



**BELGIAN STANDING INTELLIGENCE AGENCIES
REVIEW COMMITTEE**



**ACTIVITY REPORT
2024**

All rights reserved. Subject to the exceptions expressly provided for by law, no part of this publication may be reproduced, stored in an automated database or published in any way whatsoever without the express prior consent of the publishers.

Despite all the care taken in compiling the text, neither the authors nor the publisher accept any liability for any damage that may result from any error that may appear in this publication. The Dutch and French language versions of this report are the official versions. In case of conflict between those versions and the English translation, the meaning of the former shall prevail.

© Cover photo Kurt Van den Bossche
© Photo of the Committee Alain Janquart

Graphic work and layout: Central Printing Office of the Belgian 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° every year, through a general activity report which may, if necessary, contain general conclusions and proposals and which covers the period from 1 January to 31 December of the previous year. This report shall be transmitted 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 of data collection referred to in Article 18/2 of the Act of 30 November 1998 governing the intelligence and security services, to the application of Chapter IV/2 of the same Law 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 on 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 have the possibility to draw the attention of the Standing Committee I to their remarks. The report shall detail the number of authorisations given, the duration of the exceptional methods for collecting data, the number of persons involved and, where appropriate, the results obtained. The report shall also cover the activities of the Standing Committee I. The elements contained in the report must not affect the smooth operations 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 advice it has given in its capacity as data protection authority, on the investigations carried out and the measures taken in the same capacity, as well as on its cooperation with the other data protection authorities. A copy of this report shall also be addressed to the competent ministers, as well as to State Security and the General Intelligence and Security Service, who have the possibility to inform the Standing Committee I of their remarks.

Brussels, 15 April 2025



From left to right: Frédéric Givron, Registrar – Vanessa Samain, Chairwoman – Séverine Merckx, Councilwoman – Linda Schweiger, Councilwoman

PREFACE

“Change is difficult, not to change is fatal”

Having been in office since 25 September 2024, I am extremely proud to write the introduction to the present activity report. Educational outreach is part of our democratic role and that is exactly what our activity report aims to do. As a public service, we attach great importance to this aspect. This report presents a summary of the work completed that goes beyond simply meeting our obligation of accountability. It is intended to have an educational purpose, and gives us an opportunity to explain to citizens, researchers and journalists, etc., who we are, what our vision for the future is and, more specifically, what we can do for this diverse audience by performing our statutory missions.

As I look back on 2024, various words come to mind, but the most important is undoubtedly ‘renewal’. An initial observation stands out in this regard: the Standing Committee I was set up in 1991 and literally dates back to the last century... The Committee’s remit has since been significantly expanded. It started as a review committee for the intelligence and security agencies, but, 30 years later and in an ever-changing society, it finds itself tasked with more than 19 different missions, including that of appeal body on security clearances and data protection authority.

With this in mind, and with a new management team in place, 2024 was the ideal time to look to the future and modernise the Committee. And modernisation means digitisation. Like other institutions, the Committee embraces this challenge! Considerable budgetary and human resources were set aside in this regard in 2024. This digitisation process is anything but straightforward, not least on account of the confidentiality of the data the Committee handles. It will take time and energy, but we are determined to make it a success; going back is not an option.

The Committee’s activity report is not only a review of the past year, it also provides an opportunity to look ahead. In 2025, talking about the future means taking into account the current geopolitical context, which is particularly concerning for citizens. Hybrid threats, war on Europe’s doorsteps, foreign interference, industrial espionage, daily cyber-attacks, etc. Threats to national security are steadily increasing, but the diverse forms they take is of particular concern. They are more insidious and complicate the task of the intelligence and security services.

Against this background, the Committee will be more attentive than ever to its role as a democratic watchdog. The missions of the intelligence and security services in these troubled times are crucial. But the role of the Committee is just as important. If the Committee wants to continue performing its democratic function correctly, its vigilance and available resources must be commensurate with those of our intelligence and security services.

Finally, I would like to acknowledge the exceptional work and resilience of our staff. Despite the many challenges, they have ensured a remarkable level of quality. I am convinced that together we can continue building a promising future for the Committee. There are excellent opportunities ahead of us and I am confident that with our dynamic team and shared vision, we will be able to seize these opportunities and convert them into lasting successes. Together, we make a difference.

I hope you find this report an enjoyable and insightful read.

Brussels, 15 April 2025

Vanessa Samain,
Chairwoman of the Standing Intelligence Agencies
Review Committee

TABLE OF CONTENTS

1. REVIEW INVESTIGATIONS.....	1
Completed review investigations	1
An Iranian delegation in Brussels	1
Threats connected to the Iranian regime	1
Terrorist attack on Swedish football supporters - two investigations	1
Interference by foreign powers	2
Monitoring elected officials	2
Amay barracks	2
Data breach	3
Ongoing review investigations	3
Analysis methodology	3
CUTA and the threats related to the Iranian regime	3
2. COMPLAINTS HANDLING.....	5
3. CRIMINAL INVESTIGATIONS AND JUDICIAL INQUIRIES	8
4. (SPECIAL) INTELLIGENCE METHODS	10
Methods used by GISS	10
Specific methods	10
Exceptional methods	10
Ordinary 'plus' methods	11
Methods used by State Security	12
Specific methods	12
Exceptional methods	12
Ordinary 'plus' methods	13
<i>Ex post</i> control	14
Foreign interceptions, recordings and IT intrusions	15

5. OPINIONS, NEW LAWS AND REGULATIONS	17
Opinions	17
The college for security opinions within GISS	17
Security verifications and the abolition of security certificates	17
Security verifications for prison staff	18
Access to the register of the Common Guarantee Fund	18
CUTA and the recognition of local communities of recognised worship	18
Voluntary service of collective benefit	18
Access to the national register of natural persons and to the population registers	19
Implementation of the amendments to the Classification and Security Clearances Act by the Act of 7 April 2023	19
The public regulated service Galileo	19
Implementation of the amendments made to the Classification and Security Clearances Act and to the Personal Data Protection Act by the Act of 2 June 2024	19
The consent of private investigators	20
Resilience of critical entities	20
New laws and regulations	21
6. APPEAL BODY	25
Number and nature of appeals lodged	25
Decisions of the Appeal Body and acts of the Registry	27
7. INTERNAL FUNCTIONING	29
Composition	29
Parliamentary Monitoring Committee	29
Joint meetings with the Standing Committee P	29
New data protection officer	29
Integrity Unit	29
Budget	30
Digitisation	30
Synergies	30
8. INTERNATIONAL COOPERATION.....	32
APPENDICES.....	33
Abbreviations	33



1.
REVIEW
INVESTIGATIONS

REVIEW INVESTIGATIONS

Completed review investigations¹

An Iranian delegation in Brussels

The Brussels Urban Summit, an international gathering of the mayors of major cities, took place in June 2023. Representatives from more than 300 cities were invited to Brussels. In this context, Belgium granted limited territorial validity visas to 14 members of an Iranian delegation. The granting of these visas, a few weeks after the release of a Belgian aid worker, was the subject of heated debate in parliament. Revelations about alleged observation and spying on opponents of the Iranian regime by members of the delegation in question further fuelled the political and media controversy.

In 2023, at the request of the Monitoring Committee, the Standing Committee I investigated the role of the Belgian intelligence and security services in the screening process in granting visas to members of this Iranian delegation, as well as the possible monitoring of their activities during the Brussels Urban Summit.²

The investigation revealed that State Security (VSSE) correctly carried out its obligations as regards the issuance of visas, despite an unclear legal framework. In this regard, State Security followed the guidelines laid down within the organisation. However, the Standing Committee I stressed that the verifications conducted by State Security should be handled with caution. Indeed, the legal framework and resources available to the service make it unreasonable to expect State Security to provide anything more than a mere 'snapshot', which is by definition a moment in time and restricted to the information available at the time checks are made.

As regards the monitoring of the activities of the members of the Iranian delegation in Brussels, no shortcomings were identified on the part of the civilian intelligence service. As regards the General Intelligence and Security Service (GISS), the Committee noted that despite its remit focused abroad, the military intelligence services do not play any role in issuing visas. As such, the service was not involved. GISS did not monitor the activities of the Iranian delegation either during the Brussels Urban Summit, as this is also outside its remit.

