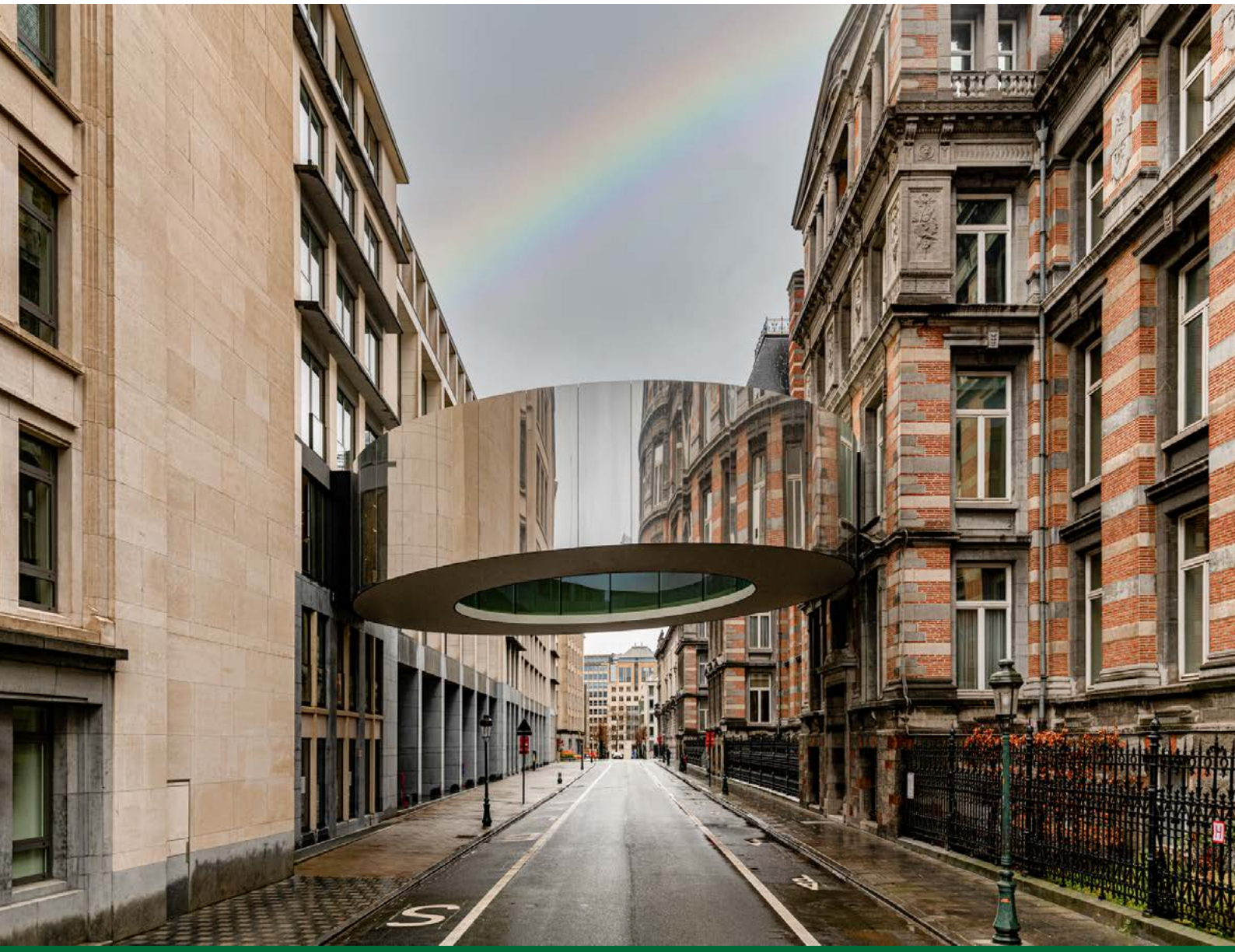
BELGIAN STANDING INTELLIGENCE AGENCIES
REVIEW COMMITTEE



ACTIVITY REPORT
2023

Graphic work and layout: Central Printing Office of the Chamber of Representatives

In accordance with article 35 of the Act of 18 July 1991 governing the review of the police and intelligence services and the Coordination Unit for Threat Analysis

§ 1. The Standing Committee I shall report to the Chamber of Representatives and to 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 by 1 June to the Presidents of the Chamber of Representatives and of the Senate as well as to the competent ministers. In this report, the Standing Committee I shall focus in particular on 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 analysis. [...]

§ 2. The Standing Committee I shall 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 submitted to the Ministers of Justice and of Defence, as well as 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 detail the number of authorisations given, the duration for which the exceptional methods for gathering information are applicable, the number of persons involved and, if applicable, the results obtained. The report shall also cover 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 jeopardize cooperation between the Belgian and foreign intelligence and security services.

§ 3. The Standing Committee I shall report annually to the Chamber of Representatives on the opinions it has provided as data protection authority on the investigations carried out and the measures taken in this quality, as well as on its cooperation with the other data protection authorities. A copy of this report shall also be provided to the competent ministers, as well as to State Security and the General Intelligence and Security Service, who may draw the attention of the Standing Committee I to their remarks.

Brussels, 23 April 2024

From left to right: Frédéric Givron, Registrar – Linda Schweiger, Counsellor – Serge Lipszyc, Chairman – Séverine Merckx, Counsellor

PREFACE

As I write the preface to the 2023 Activity Report of the Standing Committee I, for the last time, I look back on the years I have chaired the Committee.

Terrorism in all its forms is still in our midst. It requires an unwavering investment by the State in all its structures.

We are witnessing the strengthening of State Security, of the General Intelligence and Security Service and of the Coordination Unit for Threat Analysis. More generally, we see the need to increase their support for local coordination structures, as well as their cooperation in judicial matters.

These decisions are commendable. They must be sustained in the foreseeable future. In these uncertain times, bolstering our security is more than ever an obligation for the State.

We have witnessed a resurgence of far-right violence, in particular in the Jürgen Conings case, and a series of other acts against Defence in particular.

The Covid crisis was the catalyst for other attacks on state structures.

The risks associated with the strengthening of the Muslim Brotherhood in Belgium do not always seem to be fully appreciated.

The attack on Swedish football supporters on 16 October 2023 reminds us how vulnerable we still are.

Foreign interference has found an unparalleled echo chamber in the various European, federal and regional parliaments and is undeniably a serious challenge to democracy, with certain parliamentarians being held to give account. But are the current actions the tip of the iceberg, or just fleeting?

The danger has become more unpredictable due to the increased risk of criminal organisations building on their activities in the international drug trade, and the corruption that has resulted.

This alarming phenomenon prompted State Security to invest in this domain. But it also prompted the Government to extend screenings to port staff, as had previously been applicable in other areas, such as Defence, railways, communications, prison staff, etc.

The resurgence of armed conflicts has reminded us the need to anticipate the risks of men and women heading out to war zones.

We must not forget that our institutions are vulnerable to espionage.

Like many other democracies, our country is vulnerable to attempts by foreign powers to spread disinformation. This danger is even more acute with the looming elections on 9 June 2024.

Belgium is clearly an attractive target, especially given the fact that various international bodies are headquartered here.

The intelligence services therefore need to step up their efforts in the face of manifold threats.

Defence has set up the Cyber Command, which is responsible for cyber security of the networks and weapons systems used by Defence. It collects information for the General Intelligence and Security Service. This is an essential tool for our security and will definitely allow us to catch up in this area. It is crucial that it remains under the authority of GISS and under the control of the Committee in the future, as is the case today.

We cannot enhance security without strengthening the rights of citizens. Significant challenges lie ahead, not only in the area of artificial intelligence, but also in the field of new technologies which can intrude into our privacy undetected.

Intelligence services need to improve their partnerships in Belgium and abroad.

The shortcomings and failures are primarily attributable to the silos that exist between services, and a certain resistance to sharing information.

Against this background, the Standing Committee I is at a crossroads, with the appointment of two new counsellors, the arrival of a new generation of staff, but also with a significant expansion of its remit, including the growing importance of the Appeal Body in the security domain.

I would like to conclude my mandate today by expressing my sincere thanks to the Men and Women who have placed their trust in me and supported me in my pursuit of the common good and greater freedom.

I have been fortunate to share these values with many others, and they are also in my thoughts, as we have all striven, each in our own way, to make the world a fairer place.

Brussels, 18 April 2024

Serge Lipszyc
Chairman of the Standing Intelligence Agencies

TABLE OF CONTENTS

1. REVIEW INVESTIGATIONS

REVIEW INVESTIGATIONS

Completed review investigations[1]

Special funds

Like any government agency, intelligence services receive public funds to perform their legal remit. The rule for spending these funds is that there must be full transparency and control. But since certain tasks of State Security and GISS must remain secret, part of their budget avoids this rule. This part is more commonly known as the 'special funds'. Although the amount of these funds is part of the budget allocated to the services, special rules apply to their management, use and control. The Committee previously investigated what these 'special funds' are, the amounts involved and how they are allocated. It also looked into how the funds were used and how these 'special funds' interact with the 'normal' budgets. It also studied the regulatory framework and examined the control mechanisms in place, both internally (within the services) and externally (Court of Audit, Inspectorate of Finance, Standing Committee I). Since 2018 (State Security) and 2020 (GISS), the Court of Audit also conducts a periodic audit of these funds. In the process, the Court of Audit relies upon the technical support of the Standing Committee I. The Committee in turn can then perform its remit with more consideration for how these funds are used. A follow-up investigation of the management, use and control of special funds was started in 2020. The investigation was completed in early 2023. The Committee found that the two services had made progress in the control of these funds, but that there were still certain areas for improvement, such as defining precise criteria for the use of these funds.

