent are first needed (see recommendation above).

XII.1.2.3. Recommendations regarding collection and processing

The Standing Committee I recommends that by the creation of its database, State Security should make it possible to search and gather information using the 'Subject, Issue, Geography' axes (or a comparable process, since State Security intends to replace the database).

For GISS, the Standing Committee I recommends the service develop a more independent HUMINT position and assign more source managers to it. The service must also investigate and address the causes for the slow flow of information and the delay in inputting to the database.

XII.1.2.4. Recommendations regarding analysis, dissemination and cooperation

Together with CUTA, the services must investigate ways to perform more general analyses of the phenomenon. State Security and CUTA must agree – possibly within the framework of the Action Plan R – on how the tasks should be assigned.

State Security has a tool for assessing a person's degree of radicalisation and level of violence. It lacks the staff needed to make full use of this tool, which requires a huge quantity of information (about fifty indicators). According to State Security, this tool is not suited to detect lone actors. It is therefore necessary to examine whether it could be simplified and whether other methods would enable better detection of lone actors. In other services (for example at CUTA), other tools are in use or under study.

The Standing Committee I believes that increased cooperation and coordination is needed between the services in the development and use of such tools, as well as in training related to their use. The Committee also feels that such tools, which can help in detecting and assessing threats, must be systematically used to monitor all forms of extremism, and that the necessary personnel resources must be deployed. This is especially the case as the intelligence services claim that potential terrorist acts perpetrated by lone actors currently constitute the main threat from the far right.

Finally, concerning the awareness regarding the threat (or its seriousness) on the part of various actors in society, State Security, and, *a fortiori* GISS, have taken few initiatives. Given the political nature of the threat, it goes without saying

that any intervention by these services in public forums must be covered by the National Security Council or by the competent ministers.

XII.1.2.5. Recommendations regarding feedback

The Standing Committee I recommends that both services explicitly and periodically request feedback from the recipients of intelligence. It is up to these recipients to respond so that the services can refine and orient their intelligence objectives.

XII.1.3. APPLICATION OF THE DIRECTIVE ON THE RELATIONS OF THE BELGIAN INTELLIGENCE SERVICES WITH FOREIGN INTELLIGENCE SERVICES[197]

On 26 September 2016, the directive on the relations of the Belgian intelligence services with foreign intelligence services was adopted. However, the transmission of personal information/data to foreign services was only discussed cursorily. The Committee therefore stands by its previous recommendations and considers it a priority to set up an initiative in this area. In this respect, prudence must prevail in the context of exchanges of information engaged in by the intelligence services.

The directive aims to assess cooperation with foreign intelligence services with a view to determining the nature of the relationship with each of these services Provision should be made for a joint assessment, in particular concerning the 'obstacles' criterion, when the foreign partner is working with State Security and GISS.

If at some point there were to be implications concerning the protection of personal data (because the United Kingdom was to have diverged from the GDPR rules), it will be up to the intelligence services dealing with the situation to bring the matter in front of the competent national authorities (the competent ministers and the various data protection authorities).[198]

In addition, GISS should invite the Minister of Defence to adapt, together with the Minister of Justice, the directive of 26 September 2016 to make require a ministerial agreement prior to any (formal or informal) collaboration with a (state or non-state) foreign partner.

---

197 These recommendations derive from Chapter I.3.'Brexit and the relationship between Belgian and British intelligence services' and Chapter I.5.,'. The Memorandum of Understanding (MOU) between GISS and the Rwandan intelligence services'.

198 Conversely, if national authorities are aware of consequences arising from Brexit which affect the intelligence services, they should ideally inform those services in good time and possibly involve them in discussions.

Finally, GISS must, within two years, assess all of its international relations in light of the ministerial directive of 26 September 2016. This assessment must include the factors on which the categorisation is based. The biannual assessment of the cooperation with foreign intelligence services and the monitoring of the cooperation must be carried out systematically, in accordance with the directive of 26 September 2016.