Threats connected to the Iranian regime

In addition to the specific case of the Iranian delegation that took part in the Brussels Urban Summit in June 2023, the Committee, at the request of the Monitoring Committee, also opened a broader review investigation in August 2023 into how the Belgian intelligence services monitored threats from Iran in the period between 2018 and 2023.³

The investigation found that there are numerous, varied threats to Belgian interests, with Iranian involvement. From espionage and interference to terrorism and extremism, or even proliferation, the Iranian issue covers a broad spectrum of threats. Although no national plan or general directive of the National Security Council is explicitly devoted to the Iranian regime, the threats it could represent are one of the priorities identified in the national security strategy. Similarly, the strategic documents setting out the priority objectives of the intelligence services also underscore the seriousness of this threat. Nevertheless, the Committee noted that the Iranian issue is primarily handled by the civilian intelligence service. While GISS is involved in a number of specific cases, it appeared that monitoring by State Security is continuous and more structured.

Terrorist attack on Swedish football supporters - two investigations

At the request of the Parliamentary Monitoring Committee, the Committee investigated the actions taken by State Security and GISS to monitor the threat of interference by foreign powers through the financing of political parties, institutions and/or individuals in Belgium.

The investigation, started in November 2023, found that both services are aware of the threat of interference and are actively conducting intelligence investigations to tackle it. Yet, these investigations focus on threats from the activities of foreign agents of influence, and not on the potential targets of this influence, including public figures and political parties or organisations.

The investigation revealed that both services have put in place a notification procedure with respect to the competent authorities (competent minister, Prime Minister, Standing Committee I)

1 The full versions of the review investigation reports are available at www.comiteri.be

2 A similar investigation was conducted with the Standing Committee P into the role of the Coordination Unit for Threat Analysis (CUTA) in this matter (the investigation was concluded in 2023 already).

3 In a separate review investigation conducted with the Standing Committee P, the threat assessment by CUTA is being examined with regard to opponents of authoritarian regimes in Belgium (see below, "ongoing review investigations").

when political representatives are associated with a threat, but these procedures are not harmonised.

It also revealed that both services regard clandestine funding as interference. Neither State Security nor GISS found any evidence that this form of interference is a major or growing problem in the Belgian political domain. Nevertheless, the Committee noted that State Security had developed the necessary expertise to conduct financial investigations. This expertise is useful for intelligence investigations not only into threats of interference, but also for other threats for which the service is competent.

In conclusion, the Committee made a number of recommendations, including that the services should intensify, systematise and coordinate their efforts to raise awareness of potential targets of interference and espionage threats, and that the two services should coordinate their notification procedures with regard to elected officials.

Interference by foreign powers

At the request of the Parliamentary Monitoring Committee, the Committee I investigated the actions taken by State Security and GISS to monitor the threat of interference by foreign powers through the financing of political parties, institutions and/or individuals in Belgium.

The investigation, started in November 2023, found that both services are aware of the threat of interference and are actively conducting intelligence investigations to tackle it. Yet, these investigations focus on threats from the activities of foreign agents of influence, and not on the potential targets of this influence, including public figures and political parties or organisations.

The investigation revealed that both services have put in place a notification procedure with respect to the competent authorities (competent minister, Prime Minister, Standing Committee I) when political representatives are associated with a threat, but these procedures are not harmonised.

It also revealed that both services regard clandestine funding as interference. Neither State Security nor GISS found any evidence that this form of interference is a major or growing problem in the Belgian political domain. Nevertheless, the Committee noted that State Security had developed the necessary expertise to conduct financial investigations. This expertise is useful for intelligence investigations not only into threats of interference, but also for other threats for which the service is competent.

In conclusion, the Committee made a number of recommendations, including that the services

should intensify, systematise and coordinate their efforts to raise awareness of potential targets of interference and espionage threats, and that the two services should coordinate their notification procedures with regard to elected officials.

Monitoring elected officials

In (parliamentary) debates, the question is regularly asked whether and to what extent the Belgian intelligence services (may) monitor elected officials and what rules must be observed in this regard.

The Committee has looked into this issue for several years, and more specifically in how the intelligence services handle information mentioning the identity of elected officials. Several previous investigations have addressed this issue.

In 2024, the Committee conducted a new review investigation to assess how often information on elected officials collected by the intelligence services was shared with the relevant authorities during the period from 1 September 2020 to 31 December 2023.

The investigation did not reveal any evidence that the intelligence services target elected officials for reasons unrelated to the interests and threats outlined in the legal framework. Nor did it appear that the fundamental rights of elected officials were violated during the collection, analysis and dissemination of information, or that these officials were treated differently (i.e. more unfavourably) than other professional groups during the operational functioning of the intelligence services.

As for reporting the possible involvement of an elected official in the emergence of a threat, the question remains as to what steps the services can/must take if the elected official is a member of the legislature. Several options were suggested by the Committee after consultation with the services. A political consensus is urgently called for to resolve this question.

Amay barracks

On 14 March 2024, in the presence of the Chief of Defence (CHOD) and the Inspector General of Defence, the then Minister of Defence gave a press conference in which she highlighted “serious structural problems” within the 4th Engineer Battalion in Amay. These problems had been reported to her through external channels in late 2023. There were reports of abuse, beatings and injuries, blackmail and threats by several dozen soldiers - officers, non-commissioned officers and volunteers - over a period of several months. The minister stated that she had immediately informed the Chief of Defence and the Inspector General of Defence, following

which an internal investigation was launched. Preventive suspensions (pending sanctions) and transfers were rapidly implemented. Given the seriousness of the allegations, the judicial authorities were also informed.

At the request of the Monitoring Committee, the Standing Committee I opened a review investigation into the information position of GISS regarding these facts. The Committee first examined the question of whether GISS was competent on this matter. It concluded that the service was competent not only on the basis of its intelligence remit, but also and above all on the basis of its security remit, and in particular its mission to (freely translated) “*safeguard the military security of personnel under the Minister for Defence, military installations, weapons and weapons systems, ammunition, equipment, plans, writings, documents, computer and connection systems or other military objects*” (art.11 §1, 2° ISA).

The investigation revealed that GISS was confronted with two distinct cases that took place at the Amay barracks, with no apparent connection between them. One case involved weapons and drug trafficking, which was the subject of a judicial investigation (which had been concluded at the time of the investigation); the other involved drugs, weapons and sex offences (which were still under judicial investigation).

The Committee concluded that GISS appeared to have been among the first to be informed of the allegations, and had carefully handled them. Nevertheless, the Committee was cautious in its conclusions, as a series of judicial investigations were still ongoing. Several internal research reports were not available for the time being.

Data breach

The intelligence agencies are obliged to notify the Standing Committee I, in its capacity as Competent Supervisory Authority for the processing of personal data, of data breaches as soon as there is a risk to the fundamental rights and freedoms of the persons whose personal data have been leaked. In June 2023, the Committee was informed by one of the intelligence service that the latter had been subject to a data breach. This notification led to a review investigation being opened. The report was concluded in 2024 and contained several recommendations. As the report was fully classified, it was only handed over to the service in question and the responsible minister.

Ongoing review investigations

Analysis methodology

During review investigations or when handling 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 launched two investigations to understand, on the one hand, the methodology used by the intelligence and security services to assign such qualifications to a person of interest. On the other hand, jointly with the Standing Committee P, it examines the method of analysis used by the Coordination Unit for Threat Analysis (CUTA) to this end.

CUTA and the threats related to the Iranian regime

Alongside the review investigation into how the intelligence services monitored the activities of the Iranian regime between 2018 and 2023 (supra), a joint investigation was launched with the Standing Committee P to examine CUTA's assessment of the threat against opponents of authoritarian regimes 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 is also competent to deal with 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.

2024	STANDING COMMITTEE I	STANDING COMMITTEES I AND P	TOTAL
1. Submitted complaints	57	11	68
2. Inadmissible complaints	44	0	44
3. Admissible complaints	13 ⁴		24
	State Security	8	
	GISS	1	
	State Security & GISS	4	
4. Pending cases	2	0	2
5. Ongoing cases	2	2	4
6. Admissible closed cases	9	9	18
7. Corrective measures	0	2	2

The table above gives an overview of the cases handled in 2024 (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 the CUTA part of the case and in the cases handled exclusively by the Standing Committee I with respect to investigative acts relating to State Security.

In 2024, the Standing Committee I received a total of 68 complaints and reports. Following a brief preliminary investigation and verification of various objective data, the Committee rejected 44 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).

⁴ Of which 9 were DPA complaints.