The financing of political parties

Since the adoption of the Act of 4 July 1989 on the limitation and control of electoral expenditure (BOJ 20 July 1989), Belgium has had federal legislation that regulates the direct public financing of political parties. In exchange for this funding, political parties have to comply with specific obligations: restrictions on spending on electoral propaganda; a regulation of the use of certain electoral resources; a ban on donations from legal persons and de facto associations, as well as restrictions on and identification of donations from natural persons; transparency of accounts and respect for the rights and freedoms guaranteed by the European Convention on Human Rights. Following revelations in the Belgian and European press concerning Russian financial interference, the Committee produced a legal analysis of the existing rules that should allow the intelligence services to detect illegal financing from foreign countries aimed at influencing Belgian politicians.

Convention 108+

In the field of intelligence, the rights of individuals whose data are processed, and transparency in this regard, are significantly curtailed, as it is crucial for the operations of the intelligence services to remain confidential. Indeed, European instruments such as the General Data Protection Regulation or the 'Police and Justice' Directive do not apply to data processing operations carried out for national security purposes. The only legally binding international instrument is Convention No. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data ("Convention 108"), from 1981. In 2018, Convention 108 was overhauled, to become 'Convention 108+', which clarifies and strengthens the legal framework on personal data in the domain of national security.

In a review investigation, the Committee highlighted the opportunities in ratifying Convention 108+ and adapting the national legal framework, nevertheless without minimising the restrictions on the intelligence and security services.

For example, Convention 108+ invites the legislator to re-examine the way the right of indirect access to personal data is exercised, as well as the procedures for access to information from the services and the exceptions to communicating this information. These measures could enhance citizen confidence and allow for more effective control. Indeed, Convention 108+ offers the legislator the possibility to provide oversight bodies with the means to verify the effectiveness of the regulation of cross-border movement of intelligence services, review the exceptions that allow the transfer of data if there is no adequate level of protection, and to legally enshrine the principles applicable to international cooperation of the services.

Finally, Convention 108+ introduces a mechanism for cooperation and mutual assistance between oversight bodies. More specifically, the text provides for the possibility of coordinating the actions of oversight bodies, carrying out joint actions and exchanging information.

The data protection rules may be perceived by the services as a hindrance to the performance of their duties. However, this clarification of the normative framework and more transparency helps ensure their actions are more legitimate.

Although Belgium signed Convention 108+ in October 2018, it has not yet been ratified. Following its legal analysis, the Committee underlined

1 The full versions of the review investigation reports can be accessed at www.comiteri.be

the significant added value of Convention 108+, and requested the Ministers of Justice and Defence, who are responsible for intelligence and security services, to urge the Minister of Foreign Affairs to ratify it.

TikTok and security risks

In March 2023, the National Security Council took the decision to temporarily ban the use of TikTok on government devices for privacy and security reasons. At the request of the Chamber of Representatives' Monitoring Committee, the Standing Committee I drafted a paper analysing the information position of the intelligence services on this issue. Both services warned of the technical vulnerabilities of the platform, as well as the collection and sharing of (meta)data with Chinese government, among other things. The Committee's analysis also provided an overview of national measures taken by EU member states to restrict access to the platform.

The monitoring of an imam

In October 2021, a decision was taken to revoke the residence permit of a Moroccan imam, who is also an emblematic figure of the religious scene in Brussels. This decision was justified by the Secretary of State for Asylum and Migration, based on information provided by State Security. Nevertheless, a few days earlier, the Brussels family court, which had consented to the imam's request to acquire Belgian citizenship, ruled that this information was insufficiently substantiated.

In February 2022, the Committee opened a review investigation to examine the information position of State Security, the means used in monitoring the individual concerned, as well as the processing and exchange of personal data by State Security with other authorities and administrations. The investigation provided clarity on the actions of State Security in the context of two parallel proceedings concerning the imam: on the one hand, State Security had issued an opinion on the declaration of nationality submitted by the individual, and, on the other hand, the intelligence service had responded to a request for information from the Immigration Office following media reports, in January 2019, about past sermons given by the imam. State Security saw these two parallel proceedings as an opportunity to apply its 'disruption strategy' (*infra*). In this case, State Security provided information to the Immigration Office in order to revoke the individual's residence permit.

The Committee found that there were shortcomings in the management of the individual's case within State Security. Indeed, in its communications with external partners, the service disseminated strong conclusions that the Committee felt were disproportionate to the information gathered and the monitoring strategy implemented. The Committee formulated several recommendations, but acknowledged the efforts State Security was already making to improve its internal operations. In its capacity as Competent Supervisory Authority (art. 95 DP Act), the Standing Committee I recommended that corrective measures be taken.

Security screenings

In the past, the Standing Committee I, whose Chairman is also Chairman of the Appeal Body for Security Clearances, Certificates and Advice, formulated a range of recommendations related to security screenings: on the need for security screenings for positions of trust, more screenings of military and civilian personnel within Defence, on the correct application of the possibility to request security screenings, etc. Several recommendations were also formulated in the context of a broader review investigation into security screenings (2019). Accordingly, the Committee raised the issue of pre-screening prospective staff within State Security and decided, in its capacity as Competent Supervisory Authority, to investigate the matter further. After analysing existing procedures within State Security and GISS, the Committee recommended harmonising the procedure for security screening for all prospective staff at one of the intelligence services or Coordination Unit for Threat Analysis (CUTA).

A complaint by the Muslim Executive

In early 2022, a complaint was filed by the Muslim Executive of Belgium about the functioning of State Security, more specifically with regard to the systematic leaking of reports and the granting of access to reports to journalists, while the persons who are the subjects of these reports do not have this possibility. The Muslim Executive argued that in recent years reports and notes from State Security are often used as a means to discredit Muslims and mosques. The leaked notes are said to create a (lasting) negative and stigmatising image about Islam and Muslims. This systematic leaking to the media constitutes, according to the Muslim Executive, an invasion of the privacy of the persons who are the subject of these reports (art. 22 Constitution and art. 8 ECHR). As a result of its investigation, the Committee expressed a number of concerns regarding the management of information leaks within State Security at the time, but also welcomed the publication of new internal guidelines, in particular on drafting a written report on any identified security incident. However, the

Committee reiterated the legal obligation of State Security to report security breaches of personal data to the Committee in its capacity as data protection authority.

Disruption

In the past year, the Standing Committee I conducted a legal analysis of the legal options available to the intelligence community as regards disruption, namely disrupting threats so that they no longer occur or are less harmful. This analysis was intended to clarify an issue that had arisen in several cases investigated by the Committee.

The Committee wanted to examine, via this analysis, how State Security organises its disruption strategy. The Committee focused on internal regulations and whether they are compliant with the legal framework, without examining how the civilian intelligence service puts its theory of disruption into practice. It also looked at the conditions under which GISS is authorised to disrupt threats.

The risk of infiltration into the services

In recent years, the international intelligence community has been rocked by a number of cases of infiltration (insider threat) within the services themselves. The Committee took the initiative to start a review investigation into how the two intelligence services deal with the risk of infiltration: what risks are identified, what countermeasures are taken to manage them and to respond to them if they occur? Given the importance and sensitivity of this case, the Committee decided at the end of 2023 to implement permanent monitoring in this matter.

CUTA's threat analysis of an Iranian delegation in Brussels

The Brussels Urban Summit, an international gathering of the mayors of major cities, took place in mid-June 2023. Representatives from more than 300 cities were invited to Brussels for the event. In this context, Belgium issued visas 'with limited territorial validity' to the 14 members of an Iranian delegation which included the mayor of Tehran. The granting of these visas, a few weeks after the release of a Belgian national, was the subject of intense debate in parliament. The political and media controversy was further fuelled by revelations about alleged observation and spying on opponents of the Iranian regime by members of the delegation in question.

In this context and at the request of the Monitoring Committee, the Standing Committees P and I opened a joint review investigation into CUTA's information position and involvement. In this regard, the Committees identified that CUTA only intervened after issuing visas to the members of the Iranian delegation in order to respond to requests from the National Crisis Centre to assess the threat. More specifically, CUTA's dual assessment concerned a possible threat against the Brussels Urban Summit and against the mayor of Tehran. CUTA was therefore not asked about possible threats from (some members of) the Iranian delegation. CUTA did not take the initiative to make such an assessment either. However, given CUTA's mandate, this analysis would have been limited to potential extremist and terrorist threats. Nonetheless, the investigation by the Standing Committees P and I clarified that CUTA did not have any information relating to a threat against or from the Iranian delegation.