XII.1.4. APPLICATION OF ARTICLE 20 OF THE INTELLIGENCE SERVICES ACT

It is recommended that GISS invites the Minister of Defence to introduce, together with the Minister of Justice, a bill to adapt Article 20 of the Intelligence Services Act in order to ensure linguistic correspondence between French and Dutch.

XII.1.5. MINISTERIAL AGREEMENT PRIOR TO THE CONCLUSION OF COOPERATION AGREEMENTS AND SYSTEMATIC CLASSIFICATION

The Standing Committee I recommends that GISS should systematically ensure that prior ministerial agreement is obtained, without waiting for the amendment of the directive. GISS has already undertaken to do so with regard to MoUs.[199]
In addition, new MoUs with foreign partners must be systematically classified in accordance with the Act of 11 December 1998.

XII.1.6. CONCLUSION OF A COOPERATION AGREEMENT BETWEEN STATE SECURITY AND GISS

The Standing Committee I recommends that the National Security Council and the two intelligence services implement the obligation set out in Article 20 § 4 of the Intelligence Services Act[200] to draw up a directive and a cooperation agreement respectively. The Standing Committee I believes that the model of a Joint Intelligence Task Force

---

199 The Standing Committee I was informed that GISS was developing plans in connection with the conclusion of MoUs, the management of its strategic relations and the process associated with its international contacts. The Committee will assess the execution of these plans in the year following these recommendations.

200 *'In order to perform the roles described in Article 7, 3° /1 and Article 11, § 1, 5°, State Security and the General Intelligence and Security Service shall conclude a cooperation agreement on the basis of directives obtained from the National Security Council.'* The roles are '*collecting, analysing and processing intelligence relating to the activities of foreign intelligence services on Belgian territory*' (free translations).

is a successful initiative that could be applied to other areas in the future. However, both State Security and GISS must take account of the project's drawbacks, as identified in their internal assessments.

XII.1.7. AUTOMATED TOOLS FOR MONITORING SOCIAL MEDIA

The Standing Committee I has found that the monitoring of social media by the intelligence services remains a highly laborious process.[201] The services currently lack enough automated tools to take a more efficient approach. The Committee believes it is necessary to invest in this area in the future, given the growing importance of social and alternative media in the dissemination of propaganda and disinformation aimed at influencing public opinion.

XII.1.8. COMPLIANCE WITH DISCIPLINARY AND JUDICIAL PROCEDURES BY GISS (DURING FOREIGN MISSIONS)

Following incidents that occurred in an unspecified operations zone abroad[202], the Standing Committee I recommended various punctual measures (regarding in particular the use of sources) be taken in order to ensure the safety of troops deployed on the ground.

It is recommended that GISS comply scrupulously with the disciplinary and judicial procedures in force.

The Committee also reiterates a previous recommendation[203] that GISS should produce a comprehensive report of every security incident that examines and analyses all dimensions (not only technical, but also in relation to conduct), especially if one of the parties involved holds a security clearance. This report must be forwarded to the competent security authority, together with a suggested decision.

---

201 See Chapter I.6. 'Information and communication technologies in the intelligence process at GISS'.

202 See Chapter I.10. 'Incidents in a foreign operations zone'.

203 STANDING COMMITTEE I, *Activity Report 2015*, 179.

XII.2. RECOMMENDATIONS RELATED THE EFFECTIVENESS OF THE REVIEW

XII.2.1. STRICT COMPLIANCE WITH ARTICLE 33 OF THE REVIEW ACT BY GISS

The Standing Committee I again stresses that GISS is required to comply with Article 33 of the Review Act. In particular, it is recommended that GISS systematically transfer to the Committee all memorandums of understanding and corresponding ministerial authorisations, as well as ministerial approvals in the event of informal cooperation.