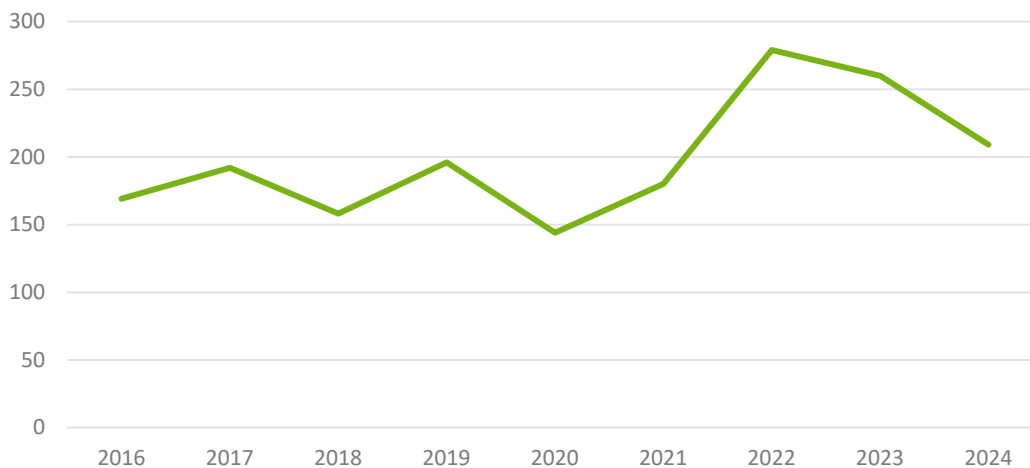
Complaints handling

18 of the admissible complaints filed in 2024 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. When complaints are declared admissible, the Committee instructs its Investigation Service to carefully investigate the complaint and issue a (classified) report.

The way in which the data is shared with foreign partners is the focus of increasing attention from the Committee, which is regularly seized by applicants who have encountered problems with border controls abroad. As supervisory authority for the processing of personal data by the intelligence services, the Committee imposed corrective measures in two cases (art. 51/3 Review Act). Depending on the case, this may involve requesting rectification or deletion of personal data, communicating the Committee's decision to partners and/or authorities, or disseminating the decision within the service concerned. Given the complexity of the topic, the Committee regularly calls on the expertise of its legal department.

20 handled complaints were closed in 2024, 4 complaints were still pending at the start of 2025. Compared to previous years, a slight rise 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 2024, State Security appears to be significantly represented..

**Admissible complaints
(2016-2024 overview)**





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 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 Chair of the Standing Committee I must ensure that the performance of the Committee's other legal remit is not disrupted.

In 2024, the Investigation Service I continued its investigation in the context of complaints lodged by State Security against 'X' for alleged breaches of professional secrecy within the service. Several official reports were drawn up at the request of the Brussels public prosecutor's office. These investigations were ongoing as of 31 December 2024.

Once the judicial investigation is completed, the Investigation Service must send a report to the Chair 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 2024.

Furthermore, article 50 Review Act states that (freely translated) *"each member of a police service who identifies a crime or offence committed by a member of an intelligence service shall make an informative report thereon and hand it over to the head of the Investigation Service I within 15 days"*. The Investigation Service received no such reports in 2024.



4.
(SPECIAL)
INTELLIGENCE METHODS

(SPECIAL) INTELLIGENCE METHODS

The Committee is tasked with the *ex post* control of the use of special intelligence methods (SIM). This control relates to the legality, proportionality and subsidiarity of these methods. The following section reports on the number and nature of methods used by the services, and how they are monitored.

Between 1 January and 31 December 2024, **1342 SIM files** were drawn up by the two intelligence services together for the use of special intelligence methods: **1,144 SIM files by State Security** (764 files related to specific methods and 380 to exceptional methods) and **198 SIM files by GISS** (86 files related to specific methods and 112 to exceptional methods). It should be noted that a SIM file may de facto consist of the use of one or more methods. In order to obtain an overarching quantitative overview, the Committee took into account the number of actual methods used by the services. As a result, the figures are obviously higher: a total of **2,937 special intelligence methods were used** by both services: **674 methods used by GISS and 2,263 methods used by State Security**, respectively. All files were subject to a check.

Methods used by GISS

Between 1 January and 31 December 2024, 674 special intelligence methods were used by GISS, of which **360 were specific methods and 314 exceptional methods**.

The tables and charts below detail the intelligence methods used by GISS during 2024.

Specific methods (GISS)	2024
Observing in publicly accessible places using technical means, or observing whether or not using technical means in a place not accessible to the public and not hidden from view (art. 18/4 §§ 1 and/or 2 ISA)	47
Real Time retrieval of police camera images (publicly accessible places) (18/4 §3 ISA)	22
Searching publicly accessible places with technical means, searching the contents of locked objects or removing these objects (art. 18/5 ISA)	2
Infiltrating the virtual world under a false identity or fictitious capacity (art. 18/5/1 ISA)	0
Inspection of identification data for postal traffic and requesting cooperation of a postal operator (art. 18/6 ISA)	0
Requesting transport and travel data from private transport and travel services (art. 18/6/1 ISA)	2
Identification, using technical means, of the electronic communication services and means subscribed to by a specific person or that are commonly used by a specific person (art. 18/7 §1, 1° ISA)	17
Requesting the assistance of the operator of an electronic communications network to obtain payment method data and identify the means and time of payment for the subscription to or use of the electronic communications service (art. 18/7 §1, 2° ISA)	1
Tracing traffic data of electronic means of communication and requesting the cooperation of an operator (art. 18/8, §1, 1° ISA)	137
Monitoring localisation data for electronic communications and requesting cooperation from an operator (art. 18/8, §1, 2° ISA)	132
TOTAL	360

Exceptional methods (GISS)	2024
Observing, whether or not using technical means, in places inaccessible to the public and hidden from view and entering places inaccessible to the public, whether or not hidden from view, in order to observe, install technical means, open or remove an object (art. 18/11 ISA)	15
Searching, whether or not using technical means, places inaccessible to the public, as well as locked or unlocked objects located there (art. 18/12 ISA)	16
Infiltration into the real world (art. 18/12/1 ISA)	0
Opening and recording post, whether or not entrusted to a postal operator (art. 18/14 ISA)	12
Collecting data on bank accounts and banking transactions (art. 18/15 ISA)	11
Penetrating a computer system (art. 18/16 ISA)	68
Tapping, intercepting and recording communications (art. 18/17 ISA)	177
TOTAL	314

In 2024, a decrease in the number of special intelligence methods was observed for GISS. Although the two most frequently used specific methods remain the tracing of traffic data of electronic means of communications and the monitoring of the origin or destination of electronic communications (art. 18/8, §1, 1° and 2° ISA), these methods were used much less often compared to 2023. Conversely, the use of real-time retrieval of police camera images nearly doubled. As regards exceptional methods, like in 2023, the most commonly used methods were penetrating computer systems (art. 18/16 ISA) and tapping communications (art. 18/17 ISA). Although opening post is used much less than the two methods mentioned above, this method was used twice as often in 2024 compared to 2023.

As in 2023, special intelligence methods were most commonly used in 2024 with regard to the espionage threat. Monitoring the threats of extremism and terrorism as well as organised crime required the use of significantly fewer intelligence methods than in 2023.

Ordinary 'plus' methods

Originally, ordinary intelligence methods were only subject to regular control by the Committee. However, several 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.

The use of these methods by GISS is lower compared to 2023. However, the reduction is limited, with the exception of the use of police camera images, which has halved, and targeted searches of passenger name record (PNR) data collected by the Passenger Information Unit, which has fallen even more sharply. This reduction is due to the fact that GISS could not access the PNR database following the ruling of the Constitutional Court of 12 October 2023 overturning Article 16/3 ISA.⁵ A remedial act passed by the legislator and adopted on 15 July 2024 allows intelligence services once again to search the PNR database a second time, explaining why these methods were resumed in mid-2024.

⁵ In its ruling (131/2023), 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 violated 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 ISA that regulated requests in the Intelligence Services Act. Until the entry into law of the Remedial Act, the intelligence services could no longer access the PNR database.

Ordinary 'plus' methods (GISS)	2024
Identification of the a telecommunication user (art. 16/2 ISA)	432
Targeted PNR data searches (art. 16/3/1 ISA)	7
Use of police camera images (art. 16/4, §2 ISA)	18
Requesting financial data (art. 16/6 ISA)	23

Methods used by State Security

Between 1 January and 31 December 2024, State Security granted 2,263 authorisations to use special intelligence methods, of which **1,630 were specific and 633 exceptional methods**.

The tables and charts below detail the intelligence methods used by State Security during 2024.