Ongoing review investigations

Access to police camera images

Pursuant to the Intelligence Services Act and the Policing Act, intelligence services can access the images of video surveillance cameras of police departments, subject to various conditions. Alerted by a local police zone's chief, the Committee sought clarification on the practical implementation of the legal framework on access to police camera images by intelligence services. The chief of police referred to agreements or understandings with police zones for the remote transfer of data. The appropriate procedure is that the images are requested in situ, with a police operator present at the management centre of the police zone. The Committee was of the opinion that in order to ensure legal certainty for all actors, this method needed to be subjected to a legal analysis.

(Specific) intelligence methods

The Committee obtained a number of possibilities to control a number of 'standard' methods. These include verifying the identification of the telecommunications user (art. 16/2 Intelligence Services Act (ISA)), access to passenger data (Passenger Name Record) (art. 16/3 ISA), access to police camera images (art. 16/4 ISA), and furthermore, control prior to interceptions, hacking IT systems and recording moving images (art. 44/3 ISA). The Committee decided to study this issue in depth for both the implementation of these methods by the intelligence services and the practical modalities for control.

Analysis methodology

During review investigations or when dealing with complaints, the Committee is often confronted with cases in which the intelligence services assign qualifications to a person of interest and link them to a threat. These qualifications are sometimes disputed by the individuals involved. The Committee started an investigation to gain insight into the methodology used by the intelligence services to assign these qualifications to a person of interest. In parallel, the analysis methodology used by CUTA to this end is being investigated, together with the Standing Committee P.

Data breaches

For certain data leaks, the intelligence services are obliged to notify the Standing Committee I, in its capacity as competent supervisory authority for the processing of personal data, as soon as there is a risk to the fundamental rights and freedoms of the persons whose personal data have been disseminated. In 2023, the Committee started a review investigation following a possible unlawful data extraction.

The monitoring of an Iranian delegation in Brussels by State Security and GISS

In June 2023, an international gathering of the mayors of major cities took place in Brussels. Belgium granted visas 'with limited territorial validity' to 14 members of an Iranian delegation. At the request of the Monitoring Committee, the Committee is, among other things, investigating the role that intelligence services played in the screening process for the issuance of these visas. A similar investigation was started together with the Standing Committee P regarding the role of CUTA in this case (*supra*).

Threats related to the Iranian regime

Besides the specific case of the Iranian delegation in Brussels in June 2023, the Monitoring Committee also requested the Committee to investigate how intelligence services monitor the activities of the Iranian regime. The investigation analyses the legal framework as well as the available means dedicated to this end by the intelligence services. Together with the Standing Committee P, CUTA's assessment of the threat against opponents of authoritarian regimes in Belgium is being examined in a parallel investigation.

Terrorist attack on Swedish football supporters

In mid-October 2023, during a football match between Belgium and Sweden, a terrorist attack in the centre of Brussels left two dead and one injured, all three Swedish nationals. The perpetrator of the attack was quickly identified. The Committee opened two review investigations examining both the information position of the intelligence services and, in a joint investigation with the Standing Committee P, CUTA's information position.

Interference by foreign powers

At the request of the Parliamentary Monitoring Committee, the Committee investigated the actions taken by the intelligence and security services to identify the threat of interference by foreign powers through the financing of political parties, institutions and/or individuals in Belgium.

2. COMPLAINTS HANDLING

COMPLAINTS HANDLING

Besides review investigations, the Committee also handles complaints and reports regarding the operations, actions, acts or omissions of the intelligence services, CUTA and its support services and their staff. Moreover, the Committee also handles individual requests relating to the processing of personal data by the aforementioned persons and services, and their subcontractors. In such cases, it acts as the data protection authority which the applicant can contact to verify whether the applicable data protection rules have been complied with, and to have their data corrected or deleted.

2023	STANDING COMMITTEE I		STANDING COMMITTEES I AND P	TOTAL
1. Complaints submitted in 2023	55		2	57
2. Inadmissible complaints 2023	40		0	40[1]
3. Admissible complaints 2023	21		2	23
	State Security	14		
	GISS	3		
	State Security/GISS	4		
4. Admissible DPA complaints 2023	17		2	19
5. Pending cases	6		0	6[2]
6. Ongoing cases	10		2	12[3]
7. Admissible closed cases	37		6	43[4]
8. Corrective measures	3		0	3[5]
9. Total complaints handled	53		8	61[6]

1 Of which 9 complaints were submitted in 2022.
2 Of which 3 complaints are pending an admissibility decision.
3 Of which 1 complaint from 2020 and 11 complaints from 2023.
4 Of which 8 complaints from 2021, 26 complaints from 2022 and 9 complaints from 2023. Added to this are the 40 complaints that were declared inadmissible.
5 Of which 2 complaints from 2022 and 1 complaint from 2023. Added to this are the 40 complaints that were declared inadmissible.
6 Sum of pending, ongoing and closed complaints. Added to this are the 40 complaints that were declared inadmissible.

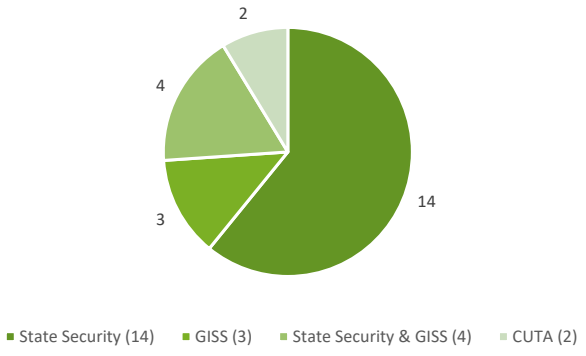
The above table gives an overview of the cases handled in 2023 (open and/or closed). The columns in the table distribute the complaints according to whether the Standing Committee I is exclusively competent or together with the Standing Committee P. It should be noted that the same complaint can be the subject of several 'cases', depending on the services involved: a complaint against CUTA as well as State Security is included both in the cases handled jointly by the Standing Committees I and P with respect to CUTA and in the cases handled exclusively by the Standing Committee I with respect to investigative acts relating to State Security.

In 2023, the Standing Committee I received a total of 55 complaints and reports. Following a brief preliminary investigation and verification of a number of objective data, the Committee rejected 40 complaints and reports as either manifestly not admissible or because the Committee did not have jurisdiction for the matter. In the latter case, complainants were referred, if possible, to the relevant authorities (e.g., the Public Prosecutor's Office, the Supervisory Body for Police Information, or the Standing Committee P).

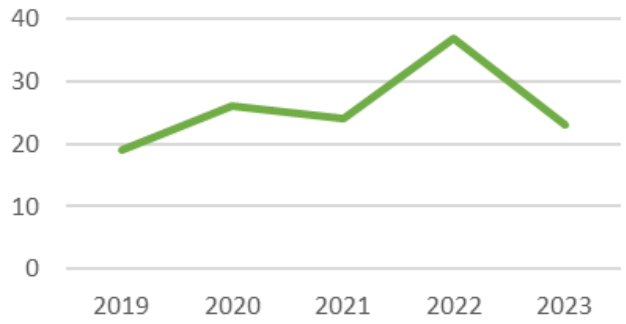
19 of the admissible complaints filed in 2023 were treated as DPA complaints. Once again, the Committee had to handle several requests submitted in the context of an application to obtain nationality or a residence permit. Faced with a negative decision based on information provided by State Security, GISS and/or CUTA, applicants turn to the Standing Committee I, among others, for a review of the processing of their personal data. The way in which this data is shared with foreign partners is the focus of increasing attention from the Committee, which is seized by applicants who have encountered problems with border controls abroad. As the supervisory authority over the intelligence services, the Committee imposed corrective measures in three cases (art. 51/3 Review Act). Depending on the case, this may involve requesting the rectification or erasure of personal data, notification of the Committee's decision to partners and/or authorities, or dissemination of the decision within the service concerned. In the context of international signalling, the Committee notes that there are limits to requests for corrective measures, as they depend in part on the goodwill of partner services in foreign countries, bearing in mind that cooperation with certain countries is sometimes limited or non-existent.

