Comité R | I
Intelligence services oversight

ACTIVITY REPORT
2025

ACTIVITY REPORT

2025

Contents

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, the Committee R/I reports on its activities in this 2025 annual report.

In this report, the Committee outlines the most important activities carried out in 2025, whether they involve review investigations, opinions issued, or the work performed by the members and the registry of the Appeal Body. Special attention is also given to the specific and exceptional intelligence collection methods used by the intelligence services in 2025, as well as to how these methods are reviewed.

Brussels, 7 April 2026

Frédéric Givron
Registrar

Vanessa Samain
Chairwoman

Séverine Merckx
French-speaking member

Filip Vanneste
Dutch-speaking member

PREFACE

Consensus is often rare, but there is one thing everyone seems to agree on: the past year was marked by profound upheavals on both the geopolitical and social fronts. Our society has rarely witnessed such a combination of tensions since the Second World War: armed conflicts, disinformation, democratic backsliding, etc. All of these factors clearly pose a challenge to our security, but the problem goes further than that; they undermine our institutions, our social cohesion, and citizens' trust in the work of government.

The example of other European countries shows how difficult it is to restore institutional independence once this has been compromised over a long period. Although the situation has not reached that point yet in Belgium, our country is unfortunately not immune to this trend of the rule of law backsliding. According to a report[1] by the Civil Liberties Union for Europe, Belgium—along with six other countries—has been given the unenviable status of being a "*slider*" ...

In these turbulent times, the democratic credibility of the work carried out by the intelligence and security services stands or falls on the existence of a strong review body that is able to fulfil its role as an independent watchdog. We are all the more determined to fulfil this remit, since trust in democracy cannot simply be claimed. It must be earned step by step, patiently and with dedication, by working rigorously, diligently, and consistently.

There was clearly no shortage of projects in 2025. Not only did the Committee R/I conclude several review investigations, but it also launched three new investigations on its own initiative, thereby demonstrating its firm commitment to making progress under all circumstances.

An analysis of the figures related to reviews of special intelligence methods (SIM) shows that the trend of recent years is continuing: the number of methods used by State Security (VSSE) and the General Intelligence and Security Service (GISS) continues to rise. The three exceptional methods most frequently used by GISS are the same as in previous years: the military intelligence service primarily relies on wiretapping, hacking into IT systems, and conducting surveillance in locations not accessible to the public. For State Security, the vast majority of the specific methods used involve gathering call and location data. One recurring observation that stands out is that the method of infiltration (in the real or virtual world) is rarely, if ever, used by either service.

There were two other new developments in 2025. Besides its standard remit (review investigations, issuing opinions, SIM reviews, etc.) the Committee R/I was requested to conduct an in-depth review of the legality of the use of special intelligence methods in the context of a legal case and at the request of the Brussels Chamber for Indictments. For the first time in its history, the Committee issued a preliminary opinion in this context in early 2025. In addition, the Committee was also called upon for the first time in its capacity as an external report channel for integrity breaches within State Security and GISS. The Committee had already anticipated this new legal competence by setting up a dedicated unit to handle it.

1 Civil Liberties Union for Europe, *Liberties Rule of Law Report 2026*, www.liberties.eu.

We cannot overlook the concerning situation of the Appeal Body either, for which the Committee R/I serves as chair and registry. In 2025, the number of appeals rose significantly as a result of the expansion of sectors for which security clearances or authorisations are necessary. In its efforts to process appeals within a reasonable time frame, the Committee R/I decided to significantly increase the number of sessions. However, given the Committee's overall mandate, and despite the goodwill of the representatives of the other bodies sitting on the Appeal Body, this increase has now reached its limits. The continued digitisation of the registry, which started in 2024, therefore remains a priority. Thanks to the ongoing dedication of all staff members at the registry of the Appeal Body, we hope to conclude this project in 2026.

Nevertheless, if this trend continues, there is a real risk of overload, and an impossible choice will have to be made between meeting reasonable deadlines, ensuring the quality of decisions, and meeting national security demands. Above all, this development poses a threat to the Committee's most important, priority role, namely reviewing the intelligence and security services.

Finally, the Committee has taken on board the need for reforms to enhance its internal operations, and various initiatives have been started in this regard.

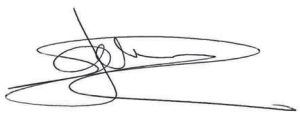
It goes without saying that an ambitious human resources policy is essential if we want to deliver high-quality work and meet the current challenges. The Committee R/I's workforce continued to expand in 2025, with virtually all departments getting reinforcements. Thanks to these efforts, the Committee can continue its work in a modern and professional manner, including by drawing up an audit plan to be implemented in 2026, as well as a strategic multi-year plan.

After 35 years, it was also clear that the Committee's visual identity needed a 'refresh'. More than just a purely aesthetic change, we wanted the new logo to be a visible expression of the profound changes and modernisation being implemented internally. We are therefore particularly proud of the result, which is the product of a long and collective process but, above all, a reflection of principles including legality, integrity, independence, and transparency—all of which guide the Committee's work.

In closing, I would like to take this opportunity—in what is more than just a routine paragraph—to express my sincere gratitude to all members of the Committee for their ongoing dedication to the public interest. Behind the Committee's ever-increasing and diverse remit are men and women who are determined to contribute to a State that is more transparent, more just, and safer.

2026 promises to be a challenging year, but I am confident that, thanks to the strength of our team, our clear vision and robust values, we will be able to meet the challenges that lie ahead. By staying on course together, we will reach our destination safely.

As a dedicated Chairwoman who is proud of the work of all members of the Committee R/I, I hope you enjoy reading our 2025 Activity Report.



Vanessa Samain
7 April 2026

REVIEW INVESTIGATIONS

THEMATIC INSIGHTS

1. COMPLETED REVIEW INVESTIGATIONS

1.1. Threats against political opponents in Belgium

In June 2023, a few weeks after the release of a Belgian aid worker (and three other Europeans) who had been arbitrarily detained in Iran for more than a year, controversy emerged regarding visas granted to an Iranian delegation visiting Brussels. Belgium issued visas 'with limited territorial validity' to 14 Iranian representatives, including the mayor of Tehran, who had been invited to participate in the *Brussels Urban Summit*, an international gathering of mayors from large cities. Revelations about alleged surveillance and spying on opponents of the Iranian regime by members of the delegation in question further fuelled the political and media controversy. In this context, the Parliamentary Monitoring Committee of the Committee P and Committee R/I requested a joint investigation on CUTA's assessment of the possible threat from the Iranian delegation. An initial joint report on this investigation was drafted by the Committee P and Committee R/I, which highlighted CUTA's limited involvement in this case—consisting solely of a dual assessment of the threat on the event and the mayor of Tehran.[1]

In addition to this specific incident, the Monitoring Committee requested that a second, broader review investigation be opened into the way in which CUTA assesses the threat posed to opponents of authoritarian regimes residing in Belgium. In this investigation, the Committees chose to focus in particular on (1) the legal and regulatory framework within which CUTA operates and the powers it has (or lacks) in analysing 'authoritarian regimes' and their activities in Belgium, and (2) where applicable, how CUTA conducts its analyses and assessments of potential threats to opponents of those regimes. The investigation also examined the relevance of the terms 'authoritarian regimes' and 'opponents', and how the CUTA applies these terms in practice.

The analysis of the legal framework confirmed that potential terrorist or extremist threats against '*opponents of authoritarian regimes present in Belgium*' do fall within CUTA's remit. CUTA can therefore conduct punctual assessments and/or strategic analyses in this domain. In practice, however, the terms 'authoritarian regime' and 'political opponent' proved to be irrelevant to CUTA. Indeed, CUTA operates on the basis of hypotheses regarding the—real or perceived—existence of a terrorist and/or extremist threat. There is no systematic monitoring (and therefore no definition or operationalisation) of these categories, although they may occasionally appear in assessments. CUTA was unable to provide figures on the number of assessment requests it receives regarding potential threats linked to (opponents of) a so-called authoritarian regime. According to CUTA, these requests generally come from the National Crisis Centre and from the Central Directorate of the Operations of Judicial Police of the Federal Police.

1 Committee R/I, *Activity Report 2023*, p. 3 ("CUTA's threat analysis of an Iranian delegation in Brussels"). At the same time, and also at the request of the Monitoring Committee, the Committee R/I launched a review investigation into the information position of the intelligence services (Committee R/I, *Review Investigation into the information position of the intelligence services and the monitoring conducted during the visit of an Iranian delegation to Brussels from 12 to 15 June 2023, for the Brussels Urban Summit, including the manner in which the screening process was conducted with a view to issuing visas to the members of this delegation*, www.comiteri.be).

In the same way as punctual assessments, strategic analyses are always started based on information regarding (potential) extremist and/or terrorist threats in Belgium or against Belgian interests abroad. Since 2020, CUTA has dedicated several analyses to the terrorist and extremist threats from the Iranian regime, following the attempted attack on a gathering of opponents of the regime in Tehran, held in Villepinte (France) in 2018 and the arrest in Belgium of a Belgian-Iranian couple in connection with that incident. CUTA describes these threats as falling under a '*foreign-linked context*' or a '*context of political opposition abroad or of interstate threats*'. Using these terms, CUTA refers to "*all actors and threats related to foreign conflicts and/or political tensions that have a certain impact on our country*." (free translated)[2] However, the Committee P and Committee R/I raised questions regarding (the scope of) this threat category, the name of which varies from document to document.

The investigation confirmed that CUTA's resources are devoted first and foremost to monitoring threats in Belgium.

The investigation by the Committee P and Committee R/I also drew attention to the ambiguity regarding CUTA's mandate with respect to 'state-sponsored threats'. In March 2022, following the Russian invasion of Ukraine, the National Security Council tasked CUTA with investigating threats originating from Russia, regardless of their nature (all-threat assessment). The Committees concluded that such a mandate would result in a potential expansion of CUTA's remit, which must be clarified and, if necessary, enshrined in law.

Recommendations

› Define the terms 'authoritarian regime' and 'opponent' and clarify the category 'foreign-linked context'

Although the investigation did not reveal any dysfunction linked to the fact that CUTA did not define the terms 'authoritarian regime' or 'opponent' of such regimes, Committee P and Committee R/I nevertheless call for consultation among the Belgian partners—for example, in the context of the T.E.R. Strategy—in order to define these terms more precisely or even operationalise them, with a view to ensuring effective communication between the services. Using different terms to describe threats linked to a foreign context ('*foreign-linked context*', '*context of political opposition abroad*', '*interstate threat*') and the lack of clarity in CUTA's responses regarding the entities in the Common Database TER (CDB TER) are causing confusion regarding the scope of this category and CUTA's powers in this regard. Consequently, Committee P and Committee R/I recommend that CUTA clarify this category of analysis.

2 CUTA, *Threat Trajectory 2023–2024*, ref. DOC CUTA/D/474035/139, p. 19.

› Developing statistical methods to assess threats connected to 'opponents'

CUTA was unable to provide statistics on the number of assessment requests it receives regarding threats linked to (opponents of) a so-called authoritarian regime. The Committee P and Committee R/I call on CUTA to continue its efforts in processing incoming and outgoing information, with the aim of compiling more accurate statistics on (among other things) the assessment requests CUTA receives.

1.2. Knowledge of and oversight of GISS Cyber Command[3]

In mid-October 2022, the Ministry of Defence established the Cyber Command. This was integrated into the Armed Forces General Intelligence and Security Service (GISS) and is therefore subject to the oversight of the Committee R/I. To ensure the efficient and effective exercise of this oversight, it was essential for the Committee to have a comprehensive understanding of all aspects of this new command. The objective of evolving Cyber Command—as part of the GISS—into a fully-fledged cyber component/cyber force could*, at first glance,* have implications for the exercise of the Committee's powers. This development raised several fundamental questions, including questions relating to GISS's performance of its duties in cyberspace, and provided the Committee with an additional reason to launch a specific review investigation into Cyber Command.

The investigation revealed that the internal governance structures and management tools confirm, in practice, the legal anchoring of Cyber Command into the GISS.

The cyber capabilities of Cyber Command currently includes leveraging cyberspace for the purposes of GISS and the Ministry of Defence, and in certain cases provide support to the nation. Depending on the mission, cyber capabilities fall under a different legal framework: the Intelligence Services Act (ISA) — in which case responsibility lies with the Cyber Command of GISS—or the Royal Decree on the Structure of the Ministry of Defence and the Act on the Deployment and Readiness of the Ministry of Defence and its implementing decree, in which case responsibility lies with the Cyber Force. Although from a legal standpoint, Cyber Command and the Cyber Force are two separate entities within the Armed Forces, this is not the case from an organisational perspective. The commander of the Cyber Command is also the commander of the Cyber Force, and there is a single organisation within which all personnel, as appropriate, serve (or are required to serve) in both capacities. While the Cyber Command's missions and authorities are legally defined in the ISA, this is not the case for the Cyber Force's missions. On the other hand, the chains of command differ depending on whether the cyber unit acts as an executive body of GISS (Chief of GISS) or as a cyber force (Chief of Defence). This dual

3 This investigation, which was concluded in December 2025, was presented in early 2026 to the Parliamentary Monitoring Committee of the Standing Police Services Monitoring Committee and the Standing Intelligence Agencies Review Committee.

legal structure, while understandable and justified, risks ambiguity in the execution of tasks and the exercise of powers, as well as disputes regarding the Committee R/I's remit, as oversight body over the activities of the cyber unit.

Recommendations

› Include the specific tasks of the Cyber Force in the Royal Decree of 30 June 2025

The Committee recommends that, as is the case with the Intelligence and Security Staff Department, the specific missions of the Cyber Force— i.e. the cyber unit acting as a combat force, in the Royal Decree of 30 June 2025, establishing the general structure of the Ministry of Defence and the powers of certain authorities. More specifically, the Committee recommends that the government specify in concrete terms in a royal decree the forms of operational deployment of the Cyber Force and, where applicable, the forms of support and military assistance.

The Committee observes that the Cyber Force cannot under any circumstances be tasked, either by regulation or in practice, with conducting intelligence activities as referred to in Article 11 of the Intelligence and Security Act, nor with carrying out the security tasks described in that provision and in the Classification Act. The Committee would also like to point out that activities falling within the legal scope of the enforcement of military security (Art. 11, §1, 2° ISA) or the protection of military secrets (Art. 11, §1, 3° ISA) cannot be assigned to the Cyber Force.