Specific methods (State Security)	2024
Observing in publicly accessible places using technical means, or observing whether or not using technical means in a place not accessible to the public and not hidden from view (art. 18/4 §§ 1 and/or 2 ISA)	245
Real Time retrieval of police camera images (publicly accessible places) (18/4 §3 ISA)	0 ⁶
Searching publicly accessible places with technical means, searching the contents of locked objects or removing these objects (art. 18/5 ISA)	0
Infiltrating the virtual world under a false identity or fictitious capacity (art. 18/5/1 ISA)	0
Inspection of identification data for postal traffic and requesting cooperation of a postal operator (art. 18/6 ISA)	0
Requesting transport and travel data from private transport and travel services (art. 18/6/1 ISA)	70
Identification, using technical means, of the electronic communication services and means subscribed to by a specific person or that are commonly used by a specific person (art. 18/7 §1, 1° ISA)	52
Requesting the assistance of the operator of an electronic communications to obtain payment method data and identify the means and time of payment for the subscription to or use of the electronic communications service (art. 18/7 §1, 2° ISA)	6
Tracing traffic data of electronic means of communication and requesting the cooperation of an operator (art. 18/8, §1, 1° ISA)	634
Monitoring localisation data for electronic communications and requesting cooperation from an operator (art. 18/8, §1, 2° ISA)	623
TOTAL	1630

6 The use of this method is not recorded separately and, where appropriate, is included in the figures relating to methods art. 18/4 §§ 1 and 2.

Exceptional methods (State Security)	2024
Observing, whether or not using technical means, in places inaccessible to the public and hidden from view and entering places inaccessible to the public, whether or not hidden from view, in order to observe, install technical means, open or remove an object (art. 18/11 ISA)	21
Searching, whether or not using technical means, places inaccessible to the public, as well as locked or unlocked objects located there (art. 18/12 ISA)	31
Infiltration into the real world (art. 18/12/1 ISA)	0
Opening and recording 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)	59
Penetrating a computer system (art. 18/16 ISA)	117
Tapping, intercepting and recording communications (art. 18/17 ISA)	380
TOTAL	633

The total number of special intelligence methods used by State Security increased in 2024, compared to the previous year. This concerns the following methods in particular: tracing traffic data of electronic means of communication, monitoring the origin or destination of electronic communications (art. 18/8, §1, 1° and 2° ISA) and requesting transport and travel data from private transport and travel services (art. 18//6/1 ISA). The latter method, which was used significantly more compared to 2023, allowed State Security to obtain transport information despite the fact that the intelligence services were unable to access the PNR database until mid-July 2024 (see above). As regards exceptional methods, like GISS, the methods used most often were the same as in 2023, namely penetrating computer systems (art. 18/16 ISA) and tapping communications (art. 18/17 ISA). Collecting bank data was the third most used exceptional method by State Security in 2024. Conversely, this is one of the least used exceptional methods at GISS. This difference was also observed in 2023. It was also observed that while in 2023 there was a significant decrease in the number of observations of places inaccessible to the public, the use of this method more than doubled in 2024.

Terrorism and espionage are the priority threats monitored by the civilian intelligence service. In addition, State Security also closely monitors threats of interference and extremism. Since 2022, State Security has also reinvested against the threat of organised crime, specifically threats to our state institutions and government services such as the police, customs and justice, as well as threats to the political world.

Ordinary 'plus' methods

The use of these methods by State Security saw a relative increase in 2024. The use of targeted PNR data searches fell dramatically, and for the same reasons as for GISS (*supra*).

Ordinary 'plus' methods (State Security)	2024
Identification of a Telecommunication user (art. 16/2 ISA)	5543
Targeted PNR data searches (art. 16/3/1 ISA)	74
Use of police camera images (art. 16/4, §2 ISA)	76
Requesting financial data (art. 16/6 ISA)	229

Ex post control

The Standing Committee I is tasked with the *ex post* control of the use of specific and exceptional intelligence methods. This control relates to the legality, proportionality and subsidiarity of these methods.

The Committee subjects *all* SIM cases to a *prima facie* investigation, with a view to a possible referral (art. 43/4 ISA). This referral can be made on the Committee's own initiative, at the request of the Data Protection Authority (DPA), on the complaint of a citizen, by operation of law if the SIM Commission has suspended a specific or an exceptional method on the grounds of illegality and suspended the use of the information or, finally, by operation of law if the competent minister has granted an authorisation based on Article 18/10 § 3 ISA.

In addition, the Committee can also be seized in its capacity as "prejudicial consulting body" (articles 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 produced intelligence which is used in a criminal case. The decision to request an opinion lies with the investigating courts or criminal judges. Strictly speaking, the Committee then does not act as a jurisdictional body.

METHOD OF REFERRAL	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
1. On the Committee's initiative	16	12	16	3	1	1	4	2	1	5	0	0
2. Data Protection Authority	0	0	0	0	0	0	0	0	0	0	0	0
3. Complaint	0	0	0	1	0	0	0	0	0	0	0	2
4. Suspension by SIM Commission	5	5	11	19	15	10	12	9	8	9	13	20
5. Authorisation by minister	2	1	0	0	0	0	0	0	0	0	0	0
6. Prejudicial consulting body	0	0	0	0	0	0	0	0	0	0	0	1
TOTAL	23	18	27	23	16	11	16	11	9	14	13	23

14

In 2024, the number of referrals increased significantly compared to previous years. The vast majority of referrals were the result of suspension by the SIM Commission. This accounts for 1.5% of all SIM cases. Of these 20 cases, two were from GISS and 18 from State Security. The Committee also received two complaints, which had not occurred since 2016.

Once seized, the Committee can take various decisions. For all referrals that followed a suspension ordered by the SIM Commission, it was ordered that the method be (partially) terminated and the illegally collected data destroyed. For referrals in response to lodged complaints, the Committee, after a thorough analysis of all SIMs relating to each of the complainants, ruled that the complaints were admissible but unfounded. The rulings were issued in January 2025.

In September 2024, the Committee was referred to for the first time in its history in its capacity as a prejudicial consulting body. In a judgment dated 24 September 2024, the Brussels Court of Appeal's Chamber for Indictments asked the Committee to rule on the legality of specific and exceptional methods carried out by the civilian intelligence service, the results of which were contained in two unclassified official reports in a court file. In January 2025, the Committee issued an opinion in which the legality of the above-mentioned specific and exceptional methods of data collection was endorsed.⁷

⁷ The extent of the case and the amount of documents and information that needed to be analysed and processed required significant capacity in 2024, for an extended period of time.

Foreign interceptions, 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 computer systems (art. 44/1 ISA) and the capture of static or moving images in foreign countries (art. 44/2 ISA) are also among the possibilities open to the military intelligence service. The Standing Committee I monitors these methods prior to, during and after their implementation.

In January 2024, the Committee received the plans for interceptions, intrusions and image recordings for that year. These plans met all legal requirements. The Standing Committee I visited the installations where the interceptions were made. Visits abroad were also conducted in 2024. However, the Committee is unable to share any further information on this 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 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 in the context of 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 based on 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 2024, the Committee was asked for its opinion 12 times: four times at the request of the Minister of Justice (in one case the request for its opinion did not come directly from the minister but through the Data Protection Authority (DPA)) four times at the request of the Minister of Home Affairs (twice via the DPA), twice at the request of the Minister of Defence and once, again via the DPA, at the request of the Minister for Economic Affairs. It was not only the executive branch that requested advice from the Committee; the Commission for Home Affairs, Security, Migration and Administrative Matters of the Chamber of Representatives also requested an opinion from the Committee on a draft law.

These were mostly requests for advice on draft royal decrees, three cases involved preliminary drafts of laws and one involved a draft law. The topics ranged from security verifications and advice to the resilience of critical entities and access to the register of the Common Guarantee Fund. The average lead time for issuing an opinion is two months. The Committee is of the opinion that this average processing time is short, taking into account the quantity of opinions submitted and the size of some of the annexes. All opinions are available in full on the website of the Standing Committee I (www.comiteri.be).

The college for security opinions within GISS

The draft submitted to the Committee for its advice sought to implement a provision inserted in 2023 in the Act of 11 December 1998, on classification and security clearances, certificates and advice (Classification and Security Clearances Act) establishing the College for Security Opinions within GISS (Art. 22sexies/2, para. 4), which is responsible for evaluating the information available when it is not possible to issue an unequivocal positive or negative opinion regarding a (future) member of the Defence staff.

In its opinion, the Committee made important comments on the delegation authority of the Director of Security of GISS and on the powers, functioning and composition of the College. There were also numerous comments on the criteria for assessing the data collected to determine the nature of the security advice; the Committee reiterated the need to comply with the legal framework.

Security verifications and the abolition of security certificates

The Committee was asked to issue an opinion on a draft bill to amend the Classification and Security Clearances Act, primarily with regard to security verifications prior to security advice and certificates. The purpose of the draft law was to harmonise the various existing procedures for security verifications, in particular by abolishing the system of security certificates and replacing it with a general system of security advice.

The Committee made numerous content-related and technical comments, and issued a negative opinion on the draft law. It had serious reservations about the choice to abolish security certificates and replace them with security advice, as this means that the ultimate responsibility for the security of the State's fundamental interests is entrusted to private or public entities that do not necessarily have the required expertise in the field. Moreover, the Committee felt that the draft law's goal of harmonising several existing screening procedures was not realised. A more comprehensive reform is called for, given the proliferation of new legal provisions on security verifications that have recently been introduced or were pending at the time the preliminary draft was examined.