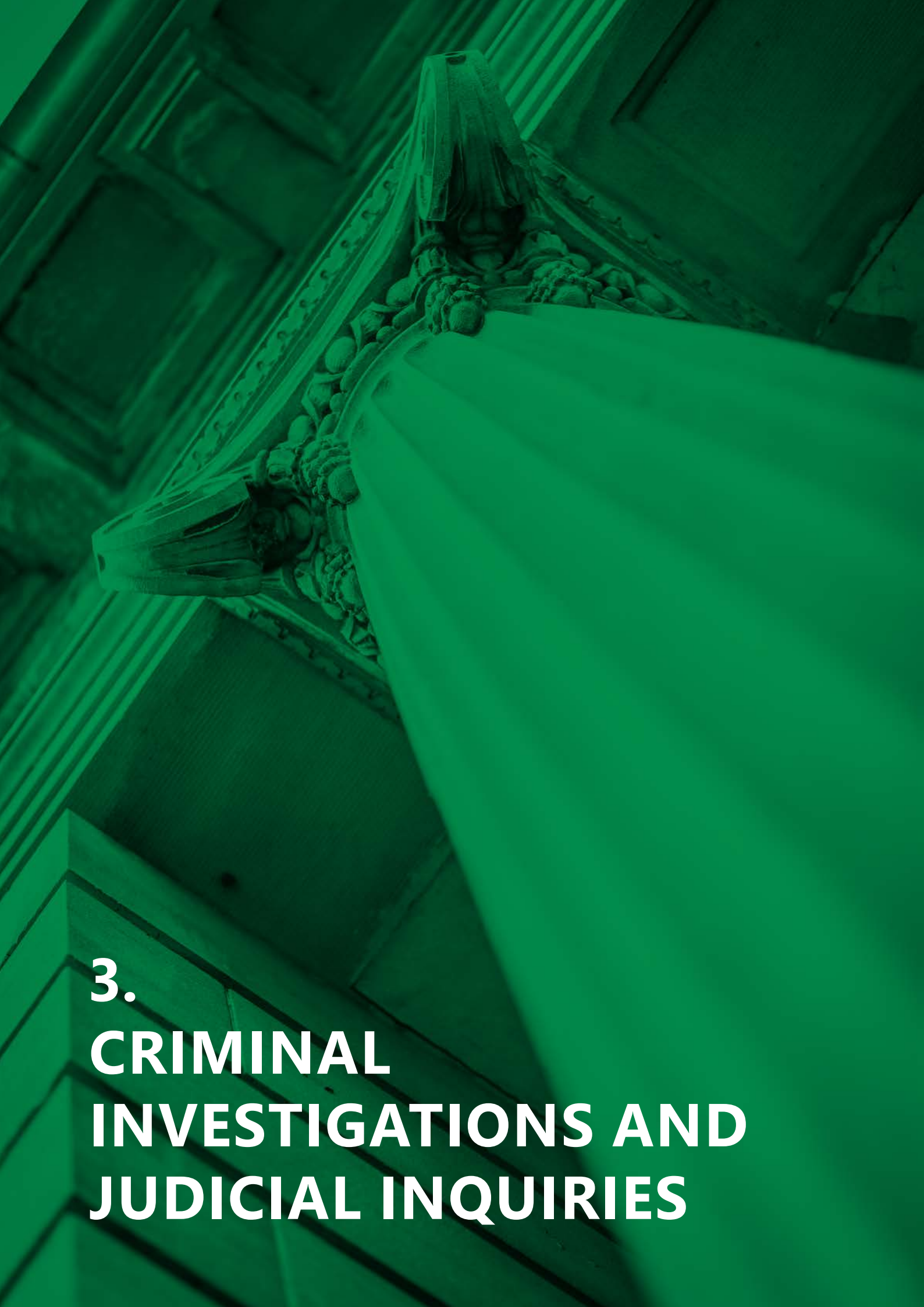
43 handled complaints were closed in 2023, 12 complaints were still pending at the start of 2024. Compared to previous years, a slight drop in the number of admissible complaints submitted to the Standing Committee I was observed. From the overview of services involved in the complaints submitted in 2023, State Security appears to be significantly represented.

Services implicated in the complaints submitted in 2023



Admissible complaints





3. CRIMINAL INVESTIGATIONS AND JUDICIAL INQUIRIES

CRIMINAL INVESTIGATIONS AND JUDICIAL INQUIRIES

The Investigation Service I of the Standing Committee I also conducts investigations on behalf of the judicial authorities into members of the intelligence and security services and of the Coordination Unit for Threat Analysis (CUTA) who are suspected of a crime and/or offence (art. 40, third paragraph Review Act).

When fulfilling a judicial police mission, members of the Investigation Service I are under the supervision of the General Prosecutor at the Court of Appeals or the Federal Prosecutor (art. 39 Review Act) and the Standing Committee I has no control over them. However, the Chairman of the Standing Committee I must ensure that the performance of the Committee's other legal missions is not disrupted.

In 2023, the Investigation Service I was tasked with managing three investigations in the context of complaints from State Security against 'X' for alleged breaches of professional secrecy within the service. These investigations were ongoing as of 31 December 2023.

Once the judicial investigation is completed, the Investigation Service must send a report to the Chairman of the Standing Committee I if the investigation highlighted a lack of efficiency within the intelligence services, insufficient coordination between them, or a violation on their part of the rights granted to individuals by the Constitution and the law. This was not the case in 2023.

4.
(SPECIAL) INTELLIGENCE METHODS

(SPECIAL) INTELLIGENCE METHODS

Methods used by GISS

The Committee is tasked with the *a posteriori* control of special intelligence methods. This control relates to the legality, proportionality and subsidiarity of these methods. For 2023, the Committee relied (for the first time) on figures supplied by the intelligence services themselves. Between 1 January and 31 December 2023, GISS granted 669 authorisations to use special intelligence methods, of which 448 were specific and 221 exceptional methods.

The tables and charts below detail the intelligence methods used by GISS during 2023.

Specific methods (GISS)	2023
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 ISA)	22
Real Time retrieval of police camera images (publicly accessible places) (art. 18/4 §3 ISA)	14
Searching places accessible to the public using technical means, searching the content of locked objects or removing these objects (art. 18/5 ISA)	0
Infiltrating the virtual world under a false identity or false capacity (art. 18/5/1 ISA).	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator (art. 18/6 ISA)	0
Requesting transport and travel information from private transport and travel services (art. 18/6/1 ISA)	0
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° ISA)	12
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° ISA)	0
Tracing call-associated data of electronic means of communication and requesting the cooperation of an operator (art. 18/8, §1, 1° ISA)	202
Monitoring localisation data for electronic communications and requesting the cooperation of an operator (art. 18/8, §1, 2° ISA)	198
TOTAL	**448**

Exceptional methods (GISS)	2023
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 ISA)	15
Real Time retrieval of police camera images (not publicly accessible places) (art. 18/11 §3 ISA)	4
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 ISA)	14
Infiltration into the real world (art. 18/12/1 ISA)	0
Opening and inspecting post, whether or not entrusted to a postal operator (art. 18/14 ISA)	6
Collecting data on bank accounts and banking transactions (art. 18/15 ISA)	14
Penetrating a computer system (art. 18/16 ISA)	40
Tapping, intercepting to and recording communications (art. 18/17 ISA)	128
TOTAL	**221**

For 2023, GISS saw a significant rise in the number of authorisations for specific methods. Above all, monitoring localisation data for electronic communications saw a sharp rise.

The military intelligence service also witnessed a rise in exceptional methods, confirming the upward trend from 2022. As in 2022, penetrating a computer system (art. 18/16 ISA) and intercepting communications (art. 18/17 ISA) were the most commonly used methods, and saw the largest rise.

In 2023, espionage was one of the priorities of GISS, in particular through surveillance of defence attachés or foreign diplomats accredited in Belgium, the European Union or NATO. Monitoring extremism within the military was also a key focus for the service. Finally, organised crime and threats against military infrastructure and personnel were specifically monitored by GISS.

Ordinary 'plus' methods

Originally, ordinary intelligence methods were only subject to regular control by the Committee. However, ordinary methods have been incorporated into the Intelligence Services Act for several years now, whereby the Committee is entrusted with a special controlling task and/or whereby an additional information requirement was imposed on the intelligence service concerned vis-à-vis the Committee (the so-called 'ordinary plus methods'). The verification or information requirement is regulated differently for each of these methods, despite the Committee's calls to harmonise them.

ORDINARY 'PLUS' METHODS GISS	2023
Identification of a telecommunication user (art. 16/2 ISA)	509
Targeted PNR data searches (art. 16/3 ISA)	51
Use of police camera images (art. 16/4, §2 ISA)	40
Requesting financial data (art. 16/6 ISA)	38

The statistics on requests for access to Passenger Name Records (PNR) by GISS end on 13 October 2023. Indeed, the Constitutional Court annulled Article 16/3 ISA with its ruling of 12 October 2023 (ruling 131/2023). Following a preliminary question to the European Court of Justice, the Court ruled that the scope of the intelligence services is much broader than what the original European regulations envisaged, and that the lack of prior independent control of the requests of the intelligence services violates the rights of citizens. For this reason, several articles in the Act of 25 December 2016 "on the processing of passenger data" have been rescinded, and therefore also article 16/3 that regulated requests in the Intelligence Services Act. As a result, GISS can no longer perform *ad hoc* requests in the PNR database. The legislator promises to resolve this as soon as possible through a remedial act that takes the Court's concerns into account.

Methods used by State Security

For 2023, the Committee relied (for the first time) on figures supplied by the intelligence services themselves. Between 1 January and 31 December 2023, State Security granted 1,718 authorisations to use special intelligence methods, of which 1,369 were specific and 349 exceptional methods. It should be noted that GISS displays the figures by article of law applied, while State Security counts the special intelligence methods (SIM) by operation. As such, there is no point in comparing the figures of the two services.