XII.2.2. INTRODUCTION OF AN INTERNAL MONITORING SYSTEM BY GISS

The Standing Committee I recommends that GISS puts in place an internal monitoring system to ensure compliance with all procedures relating to international relations.

XII.2.3. REMINDER OF THE APPLICATION OF ARTICLE 38 OF THE REVIEW ACT

Article 38 of the Review Act provides for two forms of communication from the judicial authorities to the chair of the Standing Committee I.

First of all, it states that the prosecutor-general and the auditor-general send the chair of the Standing Committee I a copy of any decisions and final judgments relating to crimes or offences committed by members of the intelligence services or of CUTA. The second paragraph states that the prosecutor-general, the labour prosecutor, the federal public prosecutor or the prosecutor-general at the Court of Appeal, as the case may be, must inform the chair of the Standing Committee I whenever a preliminary or full investigation relating to a crime or offence is opened against a member of an intelligence service or of CUTA.

COL 8/2014 specifies that this communication must be 'systematic'.

Yet, this obligation (mainly the second paragraph) is not always adhered to.[204]

---

[204] College of Prosecutors-General Circular (COL 08/2014) on the communication of information concerning or prosecutions or convictions of public officials and persons in positions of public interest where those positions involve a habitual relationship of authority with minors or vulnerable persons was revised on 9 January 2020 (free translation).

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 2022)

CHAPTER I - GENERAL PROVISIONS

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

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

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

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

The review referred to in this Act is governed without prejudice to the review or inspection governed by or by virtue of other legislation. In the event of review or inspection governed by or by virtue of other legislation, the review referred to in this Act relating to the activities, methods, documents and directives of the police

services and of the intelligence and security services, shall only be undertaken to ensure fulfilment of the assignments provided for in this Act.

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

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

Shall be equated to police services for the purposes of this Act, the people who are individually authorised to detect and establish criminal offences.

CHAPTER II - REVIEW OF THE POLICE SERVICES

This chapter that concerns review of the police services by the Standing Committee P is not reproduced.

CHAPTER III - REVIEW OF THE INTELLIGENCE SERVICES

SECTION 1 – THE STANDING INTELLIGENCE AGENCIES REVIEW COMMITTEE

Subsection 1 - Composition

Art. 28

The Standing Intelligence Agencies Review Committee, hereinafter referred to as the "Standing Committee I", shall consist of three full members, including a Chairman. Two substitutes shall be appointed for each of them. They shall all be appointed by the Chamber of Representatives, who may dismiss them if they perform one of the functions or activities or hold one of the positions or mandates referred to in paragraph 4, or for serious reasons.

The Standing Committee I shall be assisted by a registrar. In his absence, the Standing Committee I shall provide for his replacement in accordance with the terms defined in the rules of procedure referred to Article 60.

At the time of their appointment, the members and their substitutes shall satisfy the following conditions:

1° Be Belgian;
2° Enjoy civil and political rights;
3° Have attained the age of 35 years;
4° Reside in Belgium;
5° Hold a Master's degree in Law and demonstrate at least seven years' relevant experience in the field of criminal law or criminology, public law, or management techniques, acquired in positions related to the operation, activities and organisation of the police services or of the intelligence and security services, as well as having held positions requiring a high level of responsibility;
6° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

The members and their substitutes may not hold a public elected office. They may not perform a public or private function or activity that could jeopardise the independence or dignity of the office. They may not be members of the Standing Police Services Review Committee, nor of a police service, an intelligence service, the Coordination Unit for Threat Assessment, or another supporting service, nor another data protection authority, nor the administrative commission responsible for monitoring the specific and exceptional intelligence collection methods used by the intelligence and security services.

The Chairman shall be a magistrate.

The decisions assigned to the Standing Committee I by this Act or other acts shall be taken in plenary session.