Security verifications for prison staff

In its capacity as the Competent Supervisory Authority, the Committee was asked to issue opinion on the preliminary draft law seeking to amend several laws related to the Judiciary, including the Act of 23 March 2019 on the organisation of correctional services and the status of correctional staff. The amendments proposed in this law were intended to introduce a security verification for prison staff, which, while containing provisions that were inspired by the rules applicable to security advice in the Classification and Security Clearances Act, differed from them in several respects. This security verification scheme was supposed to replace the morality examination which, although introduced by the above-mentioned law, had not yet entered into force because the King had not set a date for it.

In its opinion, the Committee stated that it understood the Government's desire to deal with the issue of screenings, security verifications and other morality examinations in a differentiated way, depending on the professions and functions performed, while maintaining a coherent approach across sectors. In this regard, the replacement of the morality examination, based on similar data as a security verification but following other criteria, was welcomed. Nevertheless, the Committee called for a more comprehensive and coherent reform of the security verification system, fearing that the introduction of this new type of security verification would lead to a proliferation of different legal systems that would be similar but not identical. This would make it difficult for the public and for the institutions that apply or monitor the rules to understand them.

Access to the register of the Common Guarantee Fund

The Act of 21 November 1983 on compulsory motor vehicle liability insurance established a fund to keep a register of information and personal data on vehicles and their insurance. While the current legal framework provided for limited access to this information for the two intelligence services, the preliminary draft royal decree submitted to the Committee for advice aimed to introduce the possibility for these services to consult the register in real time, with the aim of simplifying administration and encouraging digitisation.

In its opinion, the Committee questioned whether such direct access was appropriate. Simple access via the obligation of the fund to provide the requested information as soon as possible seemed sufficient given the nature of the data in the reg-

ister. The Committee also recommended that the preliminary draft be clarified on a number of points (including the definition of relevant data that can be accessed).

CUTA and the recognition of local communities of recognised worship

The recognition of worship as well as the recognition of local communities of recognised worship is governed by the cooperation agreement of 2 July 2008 between the federal State and federated entities. It designates the federal government as responsible for issuing a security advice in the context of procedures for recognising local communities of recognised worship services; advice that may be negative if based on elements related to State security or public order.

The preliminary draft royal decree submitted for consultation aimed to expand the evaluation entrusted to the Coordination Unit for Threat Analysis (CUTA) in the context of applications from local communities for recognition. The intention was to meet the need to assess the impact of this recognition on national security and public order, that sometimes transcend the context of terrorist and extremist phenomena.

In its opinion, the Committee considered that the preliminary draft Royal Decree went beyond the powers granted to the King by the legislator in several respects by Article 3 of the Act of 10 July 2006 on threat analysis (CUTA Act). First, the draft not only broadened the scope of the threats to be monitored (which is allowed), but also gave CUTA a new, different kind of mission, namely, to provide advice on a systematic basis to prepare or support a highly specific administrative legal act (namely, recognising local religious communities). The Committee felt that only the legislator, and not the King, could entrust this new task to CUTA. Second, the preliminary draft expanded the interests to be protected by stipulating that, in addition to national security, CUTA also had to assess threats to public order. Again, this responsibility is the sole competence of the legislator. Phenomena or events affecting public order do not fall under the competence of CUTA.

Voluntary service of collective benefit

The Committee was asked for its opinion on a preliminary draft royal decree implementing the Act of 11 April 2003 establishing a voluntary service of collective benefit, as amended by the Act of 21 November 2023. The latter provides that anyone wishing to be admitted to a voluntary service of collective ben-

efit must have a positive security advice issued by the competent security authority following a security verification in accordance with the Classification and Security Clearances Act.

In its opinion as the Competent Supervisory Authority, the Committee noted a number of points where the draft needed clarifying and amending (in particular with respect to the security authority responsible for implementing security verification).

Access to the national register of natural persons and to the population registers

The Act of 8 August 1989 regulating a National Register of natural persons and the Act of 19 July 1991 on the population registers, identity cards, foreign national cards and residence documents, stipulate the requirements to be met to access the registers they manage. However, certain authorities, in particular the police, are exempt from authorisation, which means they can access data from the registers without the need for additional authorisation.

The Home Affairs Committee of the Chamber of Representatives requested the Committee's opinion on a draft law to amend the two laws mentioned above to include the two intelligence services as well as the Committee among the authorities that are exempt from authorisation, which would allow them direct access to these registers without additional authorisation.

The Committee made a number of comments on the access for the intelligence services, recalling that any processing of personal data constitutes an interference with the right to privacy and the right to protection of personal data, which is permissible only if it is necessary and proportionate to the legitimate purpose pursued. As regards its own access, the Committee pointed out that it is not the most appropriate body to comment on its own processing of personal data.

Implementation of the amendments to the Classification and Security Clearances Act by the Act of 7 April 2023

The Committee was again asked to give its opinion on the changes related to security verifications, and more specifically on a preliminary draft royal decree amending the royal decree implementing the Classification and Security Clearances Act and implementing the Act of 7 April 2023.

In its opinion, the Committee highlighted various problems that required changes or at least clarifications in the text (in particular, the lack of a legal basis for the delegation given to replace the 'lead official' and the introduced 'contact person for security').

The public regulated service Galileo

The Galileo system is part of the European Union (EU) space programme and aims to provide accurate and reliable timing and positioning information around the world. It consists of several components, including a public regulated service (PRS). This is a secure navigation service intended for users authorised by the government (such as the emergency services, fire departments and the police), which provides an additional level of protection to enhance the level of confidentiality, integrity and availability in the event of national emergencies or crisis situations (such as a terrorist attack).

In its response to the request for advice on a draft royal decree on the public regulated service, the Committee identified a number of points that needed clarification. It also highlighted the fact that by incorporating the National Security Authority (NSA) into the fold of State Security, the legislator broadened the Committee's monitoring remit, in the sense that the NSA in its entirety and for all of its activities comes under the supervision of the Committee. When the NSA acts as the Belgian responsible authority for the public regulated service, it is therefore supervised by the Committee. The Committee called for robust monitoring of the work of the NSA in implementing and managing this project, which requires an increase in the material, financial and human resources of both the NSA/ State Security and the Committee, bearing in mind the major importance of the EU space programme and the public regulated service within the Galileo programme within it.

Implementation of the amendments made to the Classification and Security Clearances Act and to the Personal Data Protection Act by the Act of 2 June 2024

The Committee was asked to provide opinion on four draft royal decrees on security verifications and security advice that implement the amendments made to the Classification and Security Clearances Act by the Act of 2 June 2024 and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (DP Act).

The draft Royal Decree implementing Chapter IV 'Security Advice' of the Classification and Security Clearances Act was given specific attention by the Committee. The Committee issued a negative opinion on the draft decree, pointing out that it unlawfully implemented the Act of 2 June 2024 by granting extensive powers to the competent administrative authority, although these powers were not defined anywhere in the Act. The Committee also pointed out that the draft decree violated the letter

and spirit of the law by providing an exemption for the Federal Agency for Nuclear Control (FANC) despite the lack of a legal basis authorising this.

The consent of private investigators

The Committee was asked to give its opinion on a draft royal decree implementing the new Act regulating private investigations approved by the Chamber of Representatives on 8 May 2024. The draft was intended to implement a provision of the Act regarding consent for an investigation of security conditions for private investigators.

In its opinion, the Committee highlighted the fact that the law provides that the investigation of security conditions can either be conducted by an official from Home Affairs or by State Security or GISS. If the investigation is entrusted to one of the two intelligence services, it is conducted in accordance with the Classification and Security Clearances Act and is therefore similar to a security investigation, which implies that more intrusive methods are used than those available to officials from Home Affairs (such as field an investigation or the consultation of databases). The Committee pointed out that the choice of having the investigation conducted by an official from the FPS Home Affairs or by State Security or GISS is therefore not without importance for the person in question, who may be expected to be able to give informed consent. The Committee therefore highlighted the need to specify in which cases the investigation would be entrusted to State Security or GISS.

Resilience of critical entities

The Committee was asked for its opinion on a draft law transposing the European Critical Entities Resilience Directive into Belgian law. This directive establishes a harmonised general framework to make critical entities more resilient to a variety of risks, ranging from natural disasters to those caused intentionally or unintentionally by humans. The transposition of this directive was intended to replace the Act of 1 July 2011 on the protection and security of critical infrastructures.