› Legally formalise the command meeting within GISS

It is standard practice within GISS to hold a command meeting every two weeks, which is attended by the Chief of GISS, the Deputy Chief, the Chief Commissioner and Deputy Chief Commissioner, the Cyber Commander, and the directors of all directorates. This command meeting *de facto* serves as the executive committee of GISS. The Committee recommends that this meeting be formally enshrined in law, through a royal decree or a ministerial decree.[4] A command meeting organised in accordance with regulations would legally confirm and perpetuate this good standard practice. In addition, it would also create an obligation for the Chief of GISS and the Cyber Commander to hold formal consultations and thereby further integrate the Cyber Command within GISS.

› Evaluate the supplied services and products

The National Strategic Intelligence Plan (NSIP) from 2022 calls for enhanced cooperation in the cyber domain between State Security and GISS. It states that, in light of the increase in allocated funds, GISS provides support to its national partners, which, among other things, involves making the intelligence collection and analysis capabilities of GISS available to State Security.

During its review investigation, the Committee received information suggesting that State Security does not currently use the cyber capabilities of GISS to a significant extent. The Committee emphasises that it has not investigated this matter further and therefore cannot confirm or refute the information in question. Nevertheless, the Committee believes that GISS should conduct a quantitative and

4 By way of comparison, the executive committee of State Security and its composition were established by royal decree (Art. 4 of the Royal Decree of 5 December 2006 on the general administration of State Security).

qualitative evaluation of the services and products it provides to other agencies, including both clients within the Ministry of Defence and external clients. In light of the government's expectations, as set out in the National Strategic Intelligence Plan, more attention must be paid to the services and products provided to State Security.

› Allocate sufficient budgetary resources for the Cyber Unit

The current geopolitical situation calls for more attention to Belgium's military cyber capabilities. The administrative and legal structure of the Cyber Command and the Cyber Force is a necessary first step in this regard. The Committee recommends that the government and the Ministry of Defence give due consideration to the necessary cyber capabilities to meet the various expectations of the political and military authorities regarding this unit. In this regard, the Committee recommends using the budgets of comparable cyber units in NATO member states as a benchmark.

› Retain 'counterattack' authority within GISS

During the review investigation, GISS announced that it would conduct a study to determine whether the Intelligence Services Act needs to be amended with regard to GISS's specific cyber operations and, in particular, its so-called 'counterattack' authority. GISS and the Cyber Unit are considering whether this authority should be removed from GISS (Cyber Command) and transferred to the Cyber Force. The Committee believes that, although this may seem logical at first glance, it is not at all the case. The authority to launch a counterattack following a cyberattack is inextricably linked to the intelligence and security remit of GISS. Furthermore, such a legal transfer to the Cyber Force would only be possible if the latter was established as a legal entity. The Committee sees no reason why the Cyber Force should be organised by law when the other branches of the armed forces, as provided for in the Constitution with regard to the organisation of the Armed Forces, are established by royal decree.

Moreover, the Committee recalls that the government decided to assign this authority to Cyber Command (see the report to the King accompanying the Royal Decree on the Structure of the Ministry of Defence of 30 June 2025).

› Allocation of staff for the Cyber Force

The Committee notes that the government decided to set up the Cyber Force as a separate branch of the armed forces. At the same time, it should be noted that every member of the military, for various reasons, is attached to a specific branch, and the setting up of the Cyber Force does not change this. For the purposes of these regulations, every member of the armed forces belongs to the Army, the Air Force, the Navy, the Medical Service, or the civilian staff. The Committee recommends examining whether a 'Cyber Force' category can be incorporated for the purposes of the above-mentioned regulations.

› Give the Parliamentary Committee on the Oversight of Military Missions to task the Committee R/I with conducting review investigations

The Committee has the authority to start a review investigation on its own initiative into the Cyber Unit acting as the Cyber Force. In connection with this, the Committee recommends that the Parliamentary Committee on the Oversight of Military Missions, which is responsible for parliamentary oversight

of the operational aspects of the Armed Forces—and therefore also of the activities of military cyber capabilities within a military operation— be granted statutory authority to task the Committee R/I with conducting a review investigation into the cyber capabilities acting as a Cyber Force. Within the federal parliament, the Monitoring Committee and a parliamentary commission of inquiry already have the authority to task the Committee R/I with conducting a review investigation.

1.3. A (controversial) French report on the Muslim Brotherhood[5]

In 2021, at the request of the Monitoring Committee, the Committee R/I conducted a review investigation into the intelligence services' monitoring of the Muslim Brotherhood and the potential threat it poses in Belgium. The publication in May 2025 of the report "*Frères musulmans et islamisme politique en France*"[6] reignited the debate over the threat posed by the Brotherhood. This report, which was highly critical of Belgium, prompted debates in the Chamber. The Monitoring Committee subsequently requested that the Committee R/I update its 2021 review investigation and assess the progress made on the recommendations.[7]

The Committee found that, since 2024, State Security and GISS have been jointly monitoring the Muslim Brotherhood as part of the joint platform *Counter Extremism & Counter Terrorism* (PFCECT). The Committee saw this as an appropriate response to its recommendation to strengthen cooperation between the two bodies in this area. The Committee also welcomes the shared definition of the phenomenon agreed upon by State Security, GISS, and their security partners. Moreover, this phenomenon will now be monitored on a permanent basis as part of the T.E.R. Strategy, in particular in the context of the Working Group on Islamic Extremism. With regard to the recommendation to raise awareness of this threat among the authorities, government agencies, and the public, the Committee took note of the initiatives undertaken by State Security and, to a lesser extent, the GISS, to improve consultation with partners by publishing memos, organising security briefings, and holding coordination meetings. State Security also drew on several of its activity reports to raise public awareness of the issues surrounding the Muslim Brotherhood. However, the Committee did not have any information regarding the progress made on the recommendation to carry out prior screening for integrity, loyalty, and discretion when awarding certain sensitive positions.

With regard to the threat assessment, the PFCECT estimates that there are around 100 individuals actively involved in spreading the ideology of the Muslim Brotherhood, and has identified several dozen organisations in Belgium that are closely aligned with the Muslim Brotherhood. Among the trends identified, the PFCECT highlights the reduction in funding for the Brotherhood, the emergence of new online religious education initiatives, and the repatriation of certain actors to Belgium following security pressure from the French authorities.

The intelligence services are of the opinion that the Muslim Brotherhood currently does not pose a direct threat of violent action in Belgium or against Belgian interests. However, the services believe that their ideology helps create a climate of polarisation. In this regard, this ideology is considered

5 This investigation was completed in December 2025 and was presented to the Monitoring Committee in early 2026.

6 Ministère de l'Intérieur, *Frères Musulmans et Islamisme Politique en France* (The Muslim Brotherhood and Political Islamism in France), available on the website www.interieur.fgouv.fr.

7 Committee R/I, *2021 Activity Report*, pp. 63–69 ("Een vernieuwde aandacht voor de Moslimbroederschap").

a potential vector of radicalisation for certain groups. The threat posed by the adherents of this ideology must therefore be assessed on an individual basis. The PFCECT expects the threat to remain stable over the coming five years. The Muslim Brotherhood will likely continue to spread their ideology, albeit to a lesser extent now that their financial income has been curtailed.

CUTA takes a different view of the phenomenon than the PFCECT, which has not changed since 2021: CUTA does not identify any direct threat that could lead to an increase in the threat level in the short or long term.

With regard to the conclusions of the French report on the presence of the Muslim Brotherhood in Belgium, the PFCECT's analysis does not entirely correspond with that of the French report: the PFCECT sees no evidence that Islamists are exercising control in Belgium and considers the influence of the Muslim Brotherhood to be more limited than what the French report suggests.

2. ONGOING REVIEW INVESTIGATIONS

2.1. The analysis methodology of State Security and GISS

State Security and GISS conduct daily individual threat assessments, in the context of which they assign labels to individuals. At various stages of an intelligence investigation, and for various reasons, these analyses may be the subject of external communication with partners and government agencies. This communication can have specific, negative consequences for citizens' rights and freedoms, as it can lead to administrative decisions that have a significant impact on them (e.g., the denial or revocation of a security clearance, refusal to issue or the revocation of a residence permit, refusal to grant Belgian citizenship, freezing of assets, etc.). However, the analysis of the intelligence services and the labels they use are sometimes contested by the individuals concerned—in particular through complaints lodged with the Committee R/I.

To shed light on what goes on behind the scenes of individual threat analyses and on how the results of these analyses are communicated to third parties, the Committee R/I launched a review investigation in 2023 regarding the analytical methodology used by intelligence and security services to classify individuals.

Following a hiatus of several months — due among other things to priority cases being processed and completed by the Committee — the investigation resumed in 2025. Additional questions were submitted to GISS and State Security, and the Committee R/I met with both services to seek clarification on certain aspects of their methodology. Inspections were also conducted on State Security's intranet. Through these investigative activities, the Committee examined what tools are available to their staff to assist them in drafting the analyses, as well as the internal quality control processes.[8]

8 A declassified version of the investigation report was presented to the Monitoring Committee in 2026.

2.2. The analysis methodology of the CUTA

In parallel with its review investigation into the analysis methodologies of State Security and GISS, the Committee R/I launched a joint investigation with the Committee P to examine CUTA's methodology in analysing individual threats.

This investigation was also suspended because other priority cases had to be processed, before being resumed in 2025. Additional questions were submitted to CUTA, which responded in writing and during meetings. CUTA's internal documentation—specifically, its threat assessment tool—was comprehensively reviewed. As part of this investigation, the Committee P and Committee R/I had a specific focus on the risk indicators used by CUTA in its threat analyses, the latter's efforts to familiarise its staff with this tool, and its internally organised quality control.[9]

2.3. (Attempts at) synergies between the two intelligence services

Among the shortcomings identified in the Belgian security chain by the parliamentary commission of inquiry tasked with investigating the terrorist attacks of 22 March 2016, the lack of cooperation between the security services and '*the lack of a culture of information sharing*' were highlighted. In its recommendations, the commission of inquiry paid particular attention to strengthening cooperation between the two intelligence services. The Committee R/I also called for better coordination between State Security and GISS on several occasions as part of its review investigations.

In response to these findings and recommendations, GISS and State Security developed a National Strategic Intelligence Plan (NSIP) in 2018. The plan was approved by the National Security Council (NSC), and a revised version was published in 2022. The aim of the Intelligence Plan is to support the agencies in carrying out their respective missions through closer cooperation, to strengthen their intelligence position, and to streamline resources. The document outlines the cooperation between the two agencies in various areas, including counterterrorism, counterintelligence, and, more specifically, IT and the organisation of training programmes. In addition to the NSIP, other instruments or protocol agreements provide for closer cooperation—or even coordination—between State Security and GISS on specific projects.

In this context, the Committee decided to launch a review investigation to identify and assess the existing and planned synergies between the two intelligence services. Synergies are defined there as sustainable forms of cooperation, in this case exclusively between State Security and GISS, characterised by the pooling of resources (e.g., human, financial, informational, or material resources) to improve effectiveness from the perspective of operations or support functions. The aim of the investigation is to determine the extent to which the synergies outlined in the action plans and policy documents are actually being implemented and how effective they are.

9 A declassified summary of this investigation report was also submitted to the Monitoring Committee in 2026.

2.4. Attack on a political opponent in Tienen

In late August 2025, the mayor of Tienen sent a letter to the Committee R/I regarding the attack on a Congolese political opponent in his municipality. Very soon after the incident, open-source information quickly revealed that the individual in question was the subject of a wanted notice issued by the Congolese authorities. The mayor complained that, in his capacity as the administrative police authority, he had not been informed by the intelligence and security services of the threat against a resident of his municipality.

This individual case is consistent with challenges that have already been examined in previous investigations by the Committee, specifically those related to the activities of foreign intelligence services against their diaspora in Belgium or those related to the transfer of intelligence to third parties. It therefore seemed appropriate to examine possible shortcomings in the intelligence services, as well as to investigate how State Security and GISS handled this case in light of previously made recommendations.

The Committee R/I's investigation concerns the information position of the services with regard to the threat against the individual in question, i.e., the information gathered by State Security and GISS and the resources they deploy to feed this intelligence gathering. The investigation also examines the exchange of information between the two intelligence services and with other partners.

3. OTHER INSPECTION ACTIVITIES

In April 2025, the Committee travelled abroad to examine Belgium's contribution to a multinational information-sharing operation in the area of counterterrorism. Inspection visits were also conducted in April 2025 regarding GISS operations in the Middle East.

For classification reasons, the results of these investigations cannot be disclosed in external reports.

INTELLIGENCE METHODS, SUPPORT MEASURES, AND DATA COLLECTION ABROAD

THE LEGAL FRAMEWORK FOR INFORMATION COLLECTION

The following sections are devoted to reviews of intelligence-gathering methods which are the subject of a specific focus by the Committee and for which it acts as a judicial body, as regards special intelligence methods (SIM). The chapter also discusses the measures that intelligence services can take to support their operations. Finally, the last section discusses foreign interceptions, video recordings, and hacking of IT systems that GISS is authorised to carry out.

1. INTELLIGENCE METHODS

Before reporting on the number of (special) intelligence methods used by the intelligence services in 2025 and the Committee R/I's review of these methods, we will briefly explain the different types of methods.

1.1. What is an intelligence method?

To gather information, the Belgian intelligence services can use three types of methods: the so-called ordinary, specific, and exceptional methods. This distinction, introduced by the legislator in 2010, is intended to classify methods according to their degree of intrusion into citizens' private lives: the more intrusive the method, the stricter the procedures and checks governing its use.

1.1.1. Ordinary methods

Ordinary methods are methods of intelligence gathering for which the legislator did not originally impose any specific prior external oversight, as this was deemed less intrusive into individuals' private lives. All methods that fall into this category are therefore subject exclusively to standard review by the Committee R/I.

Surveillance and searching publicly accessible locations without technical means (e.g. following someone on the street without filming them) and working with human sources (informants) fall under this category.