Art. 29

The registrar shall be appointed by the Chamber of Representatives, who may dismiss him or terminate his appointment in the cases referred to in Article 28, paragraph 4. At the time of his appointment, the registrar shall satisfy the following conditions:

1° Be Belgian.
2° Enjoy civil and political rights;
3° Have knowledge of the French and Dutch languages;
4° Have attained the age of 30 years;
5° Reside in Belgium;
6° Hold a Master's degree in Law relevant to the exercise of the function;
7° Have at least two years' relevant experience;
8° Hold a top secret level security clearance in accordance with the Act of 11 December 1998 on classification and security clearances.

Before taking up his duties, the registrar shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Chamber of Representatives.

Art. 30

The members of the Standing Committee I and their substitutes shall be appointed for a renewable term of six years starting from the time they take their oath. At the end of this term, the members shall remain in office till their successors have taken their oath.

The substitutes shall be appointed for a renewable term of six years starting from the time the member whom they are replacing took his oath.

A member whose mandate ends before the expiry of the term of six years shall be replaced for the remaining period of the mandate by his first substitute or if the latter relinquishes this position, by his second substitute. If a position of substitute member should become vacant, the Chamber of Representatives shall appoint a new substitute member forthwith.

For the appointment of a substitute member, the conditions laid down in Article 28, paragraph 4, shall be verified by the Chamber of Representatives upon taking up his duties.

Before taking up their duties, the members of the Standing Committee I shall take the oath prescribed by Article 2 of the decree of 30 July 1831 before the President of the Chamber of Representatives.

Subsection 2 - Definitions

Art. 31
§1. For the purposes of this chapter, "the competent ministers" shall mean:

1° The minister responsible for National Defence, with regard to the General Intelligence and Security Service;
2° The minister responsible for Justice, with regard to State Security;
3° The minister responsible for a service referred to in Article 3, 2°, in fine;
4° The minister responsible for the Interior, with regard to the assignments of State Security relating to the maintenance of law and order and the protection of people, as well as the organisation and administration of State Security when that organisation and administration have a direct influence on the execution of assignments relating to the maintenance of law and order and the protection of people;
5° The National Security Council, with regard to the Coordination Unit for Threat Assessment or the other supporting services.

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

Subsection 3 - Assignments

Art. 32
The Standing Committee I shall act either on its own initiative, or at the request of the Chamber of Representatives, the competent minister or the competent authority, or at the request of another data protection authority.

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

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

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

The intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services shall, on their own initiative, send to the Standing

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

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

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

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

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

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

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

Art. 34

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

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

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

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

When the investigation is closed, the results shall be communicated in general terms, except in the case of investigations relating to the processing of personal data by the intelligence services and their processors. The Standing Committee I shall merely inform the complainant that the necessary verifications have been made.

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

Art. 35

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

1° Annually, through a general activity report, which shall include, if applicable, conclusions and proposals of a general nature, and which shall cover the period from 1 January to 31 December of the preceding year. This report shall be sent to the Presidents of the Chamber of Representatives and the Senate, and to the competent ministers by 1 June at the latest. In this report, the Standing Committee I shall pay special attention to the specific and exceptional methods for gathering information, as referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, as also to the application of Chapter IV/2 of the same Act and to the implementation of the Act of 10 July 2006 on threat assessment.

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

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

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

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

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

§ 3. The Standing Committee I shall present an annual report annually to the Chamber of Representatives regarding the advice provided as a data protection authority on the investigations conducted and the measures taken in this quality and regarding its collaboration with other data protection authorities. A copy of this report will also be provided to the competent ministers as well as State Security, the General and Security Service which are entitled to draw the attention of the Standing Committee I on their remarks.

Art. 36

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

Art. 37

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

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

Art. 38

The prosecutor-general and the auditor-general shall ex-officio send to the Chairman of the Standing Committee I a copy of the judgments and judicial decisions relating to the crimes or offences committed by the members of the intelligence services and the Coordination Unit for Threat Assessment.