The main comments of the Committee related to the requirement for CUTA to conduct a threat assessment for the sectors and subsectors covered by the preliminary draft. The Committee noted that under the Act of 1 July 2011, CUTA was already responsible for conducting strategic threat assessments relating to critical infrastructures, which cover all types of threats that fall under the competence of the support services, and therefore are not limited to threats of terrorism and extremism. The claim

in the explanatory memorandum that the draft law expanded these threat assessments as regards the subject of the analysis was therefore incorrect.

In addition, the text proposed expanding the reporting requirement of the support services. The support services were hitherto only required to provide CUTA with relevant and available information on threats of terrorism and extremism. The draft law would oblige the support services to provide CUTA with information on any threat within their competence going forward. The Committee welcomed the planned extension and pointed out that the limited reporting requirement is problematic given that the legislator - through the Act of 1 July 2011 - entrusted CUTA with the task of preparing common strategic threat assessments covering a multitude of threats, without providing the service with dedicated legal instruments.

New laws and regulations

Various laws and regulations were amended in 2024 regarding the operations, competences and control of the intelligence and security services and intelligence work.

First, following the amendment of the Policing Act in 2019, whereby the intelligence services could now access the General National Database (GND), on 6 January 2024, the *Royal Decree of 23 November 2023 on the direct access of the intelligence and security services to the personal data and information of the General National Database referred to in Article 44/7 of the Policing Act* (BOJ 27 December 2023) entered into force. This lays down the procedures for the actions of the intelligence services and defines the categories of personal data they can access within the GND.

Subsequently, following the restructuring of the tasks of the National Security Authority (NSA) and its integration into State Security on 1 January 2024, the *Decree of the Administrator General of State Security delegating decision making authority regarding the powers stipulated in Article 1quater of the Act of 11 December 1998 on classification, security clearances, security certificates, security advice and the public regulated service* (BOJ 5 February 2024) was enacted. This clearly delegates the powers of the Administrator General to the person in charge of the NSA, so that the latter can make decisions and advice on behalf of the NSA, as well as represent it.

Although the Act of 11 December 1998 on Classification and Security Clearances had already undergone significant changes in 2023, it was the subject of even more significant changes (including its name) in 2024.⁸ First, in the nuclear and radiological sectors, a number of changes were made to reliability checks on individuals. The control system in place until then was revised by the *Act of 7 February 2024, amending the Act of 15 April 1994 on the protection of the population and the environment against dangers arising from ionizing radiation and on the Federal Agency for Nuclear Control and the Act of 11 December 1998 on classification, security clearances, security certificates, security advice and the public regulated service, concerning various aspects of the reliability check on individuals and the protection of information* (BOJ 28 February 2024), which came into force the day after its publication. The aim of the legislator was to make the system for checking the reliability of individuals 'more flexible' and 'more effective'. The royal decree implementing the new powers granted to the King by this law was approved on 14 April 2024.⁹ It should be noted that during the year other new developments in checking the reliability of individuals in the nuclear and radiological sector were introduced by royal decree.¹⁰

8 Now entitled "Act of 11 December 1998 on classification, security clearances, security advice and the public regulated service" (see below).

9 Royal Decree amending the Royal Decree of 17 October 2011 on security certificates for the nuclear sector and regulating access to security zones, nuclear material or nuclear documents in certain special circumstances and supplementing Article 30bis of the Royal Decree of 24 March 2000 implementing the Act of 11 December 1998 on classification and security clearances, security certificates and security advice, with a view to inserting an annex containing the request form for a security certificate in the nuclear and radiological sectors (BOJ 14 May 2024).

10 Royal Decree of 17 March 2024 on the security of facilities for above-ground disposal of radioactive waste (BOJ 28 March 2024); Royal Decree of 17 March 2024 on the security of radioactive substances and certain nuclear materials (BOJ 28 March 2024).

Subsequently, the Classification and Security Clearances Act was comprehensively revised with regard to security verification by the Act of 2 June 2024 amending the Act of 11 December 1998 on classification, security clearances, security certificates, security advice and the public regulated service and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (BOJ 8 July 2024). The legislator's aim was to simplify the issue of security verifications, responsibility for which was entrusted to the Federal Police by the National Security Council in its decision of 23 February 2022 ratifying the reform of the NSA. The system of security verifications was comprehensively amended by this Act, which came into force on 1 February 2025, along with several royal decrees implementing the Act that lay down a number of practical procedures.¹¹ This Act abolishes security certificates and replaces them with security advice. A new function has also been created within companies that do not have a security officer, the 'security advice administrator'. The name of the Classification Act was also changed to 'Act on classification, security clearances, security certificates, security advice and public regulated service'.

The changes to the system of security verifications and the abolition of security certificates required changes in the Appeal Body Act. These were introduced by the Act of 16 June 2024, amending the Act of 11 December 1998 establishing an appeal body on security clearances, security certificates and security advice (BOJ 16 July 2024), which also came into force on 1 February 2025. The title of the Appeal Body Act was changed to 'Act establishing an appeal body on security clearances and security advice'.

The year 2024 was also marked by an extension of security screenings of employees in Belgium, with security verifications imposed within the meaning of the Classification and Security Clearances Act for new sectors of activity such as the prison system¹², the maritime sector¹³ and the Flemish administration in charge of electronic surveillance.¹⁴

The legal framework regarding the creation of the Common Database on Terrorism and Extremism (CDB T.E.R.) was also revised in 2024. This database, set up following the attacks of 22 March 2016, collects information on individuals considered as extremists and terrorists who are monitored in Belgium in the context of the T.E.R. strategy, and allows intelligence and security agencies to share information and determine which agency is best positioned to take action. The original CDB T.E.R. was based on the Policing Act and consisted of two separate databases, Terrorist Fighters and Hate Propagandists. With the approval of the Act of 29 March 2024 establishing the common database on 'Terrorism, Extremism, Radicalisation Process' 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 (published on 16 April 2024 and entered into force on 1 January 2025), the legislator has given the database an autonomous legal framework. The functioning of the CDB was also updated, with partners expanded to include French- and German-speaking youth assistance services. The royal decree implementing the law was published on 19 July 2024.¹⁵

11 Royal Decree of 20 December 2024 implementing the Act of 11 December 1998 on classification, security clearances, security advice and the public regulated service (BOJ 22 January 2025); Royal Decree of 20 December 2024 amending the Royal Decree of 8 May 2018 laying down the list of data and information that can be consulted in the context of carrying out a security verification (BOJ 22 January 2025); Royal Decree of 20 December 2024 amending the Royal Decree of 4 February 2024 determining the amount of fees due in implementation of Article 22septies of the Act of 11 December 1998 on classification, security clearances, security certificates, security advice and the public regulated service as well as the distribution keys (BOJ 22 January 2025); Royal Decree of 20 December 2024 amending the Royal Decree of 8 May 2018 determining the sectors of activity and the competent administrative authorities referred to in Article 22quinquies, § 7, of the Act of 11 December 1998 on classification and security clearances, security certificates and security advice (BOJ 22 January 2025); Royal Decree of 20 December 2024 establishing the entry into force of the Act of 2 June 2024 amending the Act of 11 December 1998 on classification, security clearances, security certificates, security advice and the public regulated service and the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data, implementing certain provisions of the Act of 11 December 1998 on classification, security clearances, security advice and the public regulated service and repealing Chapter IIIbis of the Royal Decree of 24 March 2000 implementing the Act of 11 December 1998 on classification and security clearances, security certificates and security advice (BOJ 22 January 2025).

12 Act of 15 May 2024 containing provisions on the digitisation of the judiciary and various provisions II (BOJ 28 May 2024).

13 Act of 16 May 2024 amending the Belgian Shipping Code and various laws on shipping regulations (BOJ 4 July 2024).

14 Government of Flanders Order of 29 March 2024 amending the Flemish personnel status of 13 January 2006, regarding the modernisation of the HR policy, authority functions, top and middle management and career policy, of the Government of Flanders Order of 27 March 2020 establishing the rules for the general personnel policy in the services of the Flemish government, the Flemish public institutions and the Strategic Advisory Council SERV, and for the specific personnel policy in the services of the Flemish Government, and of the Government of Flanders Decree of 30 October 2015 regulating the delegation of decision-making powers to the heads of departments and of internally autonomous agencies, and repealing the Ministerial Decree of 14 May 2008 laying down the additional or specific assignments in the services of the Flemish Government (BOJ 7 June 2024).

15 Royal Decree of 14 July 2024 on the common database on "Terrorism, Extremism, Radicalisation Process" ("T.E.R.") (BOJ 19 August 2024).