The tables and charts below detail the intelligence methods deployed by State Security during 2023.

Specific methods (State Security)	2023
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 ISA)	142
Real Time retrieval of police camera images (publicly accessible places) (art. 18/4 §3 ISA)	0
Searching places accessible to the public using technical means, searching the content of locked objects or removing these objects (art. 18/5 ISA)	0
Infiltrating the virtual world under a false identity or false capacity (art. 18/5/1 ISA).	0
Inspection of identification data for postal traffic and requesting the cooperation of a postal operator (art. 18/6 ISA)	0
Requesting transport and travel information from private transport and travel services (art. 18/6/1 ISA)	23
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° ISA)	50
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° ISA)	0
Tracing call-associated data of electronic means of communication and requesting the cooperation of an operator (art. 18/8, §1, 1° ISA)	577
Monitoring localisation data for electronic communications and requesting the cooperation of an operator (art. 18/8, §1, 2° ISA)	577
TOTAL	**1369**

Exceptional methods (State Security)	2023
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 ISA)	5
Real Time retrieval of police camera images (not publicly accessible places) (art. 18/11 §3 ISA)	0
Searching places that are inaccessible to the public, whether or not using technical means, as well as objects located there, whether or not locked (art. 18/12 ISA)	26
Infiltration into the real world (art. 18/12/1 ISA)	0
Opening and inspecting post, whether or not entrusted to a postal operator (art. 18/14 ISA)	25
Collecting data on bank accounts and banking transactions (art. 18/15 ISA)	45
Penetrating a computer system (art. 18/16 ISA)	65
Tapping, intercepting to and recording communications (art. 18/17 ISA)	183
TOTAL	**349**

As with GISS, a strong rise in the number of specific methods can also be observed with State Security, in particular in monitoring localisation data for electronic communications. Among other things, this rise can be explained by the simultaneous increase in the number of State Security personnel, which means that more cases can be processed and more methods applied.

Regarding exceptional methods, State Security, like GISS, reports an increase in computer system penetration (art. 18/16 ISA) and communications tapping (art. 18/17 ISA). However, State Security does report a significant drop in the number of observations in non-publicly accessible places.

Among the threats monitored by the civilian intelligence services, jihadist terrorism and espionage have the highest priority. State Security is primarily interested in online terrorist networks and lone wolfs, and keeps a close eye on geopolitical conflicts in Central Asia and the Middle East, as well as threats against certain European countries such as Sweden and its citizens. In the area of espionage, Russia, China and Iran in particular are monitored. In this regard, the monitoring of these countries by State Security has intensified since the invasion of Ukraine, with a special focus on Russian intelligence agents working under diplomatic cover. The same applies to China's intelligence services and their attempts to influence universities and politicians.

Besides these two major threats, State Security also closely monitors threats of interference and extremism. Long before Qatargate, State Security had been monitoring a number of influential actors. Following the legal proceedings in this case, State Security continued to monitor the threat of interference. Since 2022, State Security has also intensified efforts against the threat of organised crime, specifically threats to state institutions and public services such as the police, customs and justice, as well as threats to politicians.

Ordinary 'plus' methods

Originally, ordinary intelligence methods were only subject to regular supervision by the Committee. However, ordinary methods have been incorporated into the Intelligence Services Act for several years now, whereby the Committee is entrusted with a special monitoring task and/or whereby an additional information requirement was imposed on the intelligence service concerned vis-à-vis the Committee (the so-called 'ordinary plus methods'). The verification or information requirement is regulated differently for each of these methods, despite the Committee's calls to harmonise them.

ORDINARY 'PLUS' METHODS STATE SECURITY	2023
Identification of a telecommunication user (art. 16/2 ISA)	4417
Targeted PNR data searches (art. 16/3 ISA)	318
Use of police camera images (art. 16/4, §2 ISA)	51
Requesting financial data (art. 16/6 ISA)	135

The statistics on requests for access to Passenger Name Records (PNR) by State Security end on 13 October 2023. Indeed, the Constitutional Court annulled Article 16/3 ISA with its ruling of 12 October 2023 (ruling 131/2023). Following a preliminary question to the European Court of Justice, the Court ruled that the scope of the intelligence services is much broader than what the original European regulations envisaged, and that the lack of prior independent control of the requests of the intelligence services violates the rights of citizens. For this reason, several articles in the Act of 25 December 2016 "on the processing of passenger data" have been rescinded, and therefore also article 16/3 that regulated requests in the Intelligence Services Act. As a result, State Security can no longer perform *ad hoc* requests in the PNR database. The legislator promises to resolve this as soon as possible through a remedial act that takes the Court's concerns into account.

Ex post control

The Standing Committee I is tasked with the *ex post* control of the use of specific and exceptional intelligence methods. The Committee subjects all authorisations to use these methods to a *prima facie* investigation, with a view to a possible referral (art. 43/4 ISA). This referral can be made at the Committee's own initiative, at the request of the Data Protection Authority (GBA), as a result of a complaint from a citizen, by operation of law if the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and has prohibited the use of the information or, finally, by operation of law if the competent minister has issued an authorisation based on Article 18/10 § 3 ISA.

In addition, the Committee can also be seized in its capacity as "Prejudicial consulting body "(arts. 131*bis*, 189*quater* and 279*bis* Code of Criminal Procedure). In such cases, the Committee issues an opinion on the lawfulness of the specific or exceptional methods that have produced intelligence used in a criminal case. The decision to request an opinion lies with the investigating courts or criminal judges. 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	2021	2022	2023
1. At the Committee's initiative	16	12	16	3	1	1	4	2	1	5	0
2. Data Protection Authority	0	0	0	0	0	0	0	0	0	0	0
3. Complaint	0	0	0	1	0	0	0	0	0	0	0
4. Suspension by SIM Commission	5	5	11	19	15	10	12	9	8	9	13
5. Authorisation by minister	2	1	0	0	0	0	0	0	0	0	0
6. Prejudicial consulting body	0	0	0	0	0	0	0	0	0	0	0
TOTAL	**23**	**18**	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**	**13**

The number of decisions taken by the Committee remained stable in 2023. All referrals were the result of suspension by the SIM Commission. Once seized, the Committee can take various kinds of (interim) decisions. In 10 cases, it was decided to cease the method; in three other cases, the Committee decided to partially cease the method, which meant that the services could only use part of the information collected.

Foreign interceptions, image recordings and IT intrusions

Article 44 of the Intelligence Services Act allows the General Intelligence and Security Service to detect, intercept, tap and record any form of communication sent or received abroad. Intrusions in IT systems (art. 44/1 ISA) and the capture of moving images in foreign countries (art. 44/2 ISA) are also among the possibilities open to the military intelligence service. The Standing Committee I reviews these methods prior to, during and after implementation.

In January 2023, the Committee received the plans for interceptions, intrusions and image recordings for that year. These plans met all legal requirements. At the end of 2023, the Standing Committee I also visited the installations where the interceptions are made. Among other things, the Committee noted the logbook's compliance with applicable laws and guidelines. The Committee confirmed that the remarks it made in 2021 had been taken into account. The facilities where GISS carries out the IT intrusions were visited by the Committee. On this occasion, it could be noted that important investments have been made and are being made to be able to carry out the planned missions. Regarding review after the implementation of interceptions, intrusions or image recordings, the Standing Committee I received all legally required lists. However, the Committee is unable to share any further information in this area due to its classified nature.

5. OPINIONS, NEW LAWS AND REGULATIONS

OPINIONS, NEW LAWS AND REGULATIONS

Opinions

The Standing Committee I can only issue an opinion on a draft of law, royal decree, circular or any other document setting out the policies of the competent ministers at the request of the Chamber of Representatives or the competent minister (art. 33 Review Act). But in addition, the Committee can also provide opinions as the Competent Supervisory Authority for the processing of personal data (arts. 73 and 95 DP Act), as well as regarding the regulation on common databases, together with the Supervisory Body for Police Information (COC). Its opinions are sometimes formulated in a dual capacity.

In recent years, the Committee has received ever more requests for opinions; the time invested in this has therefore increased substantially. In 2023, the Committee was asked for its opinion 11 times: four times at the request of the Minister of Justice (in one case the request came through the Data Protection Authority (DPA)) and seven times at the request of the Minister of the Interior. Preliminary drafts of laws were mostly submitted for an opinion, three times a draft royal decree and once a draft ministerial order. The opinions cover a diverse range of issues, from private investigation to the recognition of Buddhism, including a new Shipping Code. All opinions are available in full on the website of the Standing Committee I.