The public prosecutor, the labour prosecutor, the federal prosecutor or the prosecutor-general of the Court of Appeal, depending on the case, shall inform the Chairman of the Standing Committee I whenever a criminal or judicial

investigation into a crime or offence is initiated against a member of an intelligence service or the Coordination Unit for Threat Assessment.

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

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

The copies shall be delivered without charge.

Art. 39

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

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

SECTION 2 – THE INVESTIGATION SERVICE FOR THE INTELLIGENCE SERVICES

Art. 40

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

It shall examine the complaints and denunciations of individuals who have been directly concerned by the intervention of an intelligence service, the Coordination Unit for Threat Assessment or another supporting service. Any public officer, any person performing a public function, and any member of the armed forces directly concerned by the directives, decisions or rules applicable to them, as well as by the methods or actions, may lodge a complaint or file a denunciation without having to request authorisation from his superiors.

On its own initiative or at the request of the competent public prosecutor, military public prosecutor or examining magistrate, it shall, together with the other officers and agents of the judicial police, and even with a right of priority over them, investigate the crimes and offences which the members of the intelligence

services and the Coordination Unit for Threat Assessment are charged with. With regard to the members of the other supporting services, this provision only applies with respect to the obligation laid down by Articles 6 and 14 of the Act of 10 July 2006 on threat assessment.

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

Art. 41

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

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

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

He must have knowledge of the French and Dutch languages.

He shall retain his right to advancement and salary increase.

He may be dismissed by the Standing Committee I.

Art. 42

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

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

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

Art. 43

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

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

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

Art. 44
The members of the Investigation Service I shall be appointed and dismissed by the Standing Committee I on the recommendation of the Head of the Investigation Service I.

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

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

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

Art. 45
The Head and the members of the Investigation Service I shall have the capacity of judicial police officer, assistant public prosecutor and assistant military public prosecutor.

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

Art. 46
When a member of the Investigation Service I has knowledge of a crime or offence apart from the cases referred to in article 13/1 of the Act of 30 November 1998 governing the intelligence and security services and those referred to in articles 226, 227 and 230 of the Data Protection Act, he shall produce a formal report that is forthwith sent by the Head of the Investigation Service I to the public prosecutor, to the military public prosecutor, or the examining magistrate, depending on the case.

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

When a member of the Investigation Service I learns of an offense referred to in articles 226, 227 and 230, he shall inform the Standing Committee I as soon as possible. The latter shall follow it up within the procedures established.

Art. 47
When a member of the Investigation Service I observes facts during an investigation that could constitute a disciplinary offence, the Head of the Investigation Service I shall forthwith inform the competent disciplinary authority thereof.

SECTION 3 – INVESTIGATION PROCEDURES

Art. 48

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

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

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

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

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

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

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

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

The members or former members of the intelligence services, the Coordination Unit for Threat Assessment, and the other supporting services who refuse to testify

before the Standing Committee I, and the experts and interpreters who refuse to collaborate, shall be liable to imprisonment of between one month and one year.

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

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

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

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

SECTION 4 – POWERS OF THE STANDING COMMITTEE I AS DATA PROTECTION AUTHORITY

Art. 51/1
As data protection authority, the Standing Committee I acts either on its own initiative, or at the request of another data protection authority, or at the request of any data subjects.

Art. 51/2
To be admissible, the request is written, dated, signed and reasoned, and justify the identity of the person concerned.

Art. 51/3
In the follow-up of the cases, the Standing Committee I has the authority to:

1° conclude that the processing is carried out in accordance with the provisions of the regulations relating to the processing of personal data;
2° warn the service concerned or its processors that an intended processing of personal data is likely to violate the regulations relating to the processing of personal data;
3° call to order the service concerned or its processors when processing has resulted in a violation of a provision of the regulations relating to the processing of personal data;
4° order the service concerned or its processors to bring processing in accordance with the provisions of the regulations relating to the processing of personal data, where appropriate, in a specific manner and within a specified period;
5° impose a temporary or permanent limitation, including a ban, on processing;
6° order the rectification or erasure of personal data;
7° forward the case to the Brussels public prosecutor's office, who informs him of the actios taken on the case.