Since 2016, several new ordinary methods — known as 'ordinary methods plus' — have been introduced for which the Committee is responsible for specific review and/or for which the relevant intelligence

service has an additional obligation to provide information to the Committee. The monitoring or reporting requirements are regulated differently for each of these methods.[10]

This category includes:
- The use of images recorded by police cameras;
- Identifying the subscriber of a telecoms service (e.g. a mobile phone number or an IP address) without using a technical tool, but by submitting a request to an operator or provider;
- Identifying financial products or services used by a specific individual or company, or vice versa (e.g. verification of the identity linked to a known bank account number).

1.1.2. Specific and exceptional methods

The intelligence services may also use special intelligence methods (SIM). These methods include specific and exceptional intelligence methods. These methods must be used in accordance with the principles of legality, proportionality, and subsidiarity. The intelligence service must demonstrate that the information it is gathering in the context of its missions cannot reasonably be obtained by less intrusive means (such as an ordinary method). The scale of the resources deployed must also be proportionate to the threat level assessed by the service.

Examples of specific methods include:
- Access to call-associated and location data from electronic communications;
- Observing and searching public places using technological means (e.g., following someone on the street while taking photos or recording video).

Examples of exceptional methods include:
- Hacking an IT system;
- Eavesdropping, intercepting and recording private communications;
- Collecting information about the transactions, accounts, and assets of a specific individual, and placing the individual's transactions under supervision (real-time monitoring).

Given their more intrusive nature, special intelligence methods are subject to a **double external review** that varies depending on whether the method in question is specific or exceptional.

The administrative commission that reviews specific and exceptional methods for gathering information (the SIM Commission) conducts a **prior review** of the legality of each special intelligence method and whether it complies with the principles of proportionality and subsidiarity. The SIM Commission must be notified of any decision regarding the application of a specific method and must

10 See Committee R/I, *2022 Activity Report*, p. 84-88.

give its express consent before a service is permitted to use an exceptional method.

The Committee R/I is then responsible for the ***ex post* review** of these methods. It verifies the legality of decisions relating to these specific and exceptional methods, as well as compliance with the principles of proportionality and subsidiarity.

The Committee acts as a jurisdictional body in these cases. Prior approval from the Committee is not required to implement a SIM, but if it finds that the SIM is being used unlawfully or that the principles of proportionality or subsidiarity have not been observed, the Committee will suspend the method in question if it is still being used at that time. As data protection authority, it also orders a ban on the use and destruction of the data obtained through that method.

1.1.3. Illustration: from an ordinary observation to an extraordinary observation

In the fictitious example below, the intelligence service first uses an ordinary method before switching to a specific method and then an exceptional method to gather the necessary information. In this case, the focus is on the principles of legality, proportionality, and subsidiarity, as well as on strengthening the control and traceability mechanisms for the more intrusive methods.

An individual is flagged due to repeated contact with an extremist group that may pose a threat to national security. At this stage, there is no concrete evidence to substantiate a specific threat. The intelligence service uses an **ordinary surveillance method (Art. 16/1 ISA)**: discreet surveillance of places accessible to the public, tracking the person in question's movements, and identifying the individuals with whom they are in contact. The observation is limited to what is visible in public spaces, and no intrusive technical means are used. In practical terms, this means that the person is followed by one or more members of the intelligence service and is observed from a distance. The intelligence service can use this method without having to notify the SIM Commission or the Committee R/I.

The surveillance shows that there are regular, potentially problematic interactions in a specific building and that there is unusual activity, with people coming and going, especially at night. The intelligence service would like to examine these elements more objectively. If the potential threat is deemed significant and standard intelligence gathering methods are deemed insufficient, the intelligence service uses a **specific surveillance method (Art. 18/4 ISA)**. Specifically, this could involve setting up a camera on the street, pointed at the building's entrance, to structurally record all comings and goings. The surveillance continues outdoors and focuses exclusively on what is visible from the public domain, but is now based on a technological device that can record continuously. This specific method must be notified to the SIM Commission before it can be used. The Commission

will inform the Committee R/I. Both review bodies may terminate the use of the method at any time if they believe that the principles of legality, proportionality, or subsidiarity are no longer met.

Finally, the information gathered indicates that concrete preparations may be underway inside the building itself and that violent action is potentially being planned. The methods described above mean that the exact nature of the activities taking place behind closed doors cannot be ascertained with certainty, and no other specific methods would make that possible either. An **exceptional surveillance method (Art. 18/11 ISA)** may then be permitted, such as, for example, discreetly installing a camera inside a building that is not accessible to the public, for the purpose of observing what is going on inside. This measure constitutes a particularly significant intrusion into privacy and is only used in cases where there is a serious potential threat to national security, and is implemented within a strict legal framework. The SIM Commission must give its approval before this method can be implemented. The Committee also conducts an *ex post* review.

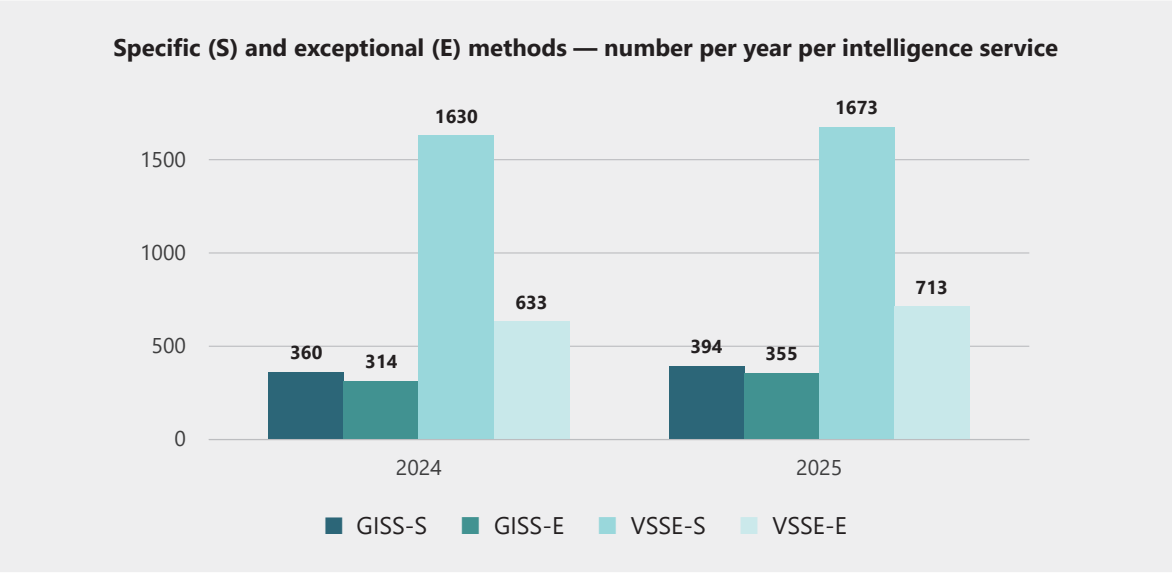
1.2. Figures on special methods and certain standard methods

1.2.1. General trends

Between 1 January and 31 December 2025, a total of **3,135 authorisations were granted for the use of special intelligence methods** by both intelligence services combined: 749 methods by the GISS and 2,386 methods by State Security. This represents a **6.7% increase compared to 2024** (when 2,937 special methods were used).[11]

11 To obtain a general quantitative overview, the Committee counts the actual number of methods used by the intelligence services. It should be noted that the intelligence services do not calculate the number of methods used in the same way. They refer to SIM files, and a file typically involves multiple methods (2.25 methods per file in 2025, compared to 2.19 in 2024). More specifically, this can be explained by the fact that some methods cannot be used independently from others. Telephone wiretapping, for example—which is an exceptional method (Art. 18/17 ISA)—cannot be carried out without collecting the call metadata, which is a specific method (Art. 18/8, §1, 1° ISA). Between 1 January and 31 December 2025, the two intelligence services together drew up 1,389 SIM files for the use of special intelligence methods: 1,152 SIM files by State Security (735 files relating to specific methods and 417 relating to exceptional methods) and 237 SIM files by GISS (112 files relating to specific methods and 125 relating to exceptional methods).

The graph below shows the trend in the number of specific and exceptional methods per intelligence service from 2024 to 2025.



A different picture emerges for the two intelligence services. Indeed, the number of SIMs implemented by State Security is considerably higher than that of GISS. This trend has been observed for many years. In 2024 and 2025, State Security's share of SIMs accounted for more than three-quarters of the total in each year.

Given that GISS exercises a large portion of its powers in a foreign context and that its missions on national territory are primarily focused on military challenges, it is logical that the number of SIMs used by this service is lower than the figure for State Security, which primarily exercises its powers in a broader domestic context. In foreign countries, GISS may also invoke Article 44 ISA, which pertains to wiretaps, video recordings, and hacking of IT systems.[12]

However, between 2024 and 2025, the number of specific and exceptional methods used by the military intelligence service rose by around 10% for both types of methods. GISS relied more on specific methods than on exceptional ones, but to a much lesser extent than State Security. This was the case both in 2024 and 2025.

For State Security, the growth curve for the number of specific methods used in 2024 and 2025 shows a slight increase (+3%), while the rise in exceptional methods is more pronounced (+13%). As mentioned above, the number of specific methods in 2025 remains significantly higher than the number of exceptional methods: for example, specific methods typically account for more than 70% of the SIMs used by State Security. This finding was also made in 2024 and confirms the trend that has been observed for several years.

12 See in this regard *"3. Foreign interceptions, recordings and hacking of IT systems"*.

1.2.2. Methods used by the GISS

Between 1 January and 31 December 2025, **749 special intelligence methods were used by GISS**, of which 394 were specific methods and 355 exceptional methods.[13]

The tables, charts, and explanatory notes below provide a detailed overview of the methods used by the GISS throughout 2025 and offer a concise analysis of how they evolved compared to the previous year.

Specific methods (GISS)

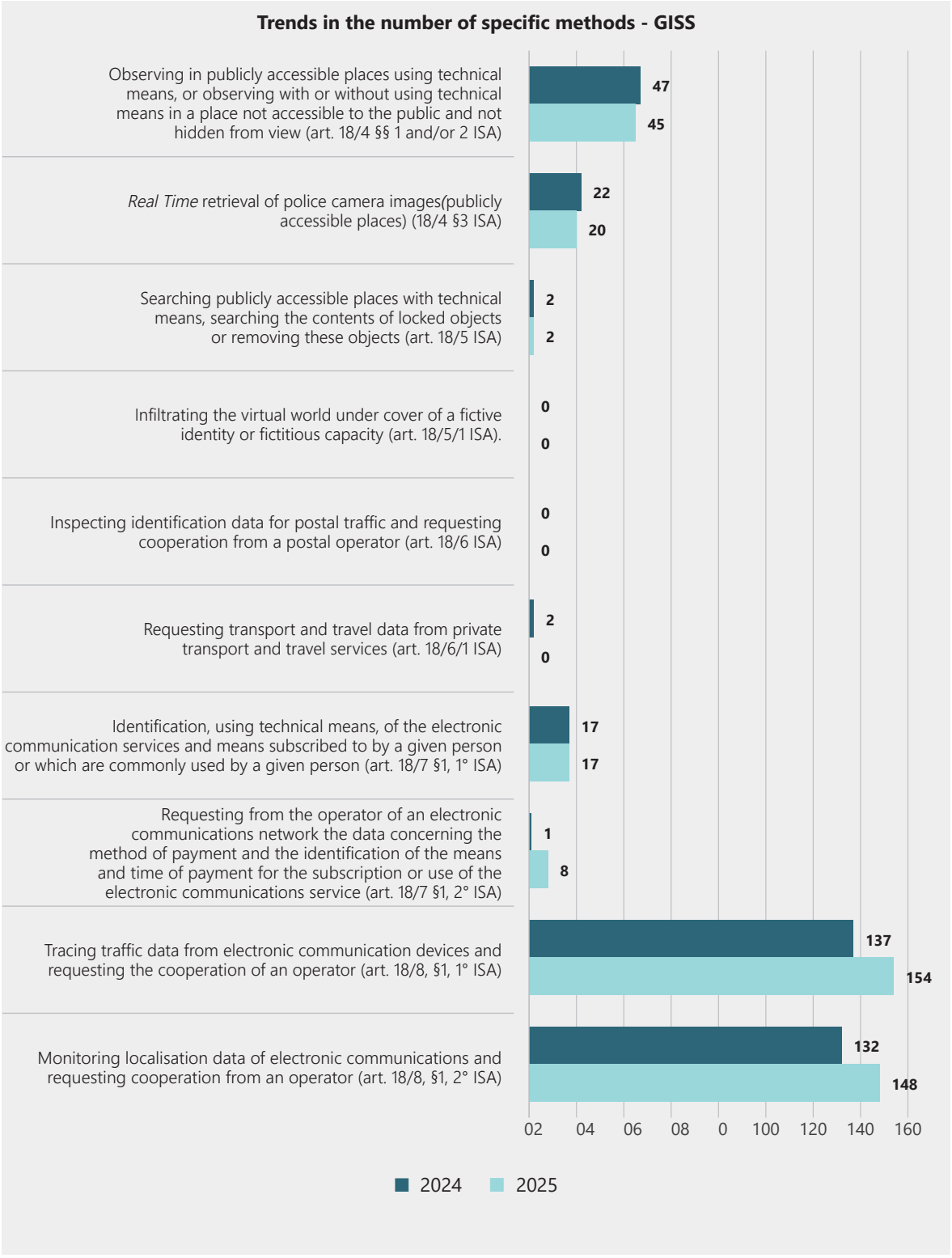
Specific methods (GISS)	2025
Observing in publicly accessible places using technical means, or observing with or without using technical means in a place not accessible to the public and not hidden from view (art. 18/4 §§ 1 and/or 2 ISA)	45
Real Time retrieval of police camera images (publicly accessible places) (18/4 §3 ISA)	20
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 cover of a fictive identity or fictitious capacity (art. 18/5/1 ISA).	0
Inspecting identification data for postal traffic and requesting cooperation from a postal operator (art. 18/6 ISA)	0
Requesting transport and travel data from private transport and travel services (art. 18/6/1 ISA)	0
Identification, using technical means, of the electronic communication services and means subscribed to by a given person or which are commonly used by a given person (art. 18/7 §1, 1° ISA)	17
Requesting from the operator of an electronic communications network the data concerning the method of payment and the identification of the means and time of payment for the subscription or use of the electronic communications service (art. 18/7 §1, 2° ISA)	8
Tracing traffic data from electronic communication devices and requesting the cooperation of an operator (art. 18/8, §1, 1° ISA)	154
Monitoring localisation data of electronic communications and requesting cooperation from an operator (art. 18/8, §1, 2° ISA)	148
TOTAL	**394**

Tracing traffic data from electronic communications devices and localisation of the origin or destination of electronic communications (art. 18/8, §1, 1° and 2° ISA) are still the two most frequently used specific methods by GISS. These methods are usually used together, which explains why their numbers are almost identical. Surveillance using technical means or in a location that is not accessible to the public (Art. 18/4, §§ 1 and/or 2 ISA) remains the third most commonly used method by the military intelligence service.