Private investigation

Private investigation activities were regulated by a law from 1991. This law was outdated and did not take into account new legal rules, new practices and new investigative possibilities. An Act regulating private and special security had already been enacted in October 2017. A new preliminary draft law now provided for a complete revision in the area of private investigation. To perform their activities, the companies offering these services must be licensed. Various safety and training requirements apply to their staff. In addition, the draft law focuses on prior control in the form of licensing systems and ID cards for staff, as well as *ex post* control as regards compliance with the law. In this way, the government wanted to ensure reliability, quality of service and respect for the rule of law. The preliminary draft was submitted for the opinion of the Standing Committee I, among others. Indeed, the draft provided for the processing of personal data by the two intelligence and security services. The Committee welcomed the return to a harmonised screening regime for all actors in the private security sector. Nevertheless, the Committee highlighted the fact that various types of screenings continue to co-exist (security screenings, security verifications, examination of security conditions, integrity screenings, etc.) while the underlying purpose of all these screenings is similar.

However, with the changes in the new draft law submitted to the Committee, there was once again a risk of a disparity between the regulations for private security on the one hand and private investigation on the other. In a second opinion, the Committee concluded that the purpose of the screening was unclear, and that the assessment framework needed to be much more precisely defined.

Direct access to the General National Database

In 2019, the Policing Act was amended to allow intelligence services access to the General National Database (GND). A draft royal decree further elaborated this provision. Specifically, the categories of personal data that are directly accessible to the intelligence services and the means of access were specified. In its opinion, the Committee asked for clarification on the concept and scope of 'direct access', on the regime for medical data, and on the justification for consultations and the registration requirement. Further processing of GND data (e.g., data transfer), processing logs, and exporting data from the GND to the files of State Security and GISS, also raised questions. Finally, there was a focus on reciprocity in terms of data sharing. This reciprocity does not require that police forces also have direct access to the databases of the intelligence services. On the contrary, the legislator appeared to assume that the current regulations, as long as they were effectively applied, already provided for reciprocity.

A draft ministerial decree on direct access of the intelligence and security services to the GND was then submitted. In a second opinion, the Committee made comments on the classification method and the difference between judicial information and administrative police data. The Committee called into question the relevance of differentiated rules, which would complicate the application and monitoring of these provisions.

Buddhism as a non-confessional philosophical organisation

A preliminary draft law sought to recognise Buddhism as a non-confessional philosophical organisation pursuant to Article 181 § 2 of the Constitution and to recognise the Belgian Buddhist Union as the representative body of this community in Belgium as well as the organisation of the functioning of local Buddhist communities and the function of Buddhist delegates. The preliminary draft provided for the introduction of new processing of personal data by the intelligence services and the Coordination Unit for Threat Analysis (CUTA). The Committee concluded that many aspects of the preliminary draft needed to be specified, so that the scope of the screening it proposed would be made legal.

The common database 'TER'

At the end of March 2023, the Council of Ministers approved a draft law and a draft royal decree on the operation of the Common Database on Terrorism, Extremism, Radicalisation Process (CDB TER). The draft seeks to incorporate the provisions of the Policing Act regarding the common databases on 'Terrorist Fighters' and 'Hate Propagandists' into an autonomous law. In this way, the law endorses the fact that there is only one common database for dealing with terrorism, extremism and radicalism (the CDB TER). This common database was created after the attacks in 2016. It contains information on individuals considered extremists and terrorists who are monitored in Belgium in the context of the 'TER Strategy'. The database allows the intelligence and security services to share information and coordinate which service is best positioned to take action. CUTA, State Security, GISS, the Public Prosecutor's Office, the Integrated Police, the Crisis Centre, the Immigration Office, among others, have roles and certain obligations in this regard. With this draft law and draft royal decree, the Ministers of Justice and the Interior wanted to improve the functioning of the common database and the security structure around it. In its capacity as Competent Supervisory Authority, the Committee expressed comments on the purposes of the processing of personal data, the applicable data protection rules, the 'need to know' for access to or consultation of personal data, but also on the retention period of the data, data logging, the links to other databases, the communication of data from the CDB TER to third party governments or services, and furthermore, the obligation for the intelligence services to feed to this common database.

The trustworthiness of individuals in the civil nuclear sector

A new preliminary draft law proposed amendments to the regulations on safety certificates for the nuclear sector. The draft law aimed to refine the system for verifying the trustworthiness of individuals in the nuclear sector, to make it more flexible and effective. To this end, it was decided to expand the derogation for the nuclear sector in Article 8*bis* Classification and Security Clearances Act. The Committee noted that this option makes an already extremely complex system for verifying the trustworthiness of individuals untransparent. It requested the authors of the draft law to analyse whether this approach was necessary, considering the intended purpose. Moreover, the draft, which aims to provide a legal basis for verifying the trustworthiness of individuals seeking access to uncategorised elements of the nuclear and radiological sector, sought to introduce a new form of security certificate. However, it was not apparent anywhere that the existing rules for the other sectors (security opinions and security certificates, provided for in art. 22*quinquies*, art. 22*quinquies*/1 Classification and Security Clearances Act and art. 22*bis*, second paragraph, Classification and Security Clearances Act, respectively) could not meet the intended purpose. Once again, this choice only complicates the system for verifying the trustworthiness of individuals. The Standing Committee I asked the sponsors of the draft law to analyse whether this approach was necessary, and justify the choice made.

Consultation opportunity of the ETIAS system

ETIAS is the new EU travel information and authorisation system. The system applies to third-country nationals who are exempt from a visa obligation and wish to travel to the Schengen area. These third-country nationals must complete an online form before travelling to the Schengen area to apply for a travel permit. The introduction of ETIAS aims to improve internal security, prevent illegal immigration and protect public health by identifying individuals who may pose a security or immigration risk, even before they leave for the EU. The preliminary draft provided that seconded personnel from both State Security and GISS would be part of a section brought under the National Crisis Centre, which is authorised to process hits relating to security and serious epidemiological risks. However, the preliminary draft expanded the scope of the European regulation by allowing the two Belgian intelligence services to use the ETIAS system for all the threats they need to monitor. This contradicts the ETIAS regulation, which limits both

consultations and listing on a watchlist to individuals who can be linked to terrorist offences or other serious criminal offences. The Committee argued that by giving the intelligence services general consultation powers, and by allowing them to place individuals on the watchlist who are beyond the scope of the ETIAS system, the regulation would not be correctly applied.

Digitisation of the Judiciary

In July 2023, the Council of Ministers approved a preliminary draft law on the digitisation of the Judiciary that made changes to various laws. These include a legal framework for keeping criminal records in a central registry, the retention period of electronic voting data and the registration of fingerprints in the European Criminal Records Information System. Specifically as regards intelligence, the draft proposed expanding the definition of methods officer (appointed to monitor the use of special intelligence methods) so that more personnel could apply for the position. In its opinion, the Committee stressed the importance of specific training for the staff tasked with internal verification of the conditions for the implementation of special intelligence methods. The Committee was of the opinion that any appointment of a methods officer by the Administrator General of State Security or the head of GISS should be made on the advice of the SIM Commission.

The integration of the National Security Authority into State Security

Until the end of 2023, the National Security Authority (NSA) was a collegial body that included both State Security and GISS, which reported to the Federal Public Service (FPS) Foreign Affairs. By law of 7 April 2023, the powers of the NSA were split between the Federal Police, which is now responsible for issuing and revoking security clearances, and the NSA, in charge of issuing and revoking security clearances and monitoring applicable security standards regarding the processing and storing of classified information. The NSA has been part of State Security since 1 January 2024, as an autonomous entity. In this context, three draft royal decrees were submitted to the Committee for opinion, which define the operation and organisation of this National Security Authority. Among other things, the Committee called into question the powers of delegation of the Administrator-General of State Security.

Port security plans and the role of the intelligence services

In September 2023, the Committee, in its capacity as Competent Supervisory Authority, was asked for its opinion on the draft law amending the Belgian Shipping Code. The amendment essentially aims to improve maritime security in Belgium in response to rising drug-related crime in and around port areas. It includes provisions on additional security checks, the introduction of security verifications for certain positions, integrity policies and regulations for cameras. The intelligence services are subject to the rules governing the installation and use of cameras in port facilities and ports. The draft also provided for procedures for accessing camera images, and audio recordings by the intelligence services. As regards this last aspect, the Committee requested that the intelligence services' access to information from cameras be uniformly regulated in the Intelligence Services Act.

New laws and regulations

Various laws and regulations were amended in 2023 regarding the operations, competences and control of the intelligence and security services and intelligence work.

Already in early January 2023, the *Act of 8 December 2022 on the reporting channels and the protection of persons notifying of violations of integrity in federal government agencies and the integrated police (BOJ 23 December 2022)* came into force. The new reporting system consists of three possibilities: internal reporting, external reporting and public disclosure. The external reporting channel for integrity breaches within federal government agencies was set up at the Federal Ombudsman services. Exceptions were nevertheless provided for. For example, the legislator designated the Standing Committee I as the external reporting channel authorised to receive and follow up reports of violations of integrity within State Security and GISS. This is an additional task for the Standing Committee I, which, as an external reporting channel, will now be responsible for providing information on the content and application of the law, receiving and following up reports of integrity breaches, as well as protecting individuals against reprisals. The law uses a specific definition of a violation of integrity; for example, workplace harassment, violence and unwanted sexual conduct, as well as violations of discrimination laws, do not fall within the scope of the whistleblower law.