On the same date as the CDB T.E.R. Act, the *Act of 29 March 2024 on the establishment and organisation of the tasks of the National ETIAS Unit* (BOJ 29 April 2024) was enacted. This new unit is responsible for implementing the ETIAS regulation adopted by the European Union in 2018, which organises the European System for Travel Information and Authorisation and introduces the obligation for citizens of several third countries exempted from visa requirement to request prior authorisation before travelling within the Schengen area. The objectives are to strengthen internal security, prevent illegal immigration and protect public health by identifying people who may pose a risk even before they leave for the EU. The ETIAS system will start in 2025, on a date specified by the European Commission. The Act also stipulates that seconded personnel from State Security and GISS will be part of the National Crisis Centre's department authorised (freely translated) "to process hits related to security risks and high epidemiological risks". The Act also amends the Organic Law on the Intelligence and Security Services of 30 November 1998, in that it provides for a new ordinary method of data collection. State Security and GISS, in the interest of carrying out their missions, may decide to access data stored in the central ETIAS system, as long as there is sufficient justification. This method will be used under the supervision of the SIM Commission and the Committee.

On 12 October 2023, the Constitutional Court issued a ruling annulling several provisions of the Passenger Name Record (PNR) law and imposing the interpretation of the Court of Justice of the EU. In response to this ruling, the *Act of 16 May 2024 amending the Act of 25 December 2016 on the processing of passenger data* (BOJ 5 July 2024) was enacted. This Act "restores" certain annulled provisions, in particular provisions relating to the possibility for the intelligence services to access information held by the Belgian Passenger Information Unit through targeted searches (art. 16/3 ISA). This ordinary method of collecting information is subject to the supervision of the Committee.

Finally, a new legal framework for private investigations was adopted with the approval of the *Act of 18 May 2024 regulating private investigations* (BOJ 6 December 2024). This Act, which came into force on 16 December 2024, replaced the Act of 19 July 1991 organising the profession of private detective, which had become obsolete. To perform the tasks of a private investigator, the law requires authorisation from the Minister of the Interior. In certain cases provided for by law, the Minister may request the relevant information that State Security or GISS has on the applicant in order to make a decision on their licence's request.

6. APPEAL BODY

APPEAL BODY

The Committee chairs and acts as registrar for the Appeal Body on security clearances and advice.¹⁶

This is an administrative jurisdictional body with jurisdiction over disputes relating to administrative decisions concerning security clearances, (certificates) and advice. It is composed of three judges, with the Chairwoman or her deputy - a council member of the Committee - presiding.

As registrar for the Appeal Body, the Committee also provides staff and resources necessary to organise the administration, correspondence and conduct of hearings.

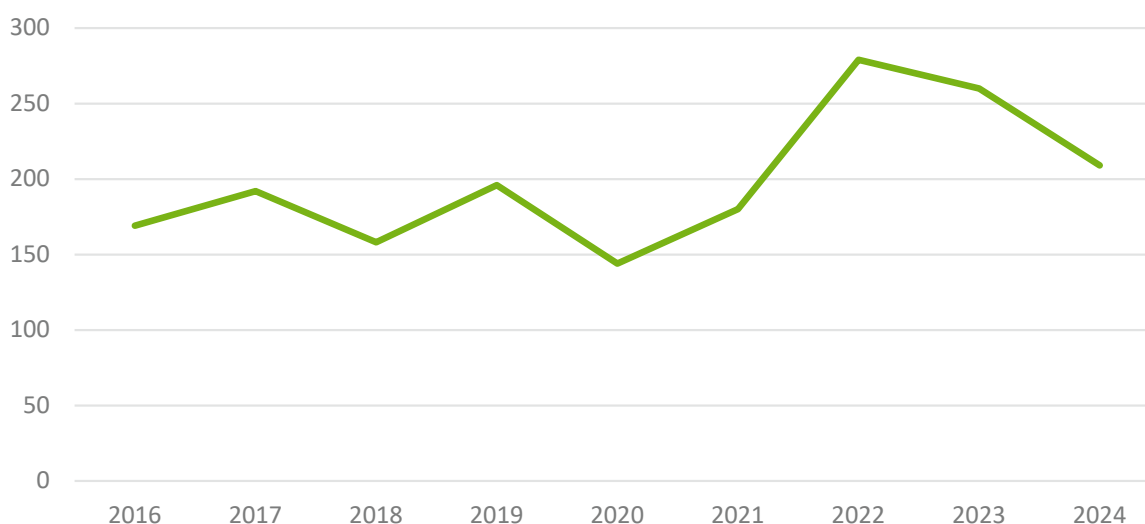
The present chapter presents and discusses some figures to illustrate the trends observed regarding appeals and the workload of the Appeal Body. For a complete overview of the figures, please see the activity report of this jurisdictional body (www.beroepsorgaan.be).

Number and nature of appeals lodged

In 2024, **209 appeals** were lodged, a lower figure compared to 2023 (260 appeals lodged) and 2022 (279 appeals lodged). Nevertheless, the figure is significantly higher compared to the number of appeals lodged in 2021 (180 appeals lodged) and 2020 (144 appeals lodged).

As regards the nature of contested decisions in 2024, the number of appeals lodged regarding security clearance decisions remained stable (i.e., 102 in 2024 compared to 105 in 2023). A similar observation can be made regarding the number of decisions relating to security certificates (22 in 2024 versus 21 in 2023). However, a sharp decrease can be observed in the number of appeals lodged regarding decisions on security advice (85 appeals lodged in 2024 compared to 134 appeals lodged in 2023).

Number of appeals lodged (2016-2024)



¹⁶ Pursuant to the Act of 16 June 2024 amending the Act of 11 December 1998 establishing an appeal body for security clearances, security certificates and security advice (BOG of 16 July 2024), the title of the appeal body was changed to “appeal body for security clearances and security advice”.

Nature of contested decisions									
	2016	2017	2018	2019	2020	2021	2022	2023	2024
Security clearances (art. 12 et seq. Classification and Security Clearances Act)	50	40	36	51	32	60	83	105	102
Security certificates (art. 22bis, para. 1, art. 22bis, para. 2 art. 8bis Classification and Security Clearances Act)	18	30	30	30	13	12	39	21	22
Security advice (art. 22quinquies Classification and Security Clearances Act)	101	122	92	115	99	108	157	134	85
TOTAL	169	192	158	196	144	180	279	260	209

Compared to 2023, a significant variation was also observed in the security and verification authorities involved in the decisions contested before the Appeal Body, and more specifically regarding security advice. In 2023, only four decisions of the Federal Police (all concerning a refusal to issue a security certificate) were contested. In 2024, there were 56 (including 50 relating to a negative security advice and six refusals to issue a security certificate).

This marked increase can be explained by the significant change in the handling of security advice: since 31 December 2023, the Federal Police has been responsible for security verifications previously carried out by the National Security Authority (NSAth). For the same reason, the number of decisions appealed in 2024 decreased significantly: in 2023, 188 NSAth decisions were contested before the Appeal Body (100 of which involved a negative security advice and 88 of which involved refused security clearances). In 2024, the number was only 77, all of which involved a refusal of security clearance.

Security and verification authorities involved ¹⁷ (2023-2024)								
	2023	2023	2023	2023	2024	2024	2024	2024
	<i>Clea- rances</i>	<i>Certifi- cates</i>	<i>Advice</i>	TOTAAL	<i>Clea- rances</i>	<i>Certifi- cates</i>	<i>Advice</i>	TOTAAL
NSAth	88	0	100	188	77	0	0	77
State Security	0	0	0	0	1	0	0	1
GISS	17	5	34	56	24	6	35	65
FANC	0	11	0	11	0	10	0	10
Federal Police	0	4	0	4	0	6	50	56
Local Police	0	1	0	1	0	0	0	0
TOTAL	105	21	134	260	102	22	85	209

Moreover, the number of French-language appeals lodged (calculated on the basis of the applicant's language) still by far exceeded the number of Dutch-language appeals. In 2024, there were 133 French-speaking appeals (159 in 2023) compared to 76 Dutch-speaking appeals (101 in 2023).

¹⁷ 'Verification authorities' are authorities authorised to issue security certificates and advice, such as, for example, the Federal Police and the Federal Agency for Nuclear Control.

Language of the petitioner									
	2016	2017	2018	2019	2020	2021	2022	2023	2024
French	99	115	83	101	83	86	201	159	133
Dutch	70	77	75	95	61	94	123	101	76
German	0	0	0	0	0	0	0	0	0

Decisions of the Appeal Body and acts of the Registry

For the 209 appeals received in 2024, the Registry had to send 56 reminders to the security and verification authorities to receive the file of the petitioner (compared to 37 reminders for the 260 appeals lodged in 2023). These numerous communication delays, beyond the control of the Appeal Body and its Registry, slowed down the processing of cases.

During the year, the Appeal Body held 29 sessions, including 18 in French and 11 in Dutch.