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

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

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

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

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

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

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

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

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

CHAPTER V - COMMON PROVISIONS

Art. 56
Each Standing Committee shall examine the complaints that are lodged with it by its former members or by former members of the Investigation Services who

believe they have been subject to prejudicial measures because of the functions they have carried out in the Standing Committees or in the Investigation Services.

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

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

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

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

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

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

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

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

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

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

In accordance with paragraph 2, the Chamber of Representatives may amend the rules of procedure after acquiring the advisory opinion of the Standing

Committee concerned. The advisory opinion shall be deemed favourable if it has not been given within sixty days of the request.

Art. 61

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

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

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

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

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

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

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

The following are excluded from this allowance:

1° The members to which Article 65 applies.

2° The members who were members of a police service or an intelligence and security service before their appointment to the Standing Committee and who integrate this service.

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

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

Art. 61*bis*
The Chairman of each Standing Committee shall, in accordance with the principle of collective responsibility, preside the meetings of that Committee and assume the day-to-day management of its activities. He shall ensure the application of the rules of procedure, the proper functioning of the Committee, as well as the proper performance of its assignments. He shall also ensure that the performance of the judicial police assignments does not impede the performance of the investigations. To this end, he shall hold the necessary consultations with the competent judicial authorities.

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

Art. 62
Without prejudice to Article 58, the registrar shall act under the collegial authority and the supervision of the Standing Committee in question, the registrar of each Committee shall among others manage the following:

- the administrative staff;
- the infrastructure and equipment of the Committee;
- the secretariat of the Committee meetings and the minutes of the meetings;
- the sending of documents;
- the preservation and protection of the secrecy of the documentation and archives.

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

Art. 63
The members of the Standing Committees are prohibited from attending the deliberations on affairs in which they have a direct or personal interest, or in which relatives by blood or marriage to the fourth degree inclusive, have a direct or personal interest.

Art. 64
The members of the Standing Committees, the registrars, the members of the Investigation Services, and the administrative staff shall be obliged to preserve the secrecy of the information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Without prejudice to Article 458 of the Penal Code, they shall be liable to imprisonment of between eight days to one year, and a fine between one hundred francs and four thousand francs, or only one of these penalties, if they divulge

these secrets in circumstances other than those stipulated by law or by the rules of procedure.

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

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

Art. 66
Excluding its Chairman, each Standing Committee shall have as many French-speaking members as Dutch-speaking members.

The Chairman of one of the Standing Committees shall be French-speaking, the Chairman of the other Dutch-speaking.

Art. 66*bis*
§1. The Chamber of Representatives shall create a permanent committee responsible for monitoring the Standing Committee P and the Standing Committee I.

The Chamber of Representatives shall stipulate in its regulation, the rules relating to the composition and functioning of the monitoring committee.

§2. The monitoring committee shall supervise the operation of the Standing Committees, and ensure observance of the provisions of this Act and the rules of procedure.

The monitoring committee shall also perform the assignments assigned to the Chamber of Representatives by Articles 8, 9, 11, 1°bis, 2° and 3°, 12, 32, 33, 35, § 1, 2° and 3°, 36 and 60.

§3. The monitoring committee shall meet at least once per quarter with the President or the members of each Standing Committee. The monitoring committee can also meet at the request of the majority of its members, at the request of the Chairman of one Standing Committee, or at the request of the majority of the members of a Standing Committee.

Every denunciation by a member of a Standing Committee relating to the inadequate functioning of that Standing Committee, the non-observance of this Act, or the rules of procedure, may be brought before the monitoring committee.

The monitoring committee may issue recommendations to each Standing Committee, or to each of its members, relating to the functioning of the Standing Committee, the observance of this Act, or the rules of procedure.