On 14 February 2023, the *Act consenting to the cooperation agreement of 30 November 2022 between the Federal State, the Flemish Region, the Walloon Region, the Brussels-Capital Region, the Flemish Community, the French Community, the German-speaking Community, the French Community Commission and the Common Community Commission establishing a mechanism for screening foreign direct investment (BOJ 7 June 2024)* was approved. As a result, the Inter-Federal Screening Mechanism (ISM) for foreign investment entered into force. The main task of the ISM is to analyse direct investments from third countries (whether through an EU company or not) that acquire a certain percentage of voting rights in a company based in Belgium, and to assess whether they pose potential risks to national security and strategic interests. The ISM can therefore identify potential threats and take preventive measures to protect sensitive national sectors, such as critical infrastructures and technologies, commodities, energy, or even defence. Since 1 July 2023, State Security has also played an important role in screening foreign direct investment in critical sectors. Indeed, a cooperation agreement provides that the Coordination Committee on Intelligence and Security (CCIV) will be consulted for any investment under the scrutiny of the ISM. State Security is responsible for assessing whether new foreign investments pose a risk to the interests it is tasked with protecting.

Based on an opinion from the Centre for Cybersecurity Belgium (CBB) and the intelligence services, the National Security Council decided, in *Circular No. 716 of 17 March 2023 Temporary Ban on the Use of the TikTok Application (BOJ 31 March 2023)*, to prohibit federal government personnel from installing and using the TikTok application on work devices, and recommended not installing it on personal devices with access to internal federal government networks. On 14 September 2023, the National Security Council decided to extend the application of the circular for six months.

On 7 April 2023, the *Royal Decree amending the Royal Decree of 23 January 2012 on the award of public contracts and certain contracts for works, supplies and services in the field of defence and security (BOJ 2 June 2023)* was approved. This amendment gave contracting authorities and public companies awarding public contracts of limited value (≤ €30,000) in the field of defence and security the same flexibility as for public contracts in the traditional sectors.

The *Royal Decree of 7 April 2023 amending the Royal Decree of 14 January 1994 on the status of the Administrator General and Deputy Administrator General of State Security and the Royal Decree of 5 December 2006 on the general administration and support cell of State Security (BOJ 17 April 2023)* was enacted on the same day. This will now make it possible to appoint a temporary replacement when the Administrator General or their deputy are absent for at least six months.

Perhaps the most far-reaching change for the intelligence community came with the *Act of 7 April 2023 amending the Act of 11 December 1998 on classification and security clearances, security certificates and security advice (BOJ 9 June 2023)*. The legislator was obliged to bring the provisions of the Classification Act of 11 December 1998 into line with the applicable international obligations, including those on information security. The National Security Authority has also been given additional powers,

and a legal framework is provided for the so-called 'public regulated service' of Galileo, the EU's global satellite navigation system.

With this law, the legislator provides for a number of amendments, so that communication in the international context and, more specifically, the exchange of classified information can be smoother, more efficient and more harmonised. As such, in addition to 'confidential', 'secret' and 'top secret', there will now be a fourth classification level: 'restricted'. The minimum protection measures will be adapted to this new classification. These measures are now divided into five categories, namely measures applicable to the management of classified information, personal security, protection measures associated with government contracts, physical security and the security of communication and information systems.

The main change in this regard is that the National Security Authority (NSA) will have several additional powers. The legislator also provided for a new organisational structure: the NSA will no longer consist of collegial cooperation between 9 federal government departments with a secretariat brought under the FPS Foreign Affairs (*supra*), but will become part of State Security. Moreover, the NSA will also no longer have powers to issue and revoke security certificates and issue security advice. These powers will be transferred to the Federal Police. An implementing decree will clarify this new structure and organisation during the course of 2024. The legislator has already confirmed the NSA's new powers. Among other things, it will be responsible for drafting Belgian security policy regarding the protection of classified information, monitoring the implementation of protection measures, issuing, modifying, suspending and revoking security clearances and approvals of physical installations, communication and information systems and cryptographic products.

With this law, the legislator also (again) created a new security screening: all military personnel and civilians in the Ministry of Defence will gradually be subject to a security verification at least every five years and will have to have a positive security advice at all times.

The legislator has also provided for the possibility of charging a fee for both the private and public sectors for all approvals issued by the NSA. Among other things, this is stipulated in Articles 46 and 47 of the *Act of 31 July 2023 to make the judiciary more humane, faster and stricter IV (BOJ 9 August 2023)*. The legislator has provided that the NSA, from now on reporting administratively to State Security, will be set up as an administrative department with accounting autonomy for the collection of fees.

Elsewhere, the Royal Decree of 4 June 2023 on maritime security (BOJ 26 June 2023) regulates the operation of the Maritime Security Cell, the National Authority for Maritime Security (NAMB) and the local Maritime Security Committees within the Directorate General (DG) Shipping of the FPS Mobility and Transport. The Maritime Security Cell is responsible for the day-to-day operations and monitoring of NAMB, a consultative body headed by the Director General of DG Shipping. This authority monitors security at ports and port facilities. From now on, NAMB will consist of the Director General of DG Shipping, the National Crisis Centre, State Security, Customs, Defence, GISS, CUTA and the Maritime Police.

Following the "La Quadrature du Net" judgment (Court of Justice of the European Union, 6 October 2020), the subsequent judgment of the Constitutional Court of 22 April 2021 (Judgment No. 57/2021) and the judgment of the same court No. 58/2021 of 18 November 2021, the legislator amended, among other things, the Act of 13 June 2005 on electronic communications through the Act of 20 July 2022 on the collection and retention of identification data and metadata in the electronic communications sector and the provision thereof to the authorities. As an extension, the *Royal Decree of 4 October 2023 on the retention of data by electronic communications operators for the authorities, in accordance with Articles 126 to 126/3 of the Act of 13 June 2005 on electronic communications and statistics on the communication of these data to the authorities* was published on 13 October 2023 in the Belgian Official Journal.

There has also been a lot of activity at the European level as well. With the *Act of 7 April 2023 consenting to the Additional Protocol to the Council of Europe Convention on the Prevention of Terrorism, done at Riga on 22 October 2015 (BOJ 24 May 2023)*, this Additional Protocol - ratified on 11 May 2023 - entered into force for Belgium on 1 September 2023. A number of new activities have now been criminalised as terrorist offences (e.g., receiving terrorist training, (financing) travelling abroad for terrorist purposes, etc.). In addition, the protocol requires member states to take the necessary measures to exchange all available information on persons travelling abroad for the purposes of terrorism, in good time.

The *Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 pursuant to Regulation (EU) 2016/679 of the European Parliament and the Council on the adequacy of the level of protection*

of personal data under the EU-US Data Privacy Framework was published in the Official Journal of the European Union on 20 September 2023. The Commission notes in this Decision that legislative changes have been made in the United States that now allow the transfer of personal data from the European Union to certain U.S. bodies.

Regulation (EU) 2023/2131 of the European Parliament and of the Council of 4 October 2023 amending Regulation (EU) 2018/1727 of the European Parliament and of the Council and Council Decision 2005/671/JHA, as regards digital information exchange in terrorism cases, was also published in the same Official Journal on 11 October 2023. Among other things, the regulation strengthens the requirements for the exchange of information regarding the investigation and prosecution of terrorist offences between national authorities and the European Union Agency for Criminal Justice Cooperation (Eurojust).

Also, the *Act of 12 February 2023 consenting to the Agreement between the Kingdom of Belgium and the Kingdom of the Netherlands on the exchange and mutual protection of classified information, done at Brussels on 5 November 2019 (BOJ 20 April 2023)* regulates the general framework for the protection and security of classified information exchanged between the two neighbouring countries.

Nevertheless, Belgium still needs to ratify *Council of Europe Convention 108+* (supra). This convention is the first international treaty that pertains more specifically to national security and therefore the intelligence and security services. It provides safeguards for the careful gathering and processing of data, and lays down principles regarding independent and effective review and supervision. The European Parliament recently adopted recommendations highlighting the importance of Convention 108+ for EU member states (P9_TA(2023)0244 dated 15 June 2023). Among other things, the European Parliament "urges all Member States to ratify this convention without delay, to already implement its standards in national law and to act accordingly over national security" (para. 47). Many countries - including France on 27 March 2023 - have since overtaken Belgium and ratified the Convention. The Standing Committee I calls for Belgium to quickly sign up to it, thereby endorsing the standards of the Convention.

6. MONITORING OF THE COMMON DATABASES

MONITORING OF THE COMMON DATABASES

In 2016, the joint 'foreign terrorist fighters' database was set up by the Ministers of the Interior and Justice. This common database (CDB) was transformed into the common database 'terrorist fighters' (CDB TF) in 2018 and, in addition to the general category of 'foreign terrorist fighters' also includes a category of 'homegrown terrorist fighters'. In addition, a separate common database for 'hate propagandists' (CDB HP) was also set up in 2018. By royal decree at the end of 2019, two additional categories of individuals were included in the CDB TF, namely the 'potentially violent extremists' (PVE) and 'persons convicted of terrorism' (PCT).