If we compare these figures with those for 2024, we see that the number of specific methods used by the military intelligence service increased by 9% between 2024 and 2025.

13 For 237 SIM files, with an average of 3.2 methods per file.

The graph below illustrates the trend in the use of specific methods by GISS from 2024 to 2025. Upon closer examination, it becomes apparent that the trends differ somewhat. Indeed, the comparison shows that, although there has been a rise in the total number of specific methods, the use of certain methods has declined slightly. This is the case in particular for surveillance as well as for *real-time* access to police camera images. On the other hand, the increase is biggest for the two specific methods that are used most frequently (access to traffic data from electronic communications and to location data (Art. 18/8, §1, 1° and 2° ISA)).



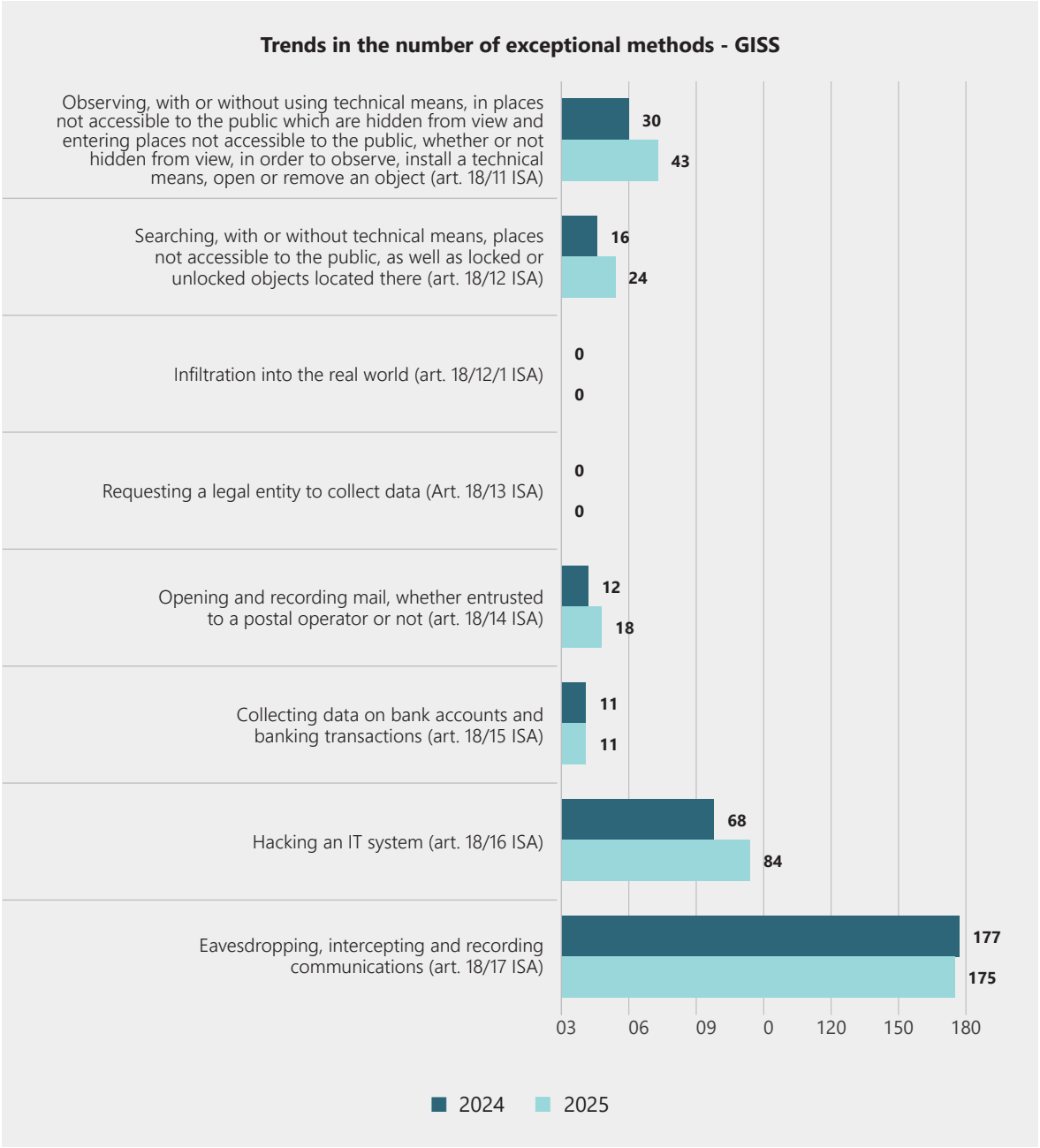
Exceptional methods (GISS)

Exceptional methods (GISS)	2025
Observing, with or without using technical means, in places not accessible to the public which are hidden from view and entering places not accessible to the public, whether or not hidden from view, in order to observe, install a technical means, open or remove an object (art. 18/11 ISA)	43
Searching, with or without technical means, places not accessible to the public, as well as locked or unlocked objects located there (art. 18/12 ISA)	24
Infiltration in the real world (art. 18/12/1 ISA)	0
Requesting a legal entity to collect data (Art. 18/13 ISA)	0
Opening and recording mail, whether entrusted to a postal operator or not (art. 18/14 ISA)	18
Collecting data on bank accounts and banking transactions (art. 18/15 ISA)	11
Hacking an IT system (art. 18/16 ISA)	84
Eavesdropping, intercepting and recording communications (art. 18/17 ISA)	175
TOTAL	**355**

Intercepting communications (Art. 18/17 ISA) was the exceptional method most frequently used by the military intelligence service in 2025, accounting for nearly half of the total number of exceptional methods. Hacking into an IT system (Art. 18/16 ISA) and surveillance in areas not accessible to the public (Art. 18/11 ISA) were in second and third place, respectively. These findings are consistent with the general trend of recent years, since these methods were also the three most commonly used exceptional methods used by the military intelligence service in 2022, 2023, and 2024.

The graph below illustrates the trend in the use of exceptional methods by GISS from 2024 to 2025. A comparison with the figures for 2024 shows that the number of exceptional methods actually used by GISS in 2025 was generally higher than in the previous year. Depending on the type of method, the trend fluctuates between a rise and stagnation. There was a very slight decrease in interceptions of communications (Art. 18/17 ISA). Hacking into IT systems (Art. 18/16 ISA) saw the largest increase in net figures for 2025 compared to 2024.

In 2024 and 2025, GISS did not use infiltration in the real world or in the virtual world (the latter being a specific method). GISS did not use a legal entity to collect data either. The same observations also apply to State Security.



Threats for which specific and exceptional measures are implemented (GISS)

As was the case last year, espionage was the threat for which GISS used the most SIMs in 2025.[14] There was a rise in the use of SIMs as part of the fight against interference. SIMs related to organised crime rose significantly, although still represent a small share overall. The number of SIMs related to extremism and terrorism remains low. This is not necessarily a surprise, given that GISS focuses on situations abroad in these cases and can invoke Article 44 ISA.[15]

14 A method can be used to address multiple threats.

15 See in this regard "*3. Foreign interceptions, recordings and hacking of IT systems*".

Ordinary 'plus' methods (GISS)

The ISA also provides for ordinary methods, for which the Committee R/I is responsible for specific review and/or for which the relevant intelligence service has an additional obligation to provide information to the Committee (the so-called ordinary 'plus' methods).[16] The requirements regarding oversight or information to be provided are regulated differently for each of these methods, despite the Committee's repeated calls to standardise the requirements.

A comparison with the figures for 2024 shows a rise in the use of these methods in 2025.

Ordinary 'plus' methods (GISS)	2025	2025
Identification of the 'subscriber or habitual user' of telecommunications (art. 16/2 ISA)	432	571
Targeted PNR data searches (art. 16/3/1 ISA)	7	21
Use of police camera images (not in real time) (art. 16/4, §2 ISA)	18	22
Requesting financial data (art. 16/6 ISA)	23	27

There has been an overall rise of around 25% in the use of the identification of the "subscriber or habitual user" of telecommunications (Art. 16/2 ISA), the use of police camera images (not in real time) (Art. 16/4, §2 ISA), and requesting certain financial data (Art. 16/6 ISA).

The use of the method of targeted searches of PNR data (Art. 16/3/1 ISA) tripled in 2025. The rise in the figures for this latter method can be explained by the fact that a decline in the number of targeted searches of PNR data was recorded in 2024, following a ruling by the Constitutional Court on 12 October 2023, which annulled Article 16/3 ISA.[17] This ruling meant that State Security and GISS could no longer conduct searches in the PNR database. A reparation Act passed by the legislator and adopted on 15 July 2024 allows the intelligence services once again to search the PNR database a second time, which explains why these methods were resumed in mid-2024.

1.2.3. Methods used by State Security

Between 1 January and 31 December 2025, State Security granted **2,386 authorisations to use special intelligence methods**, of which 1,673 were specific and 713 exceptional methods.[18]

16 See in this regard "*1.1 What is an intelligence method?*".

17 In its ruling (ruling 131/2023), the Court ruled that the scope of action for the intelligence services was 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 were rescinded, as was article 16/3 ISA that regulated such requests. Until the passage of the Reparation Act, the intelligence services could no longer access the PNR database.

18 For 1152 SIM files, with an average of 2 methods per file.

The tables, charts, and explanatory notes below provide a detailed overview of the methods used by State Security throughout 2025 and offer an analysis of how they evolved compared to the previous year.

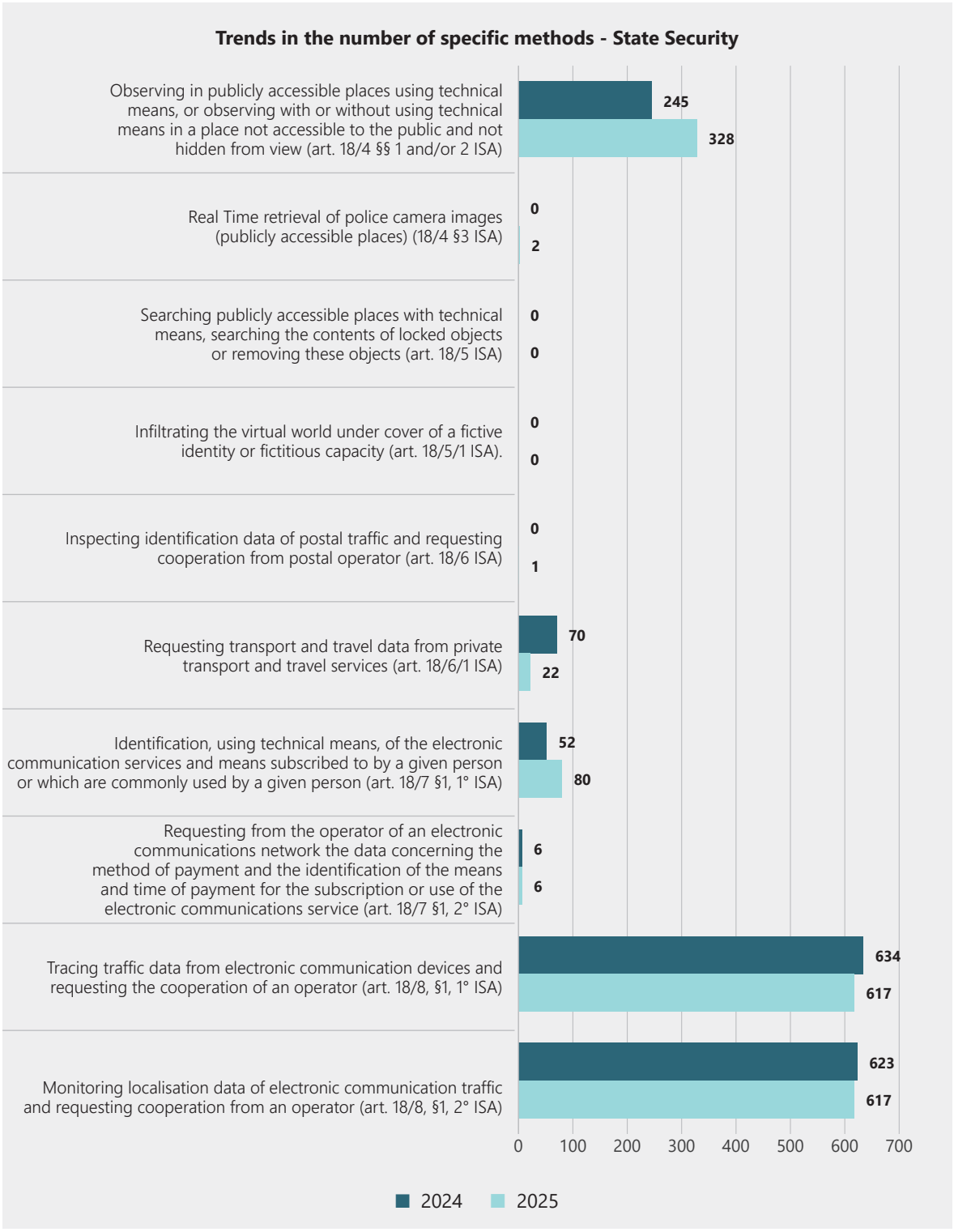
Specific methods (State Security)

Specific methods (State Security)	2025
Observing in publicly accessible places using technical means, or observing with or without using technical means in a place not accessible to the public and not hidden from view (art. 18/4 §§ 1 and/or 2 ISA)	328
Real Time retrieval of police camera images (publicly accessible places) (18/4 §3 ISA)	2
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 cover of a fictive identity or fictitious capacity (art. 18/5/1 ISA).	0
Inspecting identification data for postal traffic and requesting cooperation from a postal operator (art. 18/6 ISA)	1
Requesting transport and travel data from private transport and travel services (art. 18/6/1 ISA)	22
Identification, using technical means, of the electronic communication services and means subscribed to by a given person or which are commonly used by a given person (art. 18/7 §1, 1° ISA)	80
Requesting from the operator of an electronic communications network the data concerning the method of payment and the identification of the means and time of payment for the subscription or use of the electronic communications service (art. 18/7 §1, 2° ISA)	6
Tracing traffic data from electronic communication devices and requesting the cooperation of an operator (art. 18/8, §1, 1° ISA)	617
Monitoring localisation data of electronic communications and requesting cooperation from an operator (art. 18/8, §1, 2° ISA)	617
TOTAL	**1,673**

As regards the specific methods used in 2025, access to traffic data from electronic communications and to location data (Art. 18/8, §1, 1° and 2° ISA) were the two specific methods used most often by State Security. Together, they accounted for just under three-quarters of the specific methods used by State Security in 2025. These methods are usually used together, which explains why their numbers are identical. Surveillance using technical means in places that are not accessible to the public (Art. 18/4, §§ 1 and/or 2 ISA) remains the third most commonly used method by the civilian intelligence services. These three methods are also the ones most commonly used by GISS (see above).