§4. The members of the monitoring committee shall take the necessary measures to safeguard the confidential nature of the facts, acts or intelligence that they have

knowledge of by virtue of their position, and shall be subject to an obligation of confidentiality. They shall be obliged to preserve the secrecy of any information that comes to their attention in the performance of their duties. The obligation of confidentiality shall also apply after they leave office.

Any violation of this obligation of confidentiality shall be penalised in accordance with the rules of the Chamber of Representatives.

30 NOVEMBER 1998
ACT GOVERNING THE INTELLIGENCE AND SECURITY SERVICES
(*extract*)

TITLE I
GENERAL PROVISIONS

(…)

[TITLE IV/2

A POSTERIORI CONTROL OF THE SPECIFIC AND EXCEPTIONAL METHODS FOR THE GATHERING OF INTELLIGENCE BY THE INTELLIGENCE AND SECURITY SERVICES

Article 43/2
Without prejudice to the competences defined in Article 1 of the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment and in Article 44 of the Act of 30 November 1998 on the intelligence and security services, the Standing Committee I is also called on to conduct a posteriori control of the specific and exceptional intelligence gathering methods used by the intelligence and security services as referred to in Article 18/2.

The Standing Committee I shall rule on the legality of decisions made regarding these methods, as well as on compliance with the principles of proportionality and subsidiarity, set out in Articles 18/3, § 1, first paragraph, and 18/9, §§ 2 and 3.

Article 43/3
All decisions, opinions, authorisations and confirmations concerning the specific and exceptional intelligence gathering methods shall be reported immediately by the competent authority to the Standing Committee I, in accordance with further rules to be determined by the King.

Article 43/4
The Standing Committee I shall operate:

- either on its own initiative;
- or at the request of the Privacy Commission, in accordance with further rules to be defined by the King, in a decree deliberated in the Council of Ministers, following the opinions of that Commission and of the Standing Committee I;
- or as the result of a complaint, which must be submitted in writing on pain of invalidity, stating the grievance, from anyone who can show a personal and legitimate interest, unless the complaint is clearly unfounded;
- on any occasions where the Commission has suspended use of a specific or exceptional method on the grounds of illegality or not permitted the use of intelligence on the grounds of the unlawful use of a specific or exceptional method;
- whenever the competent minister has taken a decision on the basis of Article 18/10, § 3.

The Standing Committee I shall rule within one month following the day on which the case was referred to it in accordance with the first paragraph.

A decision by the Standing Committee I not to follow up a complaint shall be justified and the complainant shall be notified.

Unless the Standing Committee I rules otherwise, its control shall not have suspensive effect.

Article 43/5
§ 1. Control of the exceptional intelligence gathering methods is conducted inter alia on the basis of the documents provided by the Commission in accordance with Article 18/10, § 7, and of the special register referred to in Article 18/17, § 6, which is kept continuously available to the Standing Committee I, and on the basis of any other relevant document provided by the Commission or for which the Standing Committee I is required to be consulted.

Control of the specific intelligence gathering methods is conducted on the basis of any relevant document provided by the Commission or for which the Standing Committee I is required to be consulted.

The Standing Committee I shall have access to the complete dossier compiled by the intelligence and security service involved, as well as to that of the Commission and may require the intelligence and security service involved and the Commission to provide any additional information which it deems useful for the control to which it is authorised. The intelligence and security service involved and the Commission are required to follow up this request immediately.

§ 2. The Standing Committee I may entrust investigation assignments to the Investigation Service of the Standing Committee I. In this context this service may

employ all the powers granted to it under the Act of 18 July 1991 governing review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

§ 3. The complainant and his lawyer may consult the dossier at the secretariat of the Standing Committee I, for a period of five working days, on the days and times notified by the Committee. This dossier shall contain all information and intelligence relevant to this case, except for those which would breach the protection of sources, the protection of the privacy of third parties, the classification rules set out in the Act of 11 December 1998 on classification and security clearances, certificates and advice, or which would prevent the execution of the assignments of the intelligence and security services referred to in Articles 7 and 11.