Article 44/11/3quinquies/2 of the Policing Service Act entrusts the supervision of the processing of the information and personal data contained in the CDB to the Supervisory Body for Police Information (COC) and to the Standing Committee I.

Control

For the 2022 Report, produced in 2023, the COC and the Standing Committee I decided to focus their joint supervision on the follow-up of previous recommendations and on the use of common databases by the intelligence and security services. The follow-up on the recommendations of the 2021 review investigation into the radicalisation of a staff member of Defence was also included in the evaluation.

The services involved, namely the Federal Police, State Security and GISS, were surveyed in writing. An extract of the log data regarding the processing activities carried out by the two intelligence and security services was requested from the Federal Police. The full report is available on the website of the Standing Committee I.

Opinion

The Policing Act also stipulates the obligation to seek a joint opinion from the Standing Committee I and the COC, in various cases.

For example, plans to set up any new common database must be submitted in advance to the Standing Committee I and the COC for joint consultation. In addition, after consulting the above-mentioned control bodies, for each common database, a royal decree established after consultation in the Council of Ministers specifies the types of personal data processed, the rules in terms of the responsibilities in the area of protecting the privacy of the bodies, services, authorities and organisations that process data, the rules in terms of the security of the processing, the rules of the use, retention and exchange of the data. Furthermore, additional management rules for the common databases may be specified by a Royal Decree adopted after consultation in the Council of Ministers, but again after an opinion is given by the Committee and the COC. Finally, the opinion remit also extends to any draft royal decree establishing or modifying access to the common databases.

Following the case of the radicalised soldier in 2021, as well as the deadly attack on two police officers in Schaerbeek, the Ministers of Justice and the Interior commissioned a comprehensive study into what interventions are needed to improve the functioning of the common database and the security structure around it. Based on this analysis, the ministers elaborated a draft law and a draft royal decree[2]. The COC and the Standing Committee I each issued their opinions on the matter (available for consultation on the Standing Committee I website).

2 Preliminary draft law establishing the common database 'Terrorism, Extremism, Radicalisation Process (TER)' and amending the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, the Act of 30 July 2018 establishing local integral security cells on radicalism, extremism and terrorism and the Act of 5 August 1992 on the police service and the Draft Royal Decree on the common database 'Terrorism, Extremism, Radicalisation Process (TER)'.

7. INTERNAL FUNCTIONING

INTERNAL FUNCTIONING

Composition

The composition of the Committee changed in 2023: Serge Lipszyc, first substitute labour auditor at the Labour Auditor's Court of Liège, continued to serve as Chairman. Thibaut Vandamme, Deputy Public Prosecutor of the District of Luxembourg exercised the mandate of counsellor. Pieter-Alexander De Brock was replaced as counsellor on 28 March 2023 by Linda Schweiger, general advisor at the Ministry of Defence. The Investigation Service I consisted of six commissioner-auditors; the administration, headed by Registrar Frédéric Givron, had 15 employees.

Parliamentary Monitoring Committee

The composition of the Special Committee entrusted with the parliamentary monitoring of the Standing Police Services Monitoring Committee and the Standing Intelligence Agencies Review Committee (the Monitoring Committee) underwent several changes in 2023. The following served on the committee as voting members: Peter Buysrogge (N-VA), Yngvild Ingels (N-VA), Julie Chanson (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 Boukili (PVDA-PTB), Tim Vandenput (Open Vld) and Meryame Kitir (Vooruit). President of the Chamber Eliane Tillieux (PS) chaired the committee. Georges Dallemagne (Les Engagés) participated as a non-voting member.

Five meetings took place behind closed doors in 2023 during which various review investigations conducted by the Standing Committee I and the internal functioning of the Committee were discussed.

Joint meetings with the Standing Committee P

Article 52 of the Review Act provides that joint meetings must take place between the Standing Committee I and the Standing Committee P at least twice a year. During 2023, several meetings took place in connection with joint review investigations and complaints jointly investigated by both Committees.

Budget

The total budget approved by the Chamber of Representatives for 2023 was €4,933,170, and is made up of €3,317,000 allocated funds and €1,616,170 bonuses from 2022. Of these, personnel costs account for the lion's share of the budget (> 80%).

Digitisation

In late 2023, the Standing Committee I was granted a special budget by the Chamber of Representatives with a view to realising a large-scale digitisation project, to modernise its operations. This is a crucial step in streamlining administrative tasks.

Synergies

The Standing Committee I is and remains fully engaged in the search for synergies with the other institutions of the Chamber entitled to receive allocated funds. In April 2021, an agreement was reached within the Commission on Accountability on the synergies to be created between the institutions in question. The Committee participates in the working groups set up in this context (central management of synergies, ICT, harmonised statuses and government contracts). Their work continued throughout 2023. Among other things, tangible results have already been achieved in terms of sharing service vehicles.

8. INTERNATIONAL COOPERATION

INTERNATIONAL COOPERATION

- Increased international data sharing between intelligence and security services entails challenges for national oversight bodies. The oversight bodies of (originally) five European countries (Belgium, Denmark, the Netherlands, Norway and Switzerland) have therefore been deliberating for several years to meet these challenges by finding ways to reduce the risk of an 'oversight gap' (International Oversight Working Group (IOWG)). The group has since expanded to include Sweden and the United Kingdom.

  A staff meeting of the IOWG was held in The Hague in May 2023. Following a brief presentation by delegations on the most recent developments within their respective oversight bodies, a variety of topics were addressed, ranging from the challenge of communications and transparency to technical cooperation, Convention 108+ and the acquisition of commercially available datasets by intelligence services. Preparations were also made ahead of the meetings in November 2023.

  A new meeting of the IOWG was held in Oslo in November 2023, which included a staff meeting and a chair meeting with the heads of the various oversight bodies. Following a brief presentation of the latest developments within their respective bodies, the agenda of discussion topics was updated. The IOWG decided to work on the following priorities: (i) organising more technical meetings, possibly in the form of hackathons, on the topic of artificial intelligence; (ii) strengthening the use of the shared digital environment of the IOWG; (iii) jointly tackling communication and transparency challenges in the context of the work on monitoring primarily classified activities; (iv) continuing exchanges on technical cooperation, on monitoring in general, and on certain specific topics, such as the acquisition by intelligence services of commercially available datasets and Convention 108+. Preparations also began for the staff meeting of the IOWG to be hosted by the Standing Committee I in Brussels in April 2024.

- The presence in Oslo also provided an opportunity to participate in the European Intelligence Oversight Conference. This conference brought together representatives of intelligence oversight bodies from 16 countries, as well as participants from external organisations. The themes of the conference were the use of commercially available data, audit planning, the recent jurisprudence of the European Court of Human Rights, the technical basis for effective oversight, and the opportunities and challenges for accountability and communication.

- In late September 2023, the Standing Committee I received a delegation from the parliamentary committee responsible for oversight over the intelligence and security services of the German state of Brandenburg. Over the course of this two-day working visit, the Committee explained the Belgian institutional and security architecture to the German delegation, as well as the legal missions of the Standing Committee I, through a series of presentations, followed by discussions and sharing of experiences. In addition, the President of the Chamber, who also presides the Monitoring Committee, received the delegation, the Committee and several of its staff for an exchange of views.

- Finally, at the end of November 2023, a delegation of the Standing Committee I in Washington took part in the annual International Intelligence Oversight Forum (IIOF). The IIOF aims to be an international platform for intelligence, privacy and data protection regulators, and other stakeholders, including intelligence and security services, to discuss (inter)national developments and best practices.

APPENDICES

Abbreviations

BOJ	Belgian Official Journal
CDB	Common Database
Classification and Security Clearances Act	Act of 11 December 1998 on classification, certificates and advice
COC	Supervisory body for police information
Convention 108	Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
CUTA	Coordination Unit for Threat Analysis
CUTA Act	Act of 10 July 2006 on threat analysis
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
GISS	General Intelligence and Security Service
GND	General National Database
Intelligence Services Act (ISA)	Act of 30 November 1998 governing the intelligence and security services
IOWG	Intelligence Oversight Working Group
Monitoring Committee	Special Committee entrusted with the parliamentary oversight of the Standing Police Services Monitoring Committee and the Standing Intelligence Agencies Review Committee
NSA	National Security Authority
SIM	Special Intelligence Methods
SIM Commission	Administrative Commission responsible for monitoring the specific and exceptional methods of data collection by the intelligence and security services
Policing Act	Act of 5 August 1992 on the police service
Review Act	Act of 18 July 1991 governing the review of the police and intelligence services and the Coordination Unit for Threat Analysis
Standing Committee I	Standing Intelligence Agencies Review Committee
Standing Committee P	Standing Police Services Monitoring Committee
T.E.R. Strategy	Strategic Paper Extremism and Terrorism