When comparing these figures with those for 2024, it can be seen that the number of specific methods used by State Security increased only slightly between 2024 and 2025 (+43 cases, i.e. an increase of just under 3%). The breakdown by method reflects a somewhat uneven trend. The number of the two specific methods that were used most frequently appears to have decreased slightly compared to 2024. On the other hand, there was a noticeable rise in cases of surveillance conducted using technical means or in places not accessible to the public (Art. 18/4, §§ 1 and/or 2 ISA), which rose by 33% in a single year. There was also a clear decline in the number of requests for transport and travel data (Art. 18/7, §1, 2° ISA).

Finally, it should be noted that State Security did not invoke Article 18/5 ISA in 2024 or 2025 (nor in any previous years), which provides for the possibility, in the event of a potential threat falling within State Security's remit, to search publicly accessible locations using technical means and to inspect or seize the contents of locked objects found there. State Security did not infiltrate the virtual world either (Art. 18/5/1 ISA). The same applied to GISS.



Exceptional methods (State Security)

Exceptional methods (State Security)	2025
Observing, with or without using technical means, in places not accessible to the public which are hidden from view and entering places not accessible to the public, whether or not hidden from view, in order to observe, install a technical means, open or remove an object (art. 18/11 ISA)	22
Searching, with or without technical means, places not accessible to the public, as well as locked or unlocked objects located there (art. 18/12 ISA)	18
Infiltration in the real world (art. 18/12/1 ISA)	0
Requesting a legal entity to collect data (Art. 18/13 ISA)	0
Opening and recording mail, whether entrusted to a postal operator or not (art. 18/14 ISA)	17
Collecting data on bank accounts and banking transactions (art. 18/15 ISA)	82
Hacking an IT system (art. 18/16 ISA)	101
Eavesdropping, intercepting and recording communications (art. 18/17 ISA)	473
TOTAL	**713**

The most commonly used exceptional method was telephone wiretapping (Art. 18/17 ISA). This method alone accounts for more than half of the total number of exceptional methods State Security used in 2025. A similar trend was observed for GISS (see above). This is followed by hacking into an IT system (Art. 18/16 ISA), which is also the second most commonly used method by the military intelligence service. On the other hand, it appears that gathering information on bank accounts and transactions (Art. 18/15 ISA) is a method that was rarely used by GISS—about ten times a year—even though this was the third most commonly used method by State Security in 2025.

Finally, it should be noted that, compared to GISS, State Security makes less use of surveillance and search methods for places that are not accessible to the public (Articles 18/11 and 18/12 ISA). State Security used the exceptional method of observation 22 times, compared to 43 times for the GISS. State Security used the exceptional method of search 18 times in 2025, while GISS used it 24 times.

A comparison with the number of exceptional methods used by State Security in 2024 shows that the number of these methods increased by 13% between 2024 and 2025 (a net increase of 80 methods). The graph below shows the trend in the use of each exceptional method. It shows that for two of the three exceptional methods most frequently used by State Security in 2025, there was a noticeable increase compared to the previous year. These were interceptions of communications (Art. 18/17 ISA) and gathering information on bank accounts and transactions (Art. 18/15 ISA). These two methods saw a significant increase between 2024 and 2025 (from 380 to 473 and from 59 to 82 methods, respectively). This trend was not observed for GISS, where the use of both methods has remained stable *(see above)*. Finally, while hacking into IT systems (Art. 18/16 ISA) saw the largest increase in net figures for 2025 compared to 2024 among the exceptional methods used by GISS, the use of this method by State Security declined slightly compared to 2024.

From 2023 until 2025, State Security did not use infiltration in the real world or in the virtual world (the latter being a specific method). State Security did not use a legal entity to collect data either. These findings were also observed for GISS.

FOCUS: false names and fictive identities, false and fictive titles

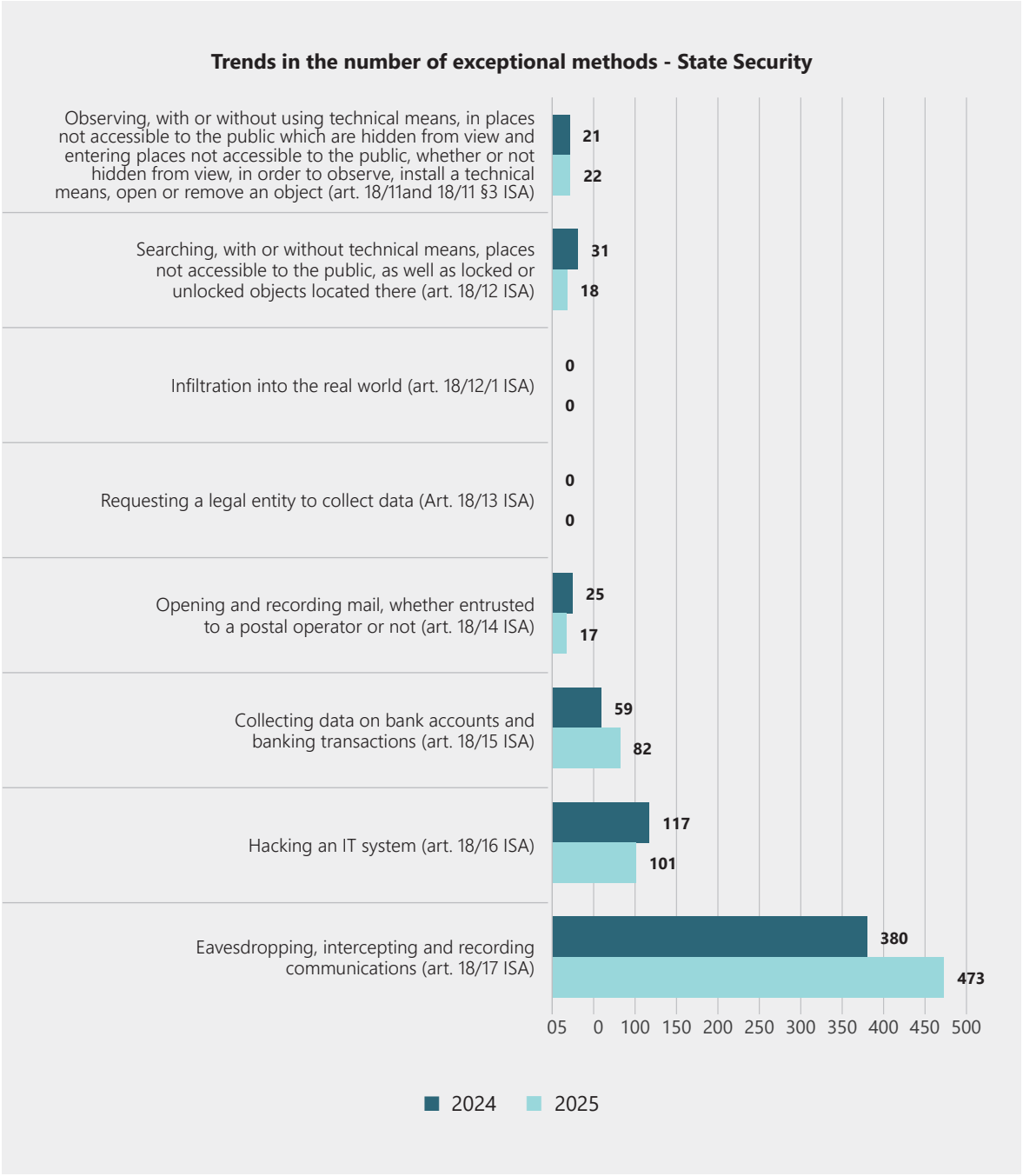
The ISA differentiates between false names and fictive identities. In both cases, a member of the intelligence and security service uses a name that is not their own.

The main difference is the proof of identity regarding the name: a **false name** does not have any official ID documents to corroborate it, whereas a **fictive identity** is substantiated by an ID card, passport, foreign national registration card, or residence permit. The false name can be supported by documents (e.g. business cards, a resume, etc.) created by the intelligence service, as long as they are not official documents included on the list for fictive identity.

The second difference is that a false name is limited to what it is—a false first and last name—while a fictive identity is a broader concept that can include all the information in the documents corroborating that identity (national identification number, date of birth, nationality, etc.).

The differences between a false name and a fictive identity therefore correspond to a spectrum ranging from the information involved, the credibility of the false information, to the state resources used to bolster this credibility.

The ISA also allows a member of an intelligence service to use a title that is not their own, such as a profession (e.g. diplomat, professor, electrician, etc.), a status (e.g. owner, political refugee), a capacity, or a position. There is also a gradation here: if there are legal consequences from the title used by the member of the intelligence service, it is a **fictive capacity**. If there are no specific legal consequences of the title used by the agent, it is a **false capacity**.



Threats for which specific and exceptional measures are implemented (State Security)

Among the threats monitored by the civilian intelligence service, terrorism and espionage account for the lion's share of special intelligence methods used, as was the case in 2024. These were followed by threats of interference and extremism, in terms of the number of SIMs. To a lesser extent (though with increasing frequency), State Security uses special intelligence methods in the context of the fight against organised crime.

Ordinary 'plus' methods (State Security)

With the exception of the use of police camera images (not in *real time*), which is declining, State Security's use of these ordinary 'plus' methods increased significantly in 2025. Identifications of the "subscriber or habitual user" of telecoms services (i.e., the identity of the person linked to the SIM card) rose from 5,543 to 6,439, requests for certain financial data remained stable (from 229 to 330), and targeted searches for PNR data saw a notable increase (from 74 in 2024 to 207 in 2025). This drastic rise, which was also observed for GISS, can be explained by the fact that a decline in the number of targeted searches of PNR data was recorded in 2024, following a ruling by the Constitutional Court on 12 October 2023, which annulled Article 16/3 ISA.[19] A Reparation Act in July 2024 made it possible for the intelligence services to consult the PNR database again.

Ordinary 'plus' methods (State Security)	2025	2025
Identification of the 'subscriber or habitual user' of telecommunications (art. 16/2 ISA)	**5,543**	**6,439**
Targeted PNR data searches (art. 16/3/1 ISA)	**74**	**207**
Use of police camera images (not in *real time*) (art. 16/4, §2 ISA)	**76**	**53**
Requesting financial data (art. 16/6 ISA)	**229**	**330**

1.3. Reviews by the Committee R/I

This section looks at the reviews of special intelligence methods by the Committee R/I. Before discussing the number and nature of the decisions made by the Committee in 2025, the review method of the SIMs will be described in more detail. There will be a special focus on the regulated professions in this regard, as well as on the first preliminary advisory opinion issued by the Committee in January 2025.

1.3.1. Nature of the review

Regarding SIMs, the Committee's jurisdictional review pertains to the legality, proportionality, and subsidiarity of specific and exceptional intelligence methods.

The Committee does not have to give its approval before a SIM is used, but it may order that a method no longer be used, prohibit the use of information collected using that method, and order the destruction of the information if it finds any illegality or non-compliance with the principles of proportionality or subsidiarity.

In order to carry out this *ex post* review, the Committee considers *all* authorisations for the use of SIM (Art. 43/3 ISA). If, during the review, there are prima facie suspicions of irregularities, the Committee will take over the case for a more comprehensive review (Art. 43/2 ISA).

19 See above.

In addition to this approach based on its own initiative, the Committee may be seised in four other ways (Art. 43/4 ISA):

- At the request of the Data Protection Authority (DPA);
- In response to a complaint from a citizen;
- By operation of law, if the SIM Commission has suspended a specific or exceptional method on the grounds of illegality and has prohibited the use of the information;
- By operation of law, if the competent minister has granted consent pursuant to Article 18/10, § 3 ISA.

Once it has been seised, the Committee can make various types of decisions.[20]

1. To discontinue the method in question if it is still being used or if it has been suspended by the SIM Commission, and to prohibit the use of information collected through this method and order that it be destroyed (Art. 43/6, §1, para. 1, ISA)&S);
2. To partially discontinue the use of an approved method;
3. To fully or partially lift the suspension and ban imposed by the SIM Commission (Art. 43/6, §1, para. 1, ISA). This means that the method approved by the head of department is (partially) considered by the Committee to be lawful, proportionate, and subsidiary;
4. To determine that the Committee R/I does not have jurisdiction;
5. To declare that the pending case is unfounded and permit the continued use of the method.

In addition, the Committee can also be seised in its capacity as "Prejudicial consulting body" (arts. 131*bis*,189*quater* and 279*bis* Code of Criminal Procedure). In such cases, the Committee issues an opinion on the legality 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.

1.3.2. Decline in the number of times the Committee was seised

In 2025, the Committee was seised **12 times**. This number, a clear decrease compared to 2024 (23 referrals), is comparable to 2023 (13 referrals).

All referrals are the result of suspension by the SIM Commission. This means that, during its *prima facie* review of all authorisations to use special methods, the Committee did not identify any elements that would require it to take action on its own initiative.

20 These are only final decisions. Several interim decisions may be made during the processing of a case (e.g., hearing the members of the SIM Commission, requesting additional information from the intelligence service).