The intelligence and security service involved shall be given the opportunity to voice its opinion on the information included in the dossier provided for consultation.

Except if it is likely to jeopardise the assignments of the intelligence and security services, the dossier made available to the complainant and his lawyer shall in any event include the following:

1° the legal basis justifying use of the specific or exceptional intelligence gathering method;
2° the nature of the threat and its degree of gravity which justified use of the specific or exceptional intelligence gathering method;
3° the type of personal data collected in the course of the use of the specific or exceptional method to the extent that this personal data only relates to the complainant.

§ 4. The Standing Committee I can hear the members of the Commission, as well as the head of service of the service involved and the members of the intelligence and security services who used the specific or exceptional intelligence gathering methods. They shall be heard in the absence of the complainant or his lawyer.

The members of the intelligence and security services are required to disclose the secrets that they know to the Standing Committee I. If these secrets relate to an ongoing criminal investigation or judicial inquiry, the Standing Committee I shall discuss this beforehand with the competent magistrate.

If the member of the intelligence and security service considers it necessary not to reveal a secret which he holds because its disclosure would prejudice the protection of sources, the protection of the privacy of third parties or the execution of the assignments of the intelligence and security services as referred to in Articles 7 and 11, the matter shall be submitted to the chairman of the Standing Committee I who shall rule after hearing the head of service.

The complainant and his lawyer may be heard by the Standing Committee I at their request.

Article 43/6

§ 1. When the Standing Committee I establishes that decisions concerning specific or exceptional intelligence gathering methods have been unlawful, it shall order the use of the method to cease if it is still in progress or if it was suspended by the Commission, and shall order that the intelligence acquired by this method cannot be used and is to be destroyed, in accordance with further rules to be determined by the King on the basis of opinions from the Privacy Commission and the Standing Committee I.

The reasoned decision shall be sent immediately to the head of service, to the minister involved, to the Commission and, where relevant, to the Privacy Commission.

If the Standing Committee I considers that a specific or exceptional intelligence gathering method has been used in compliance with the provisions of this Act, while the Commission had forbidden the use of the intelligence gathered with this method, or had suspended the use of this method, the Standing Committee I shall lift this prohibition and this suspension by means of a reasoned decision and shall immediately inform the head of service, the competent minister and the Commission.

§ 2. In the event of a complaint the complainant shall be informed of the decision under the following conditions: any information which could have an adverse impact on the protection of the inviolability of the national territory, the military defence plans, the execution of the assignments of the armed forces, the safety of Belgian nationals abroad, the internal security of the State, including aspects relating to nuclear energy, the maintenance of democratic and constitutional order, the external security of the State and international relations, the operations of the decision-making bodies of the State, the protection of sources or the protection of the privacy of third parties, shall, with reference to this legal provision, be omitted from the transcript of the decision revealed to the complainant.

The same procedure shall be followed if the decision includes information which could compromise the secrecy of the criminal investigation or inquiry, if information relates to an ongoing criminal investigation or judicial inquiry.

Article 43/7

§ 1. Where the Standing Committee I operates in the context of this Title, the functions of the secretariat shall be performed by the secretary of the Standing Committee I or by a level 1 staff member appointed by him.

§ 2. The members of the Standing Committee I, the secretaries, the members of the Investigation Service, and the administrative staff are required to maintain secrecy concerning the facts, actions or information that come to their attention as a result of their cooperation in the application of this Act. They may however use the data and information that they acquire in this context for the execution of their assignment, as set out in Article 1 of the Act of 18 July 1991 governing

review of the police and intelligence services and of the Coordination Unit for Threat Assessment.

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

Article 43/8
No appeal is possible against the decisions of the Standing Committee I.]

(…)