The Appeal Body made 259 decisions in 2024, the same number of decisions made in 2023. There were 130 decisions on cases submitted in 2024 (including 78 clearances, 13 certificates and 39 cases of advice); 115 decisions on cases submitted in 2023 (including 53 clearances, 10 certificates and 50 cases of advice) and finally 14 decisions on cases from 2022 (including 10 clearances, 3 certificates and one advice).



7.

INTERNAL FUNCTIONING

INTERNAL FUNCTIONING

Composition

The composition of the Committee changed significantly in 2024: Vanessa Samain, Deputy Public Prosecutor of Mons, took the oath of office on 25 September 2024, as the new chairwoman of the Standing Committee I. Linda Schweiger, Advisor General at the Ministry of Defence, continued her assignment as a councilwoman. On 31 January 2024, Séverine Merckx took the oath of office as a new councilwoman. She served as advisor to the Cabinet of Deputy Prime Minister and Minister of Economy and Labor in charge of justice, home affairs, security and privacy. Frederic Verspeelt was appointed as Director of the Investigation Service I in August 2024, which is composed of seven commissioner auditors. The administration, headed by Registrar Frédéric Givron, had 18 employees.

Parliamentary Monitoring Committee

The composition of the Special Committee entrusted with the parliamentary monitoring of the Standing Police Monitoring Committee and the Standing Intelligence Agencies Review Committee (the Monitoring Committee) underwent comprehensive changes in 2024. The following served on the committee as voting members: Peter Buysrogge (N-VA), Christoph D'Haese (N-VA), Maaïke De Vreese (N-VA), Stefaan Van Hecke (Ecolo-Groen), Khalil Aouasti (PS), Eric Thiébaud (PS), Francesca Van Belleghem (VB), Marijke Dillen (VB), Denis Ducarme (MR), Benoît Piedboeuf (MR), Sammy Medhi (cd&v), Nabil Boukili (PVDA-PTB), Paul Van Tichgelt (Open Vld), Brent Meuleman (Vooruit) and Benoît Lutgen (Les Engagés). President of the Chamber Peter De Roover (N-VA) chairs the committee.

Four meetings took place during 2024 during which various review investigations concluded by the Standing Committee I and the internal functioning of the Committee were discussed. In early December 2024, the Monitoring Committee made a working visit to the offices of the Committee.

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 Standing Police Monitoring Committee at least twice a year. During 2024, several meetings and events took place in connection with joint review investigations and complaints jointly handled by both Committees.

New data protection officer

Since 1 May 2024, Frédéric Amez acts as Data Protection Officer (DPO) for the Chamber and Senate, as well as for a number of institutions of the Chamber, including the Standing Committee I. As Data Protection Officer, he is responsible for assisting the Committee in all aspects of its functioning regarding the application of the General Data Protection Regulation (GDPR).

Integrity Unit

To deal with integrity violations committed within the General Intelligence and Security Service or State Security, the external reporting channel was set up within the Committee in accordance with the Act of 8 December 2022. To perform this new role, an Integrity Unit was created. The members of this unit completed advanced training in 2024.

Budget

The total budget approved by the Chamber of Representatives for 2024 was €6,295,750, and was made up of €4,764,000 allocated funds and €1,531,750 bonuses from 2023. Of these, personnel costs account for the lion's share of the budget (> 80%).

Digitisation

The Standing Committee I was granted a specific budget by the Chamber of Representatives with a view to realising a large-scale digitisation project, to modernise its functioning. This is a crucial step in streamlining administrative tasks. In the context of the digitisation of its key processes, the operation of the Appeal Body is one of the priorities. In a context where new sectors (e.g., HR Rail and port facilities) are being added to the existing security verification regimes, these IT developments are crucial for the Standing Committee I to maintain a balanced allocation of resources with regard to all of its missions. During 2024, investment priorities (hardware and software) were agreed on and several suppliers were identified. In particular, the Committee's internet network, as well as its operating system, were comprehensively overhauled to improve efficiency and security. Various projects were also initiated to modernise the Committee's classified network. To this end, contacts were made with the homologation authority. Finally, a Chief Information Security Officer (CISO) was also appointed.

Synergies

The Standing Committee I remains fully committed to 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 Accounting 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, car sharing, ICT, and government contracts). Their work continued throughout 2024. As regards harmonised statuses, the Committee is awaiting the position of the Commission on Accounting that is studying the budgetary impact with respect to the audit conducted by the Court of Audit.



8.

**INTERNATIONAL
COOPERATION**

INTERNATIONAL COOPERATION

- In late March 2024, the Committee participated in the panel 'Maintaining trust through independent oversight bodies' at the 7th U.S. Intelligence Community Civil Liberties, Privacy and Transparency Summit, hosted in Washington by the Office of the Director of National Intelligence (ODNI). The U.S. Privacy and Civil Liberties Oversight Board (PCLOB) and the French *Commission Nationale de Contrôle des Techniques de Renseignement* (CNCTR) were also represented. The Committee had the opportunity to meet with members of the Intelligence Oversight Board and the Department of Justice. More generally, the mission was an opportunity to clarify the various complex forms of oversight of the intelligence services in the United States.
- From 10 to 12 April 2024, participants from both the Technical and Staff Meetings of the International Oversight Working Group (IOWG) gathered in Brussels. The Technical Meeting discussed various aspects of artificial intelligence (AI), its potential use by the intelligence services as well as the challenges faced by oversight bodies. The participants exchanged views on possible solutions for a systematic approach to monitoring the use of AI in the intelligence community.

At the Staff Meeting, the Standing Committee I explained the results of one of its recent reviews on intelligence investigations into politicians and elected officials. The subsequent discussion confirmed the political focus on this issue and more generally on the threat of interference or spying targeting elected officials. This highly sensitive issue once again highlighted the different legal frameworks between IOWG members. The National Security and Intelligence Review Agency (NSIRA) then presented the matrix they had developed to set investigation priorities. The Canadian delegation presented their Forward Looking Plan and the processes intended to lead to the approval of new investigations. Finally, Convention 108+ was an important topic at the meeting. Although Switzerland has already ratified Convention 108+, ratification does not seem to be a priority for the other IOWG countries. The discussions confirmed how difficult it is to organise cooperation at the operational level. However, other paths of potential cooperation were identified, such as overseeing protocol agreements between intelligence services.

- In early June 2024, a representative of the Canadian National Security and Intelligence Review Agency (NSIRA) was invited to visit Brussels to present the institution, its organisation and missions to the Committee. Among other things, the discussions focused on how the NSIRA selects, processes and organises its investigation topics according to a yearly planning.
- The '7th Pan-European Conference on International Relations, European International Studies Association' was held in Lille in August 2024. Representatives of the Committee, among others, presented a paper on 'Intelligence Agencies as Suppliers, Producers and Clients of Security Screenings'.
- In mid-October 2024, a representative of the Committee attended the congress '*Les enjeux du contrôle du renseignement: un dialogue des contrôleurs*', organised by the *Commission nationale de contrôle des techniques de renseignement* (CNCTR) and *Les Etudes françaises de Renseignement et de Cyber* (EFRC) held in Paris.
- On 23-24 October 2024, the International Oversight Working Group (IOWG) met for a Technical Meeting in Sweden. Various topics were on the agenda: the framework for monitoring intelligence and security services in Sweden, monitoring the collection and processing of Big Data, and current practices and trends in this area. Participants also exchanged in-depth views on legislative developments and current issues in each of the countries represented.

APPENDICES

Abbreviations

GISS	General Intelligence and Security Service
GND	General National Database
GDPR	General Data Protection Regulation
Monitoring Committee	Special Committee entrusted with the parliamentary oversight of the Standing Police Monitoring Committee and the Standing intelligence agencies Review Committee
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
BOJ	Belgian Official Journal
CISO	Chief Information Security Officer
Convention 108	Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
DPO	Data protection officer
EU	European Union
FANC	Federal Agency for Nuclear Control
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 (Data Protection Act)
CDB	Common Database
IOWG	Intelligence Oversight Working Group
NSAth	National Security Authority
CUTA	Coordination Unit for Threat Analysis
PRS	Public regulated service
TER Strategy	Extremism and Terrorism Strategy
Standing Committee I	Standing Intelligence Agencies Review Committee
Standing Committee P	Standing Police Monitoring Committee
VSSE	State Security
Appeal Body Act	Act of 11 December 1998 establishing an appeal body on security clearances and security advice
Classification and Security Clearances Act	Act of 11 December 1998 on classification, security clearances, security certificates, security advice
ISA	Act of 30 November 1998 governing the intelligence and security services
CUTA Act	Act of 10 July 2006 on threat analysis
Policing Act	Act of 5 August 1992 on the police services
Review Act	Act of 18 July 1991 governing the review of the police and intelligence services and the Coordination Unit for Threat Analysis