Type of referral	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
1. On the Committee's initiative	16	3	1	1	4	2	1	5	0	0	0
2. Data Protection Authority	0	0	0	0	0	0	0	0	0	0	0
3. Complaint	0	1	0	0	0	0	0	0	0	2	0
4. Suspension by SIM Commission	11	19	15	10	12	9	8	9	13	20	12
5. Authorisation by minister	0	0	0	0	0	0	0	0	0	0	0
6. Prejudicial consulting body	0	0	0	0	0	0	0	0	0	1	0
TOTAL	**27**	**23**	**16**	**11**	**16**	**11**	**9**	**14**	**13**	**23**	**12**

Of these 12 referrals, 4 relate to GISS and 8 to State Security. Several authorisations concerned methods relating to the same person(s) of interest.

1.3.3. Prohibition on the use of illegally collected information and order to destroy it

For all referrals in 2025, the Committee ordered the cessation of the method and the destruction the illegally-collected information.

The decisions made can be divided into four categories based on the nature of the problem identified:

Access to more information than what is covered by the method

Three suspensions resulted from errors where too much information being disclosed about the subject. In two cases, the error was attributable to the third service requested by the intelligence service:

- An intelligence service wanted to use an exceptional method to find out which applications two targets were using and what the content of their communications via those applications was (*datatap*). The request related to three phone numbers. After receiving the SIM Commission's assent, the method was implemented by a Belgian external service. However, the intelligence service confirmed that it had received regular telephone calls on the three telephone numbers in question while this had not been requested; according to the operational decisions of the service in question, the request pertained solely to data exchanges. When the head of department discovered this error, he notified the SIM Commission. The SIM Commission saw no other option but to issue a prohibition on the use of this information, and referred the matter to the Committee. The Committee ruled that the interception of the regular phone calls was illegal. It ordered that this unlawfully obtained information not be used and that it be destroyed.
- A similar case occurred a few months later. It concerned the same intelligence service that wanted to carry out a similar operation (*datatap*) on a cell phone number.

› An intelligence service wanted to use an exceptional method to obtain information about banking transactions made on an account over a period of several months. Only specific banking transactions were targeted, which referred to a specific element in the transaction communication. After receiving a unanimous opinion from the SIM Commission, the intelligence service solicited an operator to implement the method. By mistake, the request sent to this operator did not specify that the transactions were to be sorted based on their communication. Although the intelligence service sent a new, correct request, it had in the meantime received all the transactions made in this bank account during the specified period. After the head of the intelligence service informed the SIM Commission, the latter ruled that the data had been collected illegally and prohibited its use. The Committee R/I was seised by the SIM Commission, and upheld the finding of illegality, prohibited the use of the information in question, and ordered that it be destroyed.

Gathering information about a person who is not a target

Three other decisions ordering the prohibition of use and destruction of illegal information were due to the fact that the collected information pertained to individuals who were not the targets of the intelligence service:

› An intelligence service wanted to use specific and exceptional methods to obtain call and location data, as well as the content of communications relating to a target's phone number, during a specific period. Several months after these methods were implemented, the intelligence service found that the phone number on which the methods had been used did not belong to the target, but to another person with the same first and last name who frequented the same areas as the target and also had many mutual acquaintances. The head of department informed the SIM Commission, and the latter ruled that the information collected using this method was illegal and could not be used. The Committee R/I upheld the finding that the data had been obtained illegally, thereby prohibiting its use and ordering that it be destroyed.

› An intelligence service had launched a specific method to obtain call and location data from a cell phone number. To implement the method, the assistance of a telephone operator was needed. After the method had been implemented, the intelligence service realised that the operator had made a mistake and had sent the requested information for the wrong phone number. The intelligence service informed the SIM Commission of the mistake. The SIM Commission ruled that the information collected was unlawful, prohibited its use, and referred the matter to the Committee R/I. The latter upheld the finding that the information collected was unlawful, prohibited its use, and ordered that it be destroyed.

Collecting information outside the period stipulated in an authorisation

Five decisions were made after information on the target had been collected outside the period for which authorisation had been granted:

- An intelligence service intended to continue monitoring the activities of a target, specifically using technical devices. After observing the target using a specific method, the intelligence service requested an extension of this surveillance on several occasions. However, the specific methods used in alternation meant that the intelligence service could not observe the target for a continuous period using technical devices. Indeed, there were always a few days between two surveillance periods, and those days were not covered by any method. However, during three brief periods for which no authorisation had been granted, the intelligence service collected information using technical devices. Several months after conducting the surveillance, the intelligence service reported this incident to the SIM Commission. The Commission found that the information collected during periods for which no authorisation had been granted was illegal, and prohibited its use. The Committee R/I adopted three decisions confirming this interpretation and ordered the destruction of the information in question.
- In the context of another case involving the same type of surveillance material, a similar mistake was made, which the relevant intelligence service also reported to the SIM Commission. Following the SIM Commission's decision to prohibit the use of the data, the Committee R/I also ruled that the information collected outside the authorised period was illegal, that it could not be used, and that it must be destroyed.
- An intelligence service had launched a specific method to obtain call and location data from a cell phone number, for a limited period of time. However, the operator provided information to the intelligence service for a period longer than that specified in the authorisation. After being informed of this by the intelligence service, the SIM Commission decided to prohibit the use of the data that had been collected outside the period covered by the authorisation. After the Committee R/I had been seised by the SIM Commission, it upheld the finding that the information has been collected unlawfully, prohibited its use and ordered its destruction.

A disproportionate measure

- An intelligence service wanted to extend an observation method targeting a vehicle. However, based on information the intelligence service had previously gathered, it appeared that the vehicle was no longer used by the target of the measure. Consequently, the SIM Commission concluded that the head of department's decision did not justify the need for the specific method; it considered that both the factual circumstances and the justification as regards subsidiarity and proportionality were insufficient. The SIM Commission ordered the suspension of the method in question and prohibited the use of the collected information. After the case was referred to the Committee R/I, it upheld the finding that the measure was unlawful, prohibited the use of the information collected through this measure, and ordered that the data be destroyed.

1.3.4. The Committee's special focus on specific profiles

Regulated professions

The ISA stipulates that SIMs targetting a lawyer, doctor, or journalist can only be authorised if it is strictly necessary to fulfil the legal remit of the intelligence services and no less intrusive measure is possible. Authorisation is subject to a stricter procedure and a specific review. Furthermore, information subject to professional secrecy or source protection may be used only to the extent that it is strictly relevant to the threat in question, in order to minimise the impact on fundamental rights.

In 2025, SIMs were used in only a very limited number of cases against professions that enjoy special protection. In the context of its control remit, the Committee conducted the necessary verifications and ruled that the guarantees and conditions stipulated by law had been met.

Other titles: elected officials and diplomats

The ISA does not provide a specific protection scheme for elected officials or diplomats that is comparable to the scheme in place for lawyers, doctors, or journalists. However, given the specific nature of their functions and their role in society, it is essential to pay special attention to the potential involvement of these individuals when SIMs are used, in order to assess their scope and consequences with the necessary precaution.

In 2025, SIMs were used against elected officials and diplomats in only a limited number of cases. The Committee conducted the necessary verifications and ruled that the guarantees and conditions stipulated by law had been met.

1.3.5. A first preliminary opinion issued in January 2025

In 2024, the Committee R/I was asked for the first time since its inception to issue a preliminary opinion on the legality of specific and exceptional methods, after information collected through these methods had been used in a criminal case.[21] The Committee issued its opinion in January 2025. The course of the investigation, as well as a discussion of a number of questions that arose during it, are summarised below.

21 Apart from the various ways in which the Committee can be seised to conduct an *ex post* review of specific and exceptional intelligence methods (see, in this regard, point "*1.3.1 Nature of the review*"), the Committee may also be seised in its capacity as a "prejudicial consulting body" (Articles 131*bis*, 189*quater*, and 279*bis* of the Code of Criminal Procedure). Where appropriate, the Committee issues advice on the legality of the specific or exceptional methods used to collect information in the context of a criminal case. Requests for advice are submitted by the preliminary courts or the criminal courts.

Review of the file and the Committee's advice

The request was lodged with the Chamber for Indictments of the Brussels Court of Appeal by a suspect who sought a preliminary review of the legality of the proceedings brought against him.

Based on a combined reading of Articles 235*bis* and 131*bis* of the Code of Criminal Procedure (Sv.), the Committee can be requested to issue an opinion when reviewing the regularity of the proceedings, even before the stage of determination of the court proceedings, the Chamber for Indictments, in its judgment of 24 September 2024, requested the Committee R/I to rule on the specific and exceptional methods used by State Security.

In the case in question, State Security had used a significant number of specific methods of intelligence gathering before informing the SIM Commission of the existence of criminal offences that subsequently became the subject of a declassified official report pursuant to Article 19/1 ISA.

After reviewing the case file, the Committee concluded that the special intelligence methods in question were decided upon and implemented in accordance with the law.[22]

This case also gave the Committee R/I an opportunity to address a number of questions (summarised below) regarding the scope of the referrals made to it, as well as the overlap between criminal and intelligence investigations.

Scope of the referrals made to the Committee

During its investigation, the Committee ruled that the scope of the referrals made to it varies depending on whether it is seised with an *ex post* review pursuant to Articles 43/2 et seq. ISA (e.g. in response to a complaint) or through a preliminary opinion based on the Code of Criminal Procedure (Sv).

Pursuant to Article 43/2 ISA et seq., this review by the Committee R/I pertains to the legality, proportionality, and subsidiarity of the specific and exceptional methods of gathering information used by the intelligence and security services against an individual who can demonstrate a personal interest. In this case, the Committee examines the specific methods used by both intelligence services that were specifically targeted at the individual in question or which, even if they were not targeted at the individual in question, made it possible to collect personal information regarding the individual directly. 'Direct collection' refers to any situation in which the individual is the source of the information collected about that person when the method is applied. In other words, 'direct collection' refers to the collection of

22 During the review of the case file, State Security answered all of the Committee's questions and submitted all necessary documents.

information that the individual directly provides himself or herself, discloses, or communicates, and that is then collected by the intelligence service. This therefore does not apply to situations in which information about the individual is collected from a third party.

In the preliminary assessment, the scope of the referral is broader, as it concerns all special methods of information collection that have been used and led to the release of a declassified official report of the SIM Commission pursuant to Article 19/1 ISA.

As a result of this difference, the scope of the Committee's review of the same intelligence investigation is not necessarily the same depending on whether it comes from a complaint or a request for a preliminary opinion.

Concurrent criminal and intelligence investigations

The Committee confirmed that intelligence services may conduct an intelligence investigation concurrently with a criminal investigation carried out by the judicial authorities.

Although the intelligence services are obliged to provide a report to the SIM Commission if they become aware of certain indications of criminal offences, the purpose of an investigation by an intelligence service is to collect information related to their legal remit.

Articles 13/5 and 19/1 ISA contain provisions regarding the interaction between an intelligence investigation and a criminal investigation. Article 13/5 ISA therefore cannot be interpreted to mean that a criminal investigation takes precedence over an intelligence investigation, or that conducting these two types of investigations concurrently is prohibited. On the contrary, this article allows for numerous scenarios in which an intelligence investigation is conducted concurrently with a criminal investigation.

Article 19/1 ISA also provides a framework for what happens when the intelligence services report certain indications or facts to the SIM Commission. The implications regarding the probative value of a declassified official report must be assessed by the criminal court and not by the Committee.

The Committee can verify whether the intelligence and security services have in fact complied with these two articles. However, the Committee does not have the authority to review the operations of the SIM Commission, whose independence is guaranteed by law.

Finally, the Committee R/I is of the opinion that any shortcomings in the consultation and/or communication between an intelligence service and the SIM Commission, on the one hand, and the judicial authorities, on the other, do not impact the legality of the methods.

2. SUPPORT MEASURES

Since the 2022 legislative amendment, intelligence services can request support measures. Articles 13/1 to 13/3 ISA provide for the possibility of committing criminal offences, using false names, and setting up legal entities for the sole purpose of improving the intelligence service's information position through an agent or a source. These are so-called 'support measures' and not intelligence methods, as they cannot be used to gather information. However, they must be proportionate to the intended purpose, and the physical integrity of individuals must never be compromised in implementing these measures. The intelligence services implement support measures to protect or improve their intelligence position; for example, a source who makes statements online that are punishable under criminal law, to demonstrate his loyalty to an extremist group.

Support measures are also subject to strict rules. In cases involving criminal offences, the requesting intelligence service must always submit the request to the SIM Commission, so that the latter can make a decision regarding the proportionality. For the use fictive identities, the intelligence service only needs to send a monthly list.[23]

In 2025, the SIM Commission approved 17 requests for authorisation to commit criminal offences by agents or human sources. These were all submitted by State Security.

3. FOREIGN INTERCEPTIONS, RECORDINGS AND HACKING OF IT SYSTEMS

Article 44 ISA allows GISS to detect, intercept, eavesdrop and record any form of communication sent or received abroad.

In this context, GISS is tasked with drawing up an interception plan, a hacking plan, and an image recording plan each year, in which it "*compiles a list of organisations or institutions whose communications will be the subject of interception, hacking into their IT systems, or recording of still or moving images during the coming year. These lists must specify, for each organisation or institution, the reason why it is the subject of an interception, hacking, or recording of still or moving images in connection with the tasks referred to in Article 11, §1, 1° through 3° and 5°, and must state the expected duration*" (freely translated) (Art. 44/3 ISA).

These powers are subject to a three-phase review by the Committee—before, during, and after the interception, hacking, or recording takes place. The *a priori* review is conducted on the basis of the lists compiled by GISS each year and submitted to the Minister of Defence for approval. The review *during* the interception, hacking, or recording of images takes place "*at any time through visits to the places where GISS conducts these interceptions, hacking, and recordings of still or moving images.*" The review *after* the operation takes place on the basis of monthly lists of countries, organisations,

23 For more information on the duties assigned to the Committee R/I in this regard, see Committee R/I, *2022 Activity Report*, p. 89.

or institutions that have actually been the subject of an interception, hacking, or video recording operation, as well as through the review of logs that are continuously updated at the place where the interception, hacking, or video recording takes place.

The Committee R/I received the three plans for the year 2025 in December 2024, after they had been approved by the Minister of Defence, as stipulated in the ISA.

In 2025, the Committee conducted a series of site visits and held several meetings with GISS, allowing it to gather additional information on how GISS performs this task.

The Committee also issued an opinion in 2025 on a draft royal decree laying down certain rules for exercising these powers.

COMPLAINTS

IDENTIFYING, UNDERSTANDING, AND ADDRESS SHORTCOMINGS

Pursuant to Article 34 ISA, the Committee R/I investigates complaints from citizens. These are divided into three categories:

- **complaints regarding operations**, conduct, actions, or omissions of the intelligence services, CUTA and its support services and their staff.
- **complaints regarding the use of special intelligence methods** (SIM) by State Security or GISS;
- **individual requests relating to the processing of personal data** by the above-mentioned persons and services, their staff members and their processors. In such cases, the Committee R/I 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 (so-called DPA[24] complaints).

1. OVERVIEW IN FIGURES

In 2025, the Committee R/I received a total of **63 complaints.**

The columns in the table below categorise the complaints based on whether the Committee R/I has exclusive competence or shares competence with the Committee P or the Supervisory Body for Police Information (COC).[25]

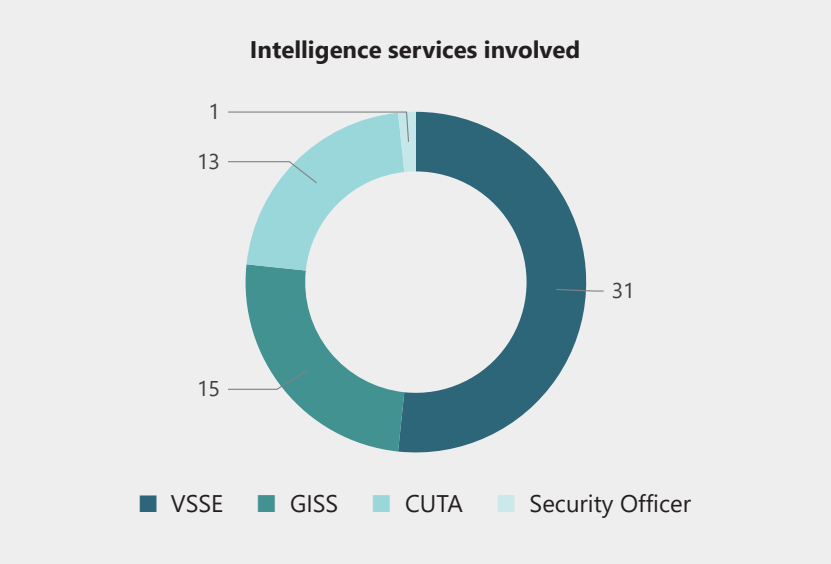
2025	COMMITTEE R/I	COMMITTEE R/I and COMMITTEE P	COMMITTEE R/I and COC	TOTAL
Complaints submitted	58	3	2	63
Inadmissible complaints	20	1	0	21
Admissible complaints	38	2	2	42
Pending cases	0	0	0	0
Ongoing cases	3	0	0	3
Admissible closed cases	35	2	2	39
Corrective measures	4	1	0	5

24 DPA stands for Data Protection Authority.

25 Please note that the same complaint can be the subject of several 'cases', depending on the services involved: for example, a complaint against CUTA as well as State Security is included both in the cases handled jointly by the Committees R/I and P with respect to CUTA and in the cases handled exclusively by the Committee R/I with respect to investigative acts relating to State Security.

61 cases were closed in 2025. Only a limited number of complaints were still pending at the start of 2026. Following a brief preliminary investigation and verification of a number of objective data, the Committee R/I rejected 21 complaints and reports as either clearly inadmissible or because the Committee R/I did not have jurisdiction for the matter. Compared to previous years, **a slight rise in the number of admissible complaints submitted to the Committee R/I** was observed.

To be admissible, the complaint or report must relate to at least one of the intelligence services subject to review (State Security, GISS, or CUTA). If the complaints concern police actions or the functioning of the judiciary, the complainants are referred, if possible, to the appropriate bodies (e.g., the Supreme Judicial Council, the Public Prosecutor's Office, the COC, or the Committee P). If the reports contain only information that might be of interest to the intelligence services, the information is forwarded to them. The Committee is not competent to investigate complaints regarding the operations of foreign intelligence services on Belgian territory. Complaints regarding the operations and/or decisions of the Local Task Forces (LTFs) and the Local Integrated Security Units on Radicalism, Extremism, and Terrorism (LIVC-Rs) are inadmissible, unless they concern the contributions of the intelligence and security services in these forums. Furthermore, a complaint is admissible only if the complainant or person filing the report provides proof of identity within 30 days. Anonymous complaints will not be handled, but the complainant's identity may be kept confidential if requested (except in the case of DPA complaints, where the identity is crucial to conduct the investigation).



From the overview of intelligence services involved in the complaints submitted in 2025, State Security appears to be significantly represented.

2. NATURE OF THE ADMISSIBLE COMPLAINTS

Of the 42 admissible complaints, 24 concerned dysfunctions within the service(s), and 18 requests relating to the processing of personal data (DPA complaints) were handled. No complaints were lodged regarding the use of special intelligence methods in 2025.

2025	COMMITTEE R/I	COMMITTEE R/I and COMMITTEE P	COMMITTEE R/I and COC	TOTAL
Complaints about dysfunctions	23	1	0	24
SIM Complaints	0	0	0	0
DPA Complaints	15	1	2	18

2.1. Complaints about dysfunctions within the services

24 complaints concerned the functioning, conduct, actions or omissions of the intelligence services, CUTA and its support services, and their staff. **Only three of these were deemed valid.**

In these three cases, the intelligence services took **concrete measures to address the underlying operational problem**. Two of these cases involved appeals lodged with the Appeal Body against a failed security clearance, in which the decision was not reversed. Another case involved a candidate who had been ranked at the top of the list for a position with an intelligence service but, due to an administrative error, was never invited to take up the position.

The 21 remaining unfounded complaints were highly diverse. It was found that certain cases involved underlying civil, disciplinary, or criminal remedies that fell outside the Committee's competence. In two cases in which the complainants were named as suspects in a criminal case, they claimed—wrongly—that they had worked for years as "informants" for an intelligence service and, in that capacity, were entitled to a form of criminal immunity. Many people believed they were the subject of ongoing surveillance by the intelligence services, either by alleged physical agents in their environment (surveillance) or through cognitive manipulation. Following an investigation, none of these complaints were declared well-founded.

2.2. DPA complaints

18 of the 42 admissible complaints lodged in 2025 were treated as DPA complaints. 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 Committee R/I, among others, for a review of the processing of their personal data. The way in which this data is and was shared with foreign partners is a permanent focus point for the Committee, which is seised by applicants who encounter problems with border controls. It is not uncommon for these cases to involve individuals who were previously linked with terrorism, extremism, or radicalism, but regarding whom no current information is

circulating and who are no longer being monitored. Due to the global proliferation of watchlists following the terrorist attacks, it appears that certain individuals remain on foreign watchlists and encounter difficulties as a result. However, the Committee has no jurisdiction over foreign intelligence services and can only request that State Security and GISS notify their foreign partners accordingly. In other words, it depends on the goodwill of these services, bearing in mind that cooperation with them is sometimes limited or non-existent.

In 2025, the Committee R/I handled a **DPA complaint for the first time against a security officer from an independent federal supervisory authority** who had no connection to the intelligence and security services. However, due to a recent change in the law, the Committee R/I now has residual jurisdiction over all DPA complaints against security officers, both in the public and private sectors.

As the review body, the Committee imposed **corrective measures in two cases** (art. 51/3 Review Act). The Committee R/I cannot, however, take the place of the relevant services in the sense that it can conduct its own intelligence analysis, but it can issue binding decisions in cases of unlawful personal data processing. Depending on the case, this may involve requesting rectification or deletion of personal data, communicating the Committee R/I's decision to partners and/or authorities, or disseminating the decision within the service concerned.

OPINIONS

A COHERENT SET OF LEGAL POSITIONS

The Committee R/I can only issue an opinion at the request of the Chamber of Representatives or the competent minister on a draft law, royal decree, circular or any other document setting out the policies of the competent ministers (Art. 33 Review Act). In addition, the Committee must also issue an opinion in its capacity as the Competent Supervisory Authority (CSA) with regard to the processing of personal data (Articles 73 and 95 of the Data Protection Act). Its opinions are sometimes formulated based on a dual capacity.

In 2025, **the Committee was asked for its opinion** four times: twice by the Minister of the Interior, once by the Minister of Defence, and once by the Chamber of Representatives. The average time it takes to issue an opinion is approximately two months.

The following is a summary of the opinions issued, briefly outlining the main arguments presented. To gain a comprehensive understanding of their scope and coherence, it is recommanded that the full opinions be consulted.[26]

1. CONSULTATION ORGANISED PURSUANT TO ARTICLE 458*TER* OF THE PENAL CODE

Article 458*ter* of the Penal Code states the following (freely translated):

> "§ 1. No offence is committed when a person who, by virtue of their position or profession, is entrusted with secrets, discloses them in the context of a consultation organised either by or pursuant to a law, decree, or ordinance, or by reasoned authorisation from the public prosecutor. Such consultations may be organised solely either for the purpose of protecting the physical and psychological integrity of the individual or of third parties, or to prevent the offences referred to in Title Iter of Book II or offences committed in the context of a criminal organisation, as provided for in Article 324*bis*. The law, decree, or ordinance referred to in the first paragraph, or the reasoned authorisation from the public prosecutor must at least specify who can participate in the consultation, the purpose of the consultation, and the procedures under which it will take place.

26 All opinions can be found on the Committee's website (www.comiteri.be).

§ 2. Participants are obliged to maintain confidentiality regarding any confidential information disclosed during the meeting. Individuals who violate this confidentiality shall be punished in accordance with the penalties of Article 458. The confidential information disclosed during these consultations may only give rise to criminal prosecution for the offences for which the consultations were organised."

This provision, introduced by the Act of 6 July 2017[27]— makes it possible to disclose (protected) information in the context of confidential consultations with the police services or at the request of the public prosecutor, if the purpose is to protect the physical or mental integrity of a person or third parties, or to protect public security. This provision applies in particular to consultations that take place in the context of the Local Integrated Security Cells on Radicalism (LISC-R). Since personal data is processed in the context of these consultations, a specific legal basis was necessary to establish a framework for these processing activities.

On 12 November 2024, a **draft law** concerning the processing of personal data in connection with participation in a consultation organised pursuant to Article 458*ter* of the Penal Code was introduced in the Chamber of Representatives. Through the Data Protection Authority (DPA), the Committee was requested to issue an opinion on the text of the draft law.

In its opinion, issued on **25 February 2025**, the Committee noted that the proposal was not clear as regards exactly which public authorities were referred to. As there was no provision that formally designated the public authorities referred to in Title 3 of the Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Personal Data Act)[28], the Committee R/I ruled that the text did not apply to the public authorities for which it is the competent supervisory authority for data protection and that, consequently, it was not competent to issue an opinion. However, it added that, assuming the parties who drafted the text intended to designate certain public authorities under Title 3 of the Data Protection Act, the provisions of the draft law would have to be explicitly supplemented to that effect, and that the essential elements of the processing operations would have to be regulated. As there were no such provisions, and given the lack of the relevant elements, the draft law compromised the principle of legality.

On 18 June 2025, the authors submitted a new version to the Chamber, which clarified a number of points.[29] The draft law was approved during the plenary session on 8 January 2026.

27 Act of 6 July 2017, on the simplification, harmonisation, digitisation, and modernisation of provisions of civil law and civil procedure, as well as of the notarial profession, and containing various judicial provisions, Belgian Official Journal, 24 July 2017.

28 Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data Belgian Official Journal, 5 September 2018.

29 Draft law concerning the processing of personal data in connection with participation in a consultation organised pursuant to Article 458*ter* of the Penal Code, *Parl. St.*, Chamber of Representatives, 2024–2025, Doc. 56 0935/001, 18 June 2025.

2. INTERCEPTION OF COMMUNICATIONS ABROAD BY GISS

GISS may detect, intercept, eavesdrop on, monitor, and record any form of communication sent or received abroad. Articles 44 to 44/5 of the Intelligence Services Act (ISA) contain the specific provisions governing how these powers are exercised, as well as the procedures regarding the reviews carried out by the Committee R/I in this regard.

On 28 July 2025, the **Minister of Defence** requested the Committee to issue an opinion on a draft royal decree (RD) laying down the rules for destroying illegally collected information as referred to in Article 44/4 ISA and establishing the rules regarding cooperation as referred to in Article 44/5 ISA.

The purpose of the draft royal decree submitted for an opinion, as its title indicates, was to further specify certain procedures for implementation and reviews, namely:

- the rules governing the destruction of unlawfully collected data in this type of interception (Article 44/4 ISA) ;
- the rules that apply in cases where the cooperation of a network operator or service provider is required to make an interception possible (Article 44/5 ISA). The aim of the draft RD was to provide a framework for the flows of data and metadata that are intercepted, through restrictions and safeguards.

In its opinion of **11 September 2025**, the Committee made a number of remarks, in particular regarding the destruction of illegally collected data. In this regard, it welcomed the central role given to the data protection officer (DPO) in the procedure for destroying data and invited the legislator to assign the DPO a similar role in the procedure for destroying data unlawfully collected using a special intelligence method. To ensure that the Committee could fully exercise its review remit, it called for an additional provision to oblige GISS to submit any official report documenting the destruction of illegally collected information within two weeks. With regard to the rules governing interceptions that require the cooperation of service providers or network operators, the Committee requested that certain terms be better defined (e.g. ''automatic transmission of data streams and metadata' and 'operations manager'), and that certain procedural periods be specified. Furthermore, the Committee pointed out that any system or equipment used by an intelligence service for the automated processing of personal data must meet the technical requirement of explainability.[30]

30 Gathering information through an automated flow of (meta)data requires that it is possible to explain, both upstream and downstream, how the system arrived at a specific result.

3. ADMINISTRATIVE BAN ON RADICAL ORGANISATIONS

In a letter dated 31 July 2025, the Committee R/I received a request from the **Minister of the Interior** to issue an opinion on a preliminary draft law concerning the administrative ban on legal entities, unincorporated associations, societies, or de facto groups that pose a serious and current threat to national security or the continuation of the democratic and constitutional order.

The purpose of the preliminary draft law was to establish a mechanism for imposing an administrative ban on organisations which, through their specific, coordinated, and persistent activities, pose a serious and immediate threat to national security or to the foundations of the rule of law. The draft law provided that such a ban could take two forms: the administrative dissolution of the organisation or a ban on its activities.

In its opinion of **9 October 2025** , the Committee R/I limited itself to discussing aspects related to the activities and obligations of the intelligence services.[31]

As regards the grounds that may lead to an administrative ban, the Committee noted in particular that the draft law was limited to three threats to national security, i.e., terrorism, violent extremism, and violent radicalism, whereas the ISA lists several explicit threats to national security.[32] The Committee questioned the decision to limit the scope to these three threats and asked the author to provide further details on the reasons for this decision. The Committee also invited the author to further clarify the meaning of these three terms, which are not defined in the draft law. It also highlighted the substantive difference between the concept of 'radicalism', on the one hand, and the concepts of 'radicalisation process' and 'radicalisation', on the other. The first is a state; the other two are a process.

Regarding the procedure, the Committee highlighted the central role assigned to the Coordination Committee on Intelligence and Security (CCIV), which was tasked with conducting an analysis that could serve as the basis for a potential administrative ban. The Committee had several questions regarding the assignment of this new formal task. More specifically, the question is to what extent the CCIV's existing operational rules will need to be amended to perform this new role, but also whether the CCIV has sufficient authority to properly perform the role and whether its legal framework needs to be amended. The Committee recommended that the draft law set out the rules regarding the quorum and the required majority for the body to adopt a formal decision when an analysis or report is issued in the context of the relevant procedure. The Committee also highlighted the fact that the draft law made no mention of the work prior to the analysis of the CCIV. Prior work refers to obtaining the necessary information from the relevant operational services (e.g. State Security or GISS) and the joint analysis of that information by the members of the CCIV, with the aim of preparing and approving an analysis. However, the Committee highlighted various issues that needed to be clarified

31 For a more general overview, see in particular the opinions of the Council of State (January 2026) and the Federal Institute for the Protection and Promotion of Human Rights (FIRM) (September 2025).

32 These include espionage, terrorism, extremism, proliferation, harmful sectarian organisations, criminal organisations, and interference (Article 8, 1°, paragraph 2 ISA).

in this regard, such as the identity of the service actually responsible for the analysis or the procedure to be followed if the CCIV believes that it does not have sufficient information to make a decision.

Finally, with regard to appeal possibilities, the draft law provided for judicial review by allowing appeals to be lodged with the Council of State against any administrative ban. In this regard, the Committee referred to the established case law of the European Court of Human Rights concerning the applicable requirements when public authorities use classified or secret information in an individual administrative decision: the Court recognises that, for reasons of national security, a person's access to their file may be restricted, but that a judge or other independent authority must have access to the entire file, including all classified or confidential documents, so that a judicial appeal procedure would satisfy the right to a fair trial (Art. 6 of the ECHR) as well as the right to an effective remedy (Art. 13 of the ECHR). The essential question which, in the Committee's view, could be addressed in the context of the jurisdictional appeal provided for in the draft law concerns the seised court's access to the classified documents on which the CCIV's opinion—and, consequently, the contested decision—is based. The Committee noted that the appeal procedure before the Council of State described in the draft law might not meet the requirements of the European Court in cases where the CCIV's analysis is based on classified information. If the CCIV's analysis is based on classified information originating from an intelligence service, and even if the latter has decided to provide the CCIV with an unclassified memorandum, the underlying file is still classified. The CCIV's decision will therefore be based on classified information to which the court responsible for issuing a judgment should be granted access in order to comply with the requirements of the European Court. The draft law does not include any such compensatory measures. To address this fundamental shortcoming, priority should be given to the option of entrusting this task to the Committee, in light of the prerogatives conferred upon it by law and its area of expertise.

In early 2026, the Minister of the Interior announced that the draft law would be revised based on the various opinions that had been issued.

4. PNR AND ETIAS LISTS

On 15 September 2025, the **Minister of the Interior** requested that the Committee issue an opinion on two draft royal decrees establishing, on the one hand, a framework for the purposes of processing passenger data (Passenger Name Record, PNR) and, on the other hand, a framework for consulting data from the *European Travel Information and Authorisation System* (ETIAS) for law enforcement purposes.

The purpose of the draft RDs was to draw up, in accordance with statutory provisions, lists of criminal offences under national law that correspond to the offences referred to by the European legislator. With regard to the PNR, this concerns terrorist offences and serious forms of crime as defined in Article 3, points 8 and 9, of the PNR Directive.[33] As for ETIAS data, this refers to terrorist offences and serious criminal offences as defined in Article 3, points 15 and 16, of the ETIAS Regulation.[34] The purpose of both lists was to provide the competent authorities and operational services with a framework to ensure compliance with the law enforcement purposes of data processing.

In its opinion of **18 November 2025**, the Committee R/I reiterated the general restriction established by the European legislator: in order for a criminal offence to be included in the PNR or ETIAS list, it must be punishable by a custodial sentence or a measure with a maximum penalty of at least three years. Furthermore, the Committee noted that the European legislator had imposed few (if any) substantive restrictions on the interpretation to be given to certain terms. Consequently, the Committee noted that the author had defined certain terms restrictively (specifically, the term 'participation in a criminal organisation') and that as a result, a number of criminal offences could be added to both lists. Moreover with regard to the definition of the term 'sabotage', the Committee noted that if the act of the perpetrator was intentional, this should be included.

33 Directive 2016/681 of the European Parliament and of the Council of 27 April 2016, on the use of passenger name record (PNR) data for the prevention, detection, investigation, and prosecution of terrorist offences and serious crime.

34 Regulation 2018/1240 of the European Parliament and of the Council of 12 September 2018 establishing a European Travel Information and Authorisation System.

THE INTEGRITY CELL

EXTERNAL REPORTING CHANNEL FOR INTEGRITY BREACHES

1. THE 'WHISTLEBLOWER ACT'

Misconduct or fraudulent practices within a professional context—so-called integrity breaches—can be reported. Whistleblowers play an important role by bringing to light fraud and irregularities identified within public institutions (or private companies). However, the fear of retaliation can deter whistleblowers from taking the step of reporting incidents. Whistleblowers therefore deserve appropriate recognition, support, and protection, as they may face significant professional and personal risks.[35]

A European directive[36] provides protection to individuals who report or disclose such violations of the law or suspected integrity breaches. This Directive was transposed into national law by the Act of 8 December 2022 on the reporting channels and the protection of persons notifying of integrity breaches in federal government agencies and the integrated police (Whistleblowers Act).[37] The law entered into force on 2 January 2023. Acting as a whistleblower has therefore become a right, and whistleblowers can rely on certain minimum standards designed to protect them if they fear that their whistleblowing could have adverse consequences for their (professional) situation.

The Act requires government agencies to set up a whistleblower reporting system at various levels: a whistleblower must have the option to report something internally, within their own organisation, or externally, or they may choose to publicly disclose the misconduct immediately.[38] These three levels are not hierarchical; the level chosen by the whistleblower is not subject to the principle of subsidiarity. The whistleblower is free to choose at his or her own discretion.

The protection and support provided apply to the various whistleblowing methods and involve a range of measures.[39] In addition, retaliatory measures are prohibited, and whistleblowers can count on receiving information and advice (both technical and legal), psychological support, and legal assistance. The Act outlines a procedure that describes the process for internal or external whistleblowing.

In connection with potential whistleblowing of integrity breaches within GISS or State Security, the Committee R/I was tasked with serving as an external whistleblower channel.[40]

35 Federal Institute for the Protection and Promotion of Human Rights (FIRM), *Guide for Whistleblowers*, December 2024, https://federaalinstituutmensenrechten.be/en/publications/guide-for-whistleblowers, accessed on 3 March 2026.

36 Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law, *Official Journal of the European Union*, 26 November 2019, L305/17.

37 Belgian Official Journal, 23 December 2022.

38 Art 7, §1, 2° Whistleblower Act.

39 Art 28 and 29 Whistleblower Act.

40 Art 14 §1, 3rd para. Whistleblower Act.

2. THE INTEGRITY CELL WITHIN THE COMMITTEE R/I

As external whistleblower channel for integrity breaches at GISS and State Security, the Committee R/I set up an Integrity Cell with a view to ensuring linguistic parity as well as equal representation of men and women. The cell consists of four employees from the Committee R/I: two members of the IInvestigation Service and two legal advisors.

Employees of GISS or State Security can now contact the Committee R/I to report an (alleged) integrity breach. The Integrity Cell will investigate these reports to determine whether they are admissible and well-founded, and what can or must be done to put an end to the breach or to prevent it from recurring in the future.

To this end, the Cell has a broad range of powers and investigative measures at its disposal: the relevant individuals may be invited to cooperate, relevant documents may be requested, and individuals may be interviewed... This remit as an external reporting channel not only entails extensive powers for investigating potential integrity breaches, but also a responsibility to protect the whistleblower and the individuals cooperating with the investigation from retaliation. [41] In late 2024 and early 2025, the members of the Integrity Cell underwent special training on how to handle and investigate reports.[42]

At the end of 2025, the Integrity Centre of the Federal Ombudsman took the initiative to set up an informal network that brings together the various external reporting channels in the public sector, in which members of the Integrity Cell also participate. It is an informal exchange platform intended to bring together experts from the relevant reporting channels to discuss common challenges and issues faced by their services. The first meeting took place in January 2026. The network should meet three to four times a year. Among other things, the network aims to strengthen ties between external reporting channels, share knowledge and best practices, enhance their visibility, and reaffirm their strategic role in protecting whistleblowers within the public sector.

41 Art 14 §1, 6° Whistleblower Act.

42 Art 14 §2 Whistleblower Act. The programme in question was the "*Masterclass in Fraud Auditing*" at the Institute of Fraud Auditors (IFA), a post-master's executive programme for professionals specialising in fraud prevention, investigation, and control. It aims to train individuals to become effective fraud auditors by inculcating in-depth knowledge and practical skills in fraud risk management, fraud prevention and investigation, interview techniques, cybercrime, analysing fraud scenarios, and best practices in the public and private sectors. Every member of the Integrity Cell successfully completed the programme in 2025.

3. SCOPE AND LIMITATIONS

3.1. An additional challenge: "national security"

As an external reporting channel for GISS and State Security, the Committee R/I investigates any reports of abuse, irregularities, and fraud within these two intelligence services. This poses an additional challenge: the specific operations of the intelligence services are geared toward "national security,"[43] and the Whistleblower Act specifically excludes the domain of national security from its scope. Indeed, Article 4 of this Act states (freely translated):

> *"§1. This Act does not apply to:*
> *1° classified information*
> *...*
> *§2. This Act does not apply to national security, except with respect to reports of violations of public procurement rules in the areas of defence and security as referred to in Article 3, §4, paragraph 1."*

GISS and State Security are responsible for "national security."[44] The explicit exclusion of the above-mentioned violations makes it difficult—in fact, *quasi* impossible—to apply the Whistleblower Act in the operations of the intelligence services and to fulfil its protective remit. The explanatory memorandum to the Whistleblower Act had already noted at the time, in connection with the exclusion of violations committed during work that falls under national security (freely translated):

> *"[...] A specific reporting system (internal and external) will be set up in a separate Act to address these violations. "This separate Act will include sufficient safeguards to ensure that the secrecy of the operations of the intelligence and security services remains guaranteed [...]".*[45]

43 In accordance with the explanatory memorandum, "national security" is defined here as "*all activities of intelligence and security services as referred to in Articles 7 and 11 of the Act of 30 November 1998 regulating the intelligence and security services.*"

44 Articles 7 and 11 ISA.

45 Draft law on the reporting channels and the protection of persons notifying of integrity breaches in federal government agencies and the integrated police, 3 November 2022, Explanatory Memorandum, p. 170.

In its opinion[46] on the draft law for the Whistleblower Act in the public sector, the Committee R/I warned of a distinction that would be difficult to apply:

> *"[…] With regard to integrity breaches involving intelligence services, the Committee is nevertheless of the opinion that in practice it will be impossible to draw a clear distinction between integrity breaches committed outside the scope of the remit of these services and integrity breaches committed within it […]"*

By early 2026, it must be confirmed that there is still no fully-fledged alternative for the protection of whistleblowers who report integrity breaches in the domains excluded under Article 4 of the Whistleblower Act. A draft law is being prepared to amend the whistleblower status with regard to the integrity breaches that were excluded from the original Act.

3.2. Reports still possible nonetheless…

However, the fact there is no protection status for whistleblowers reporting integrity breaches committed in the context of national security does not mean that these reports cannot be made.

Indeed, the Committee R/I has various options for conducting an investigation, albeit outside the scope of the Whistleblower Act. Without a specific Act, there is currently a lack of additional protection that offers that extra incentive in such situations and could encourage people to actually report a situation.

In practice, the exclusions set out in Article 4 of the Whistleblower Act mean that it is currently very difficult for the Committee to fully play its role as an external reporting channel. As soon as a breach committed within GISS or State Security is reported, it affects services whose very raison d'être is to carry out missions related to national security. The Committee R/I therefore emphasises the importance of a supplementary legislative framework so that whistleblowers who report integrity breaches within GISS or State Security can also enjoy the same right to protection and support as intended by the directive (see below), without infringing upon other interests that, due to their specific nature, must not be overlooked.

46 Committee R/I, Opinion No. 005/VCI/2022 of 30 August 2022, on the draft law for the Whistleblower Act in the Public Sector (the current Whistleblower Act)(www.comiteri.be).

3.3. Protection and support measures

When a whistleblower's report is deemed admissible, he or she can count on the protective measures provided for by the Act.[47] In the first instance, this is protection against retaliatory measures. If an individual believes they have been the victim of such a measure, they can file a complaint with the appropriate external reporting channel.

Retaliatory measures can take a wide variety of forms: suspension, demotion, negative performance evaluations, discrimination, coercion, intimidation... The burden of proof that the measure in question is not retaliation for the report lies with the relevant government agency. Individuals who assist the whistleblower and/or have cooperated with the investigation can also count on the envisaged protection and support measures, which include information and advice, legal assistance, psychological support, media-related support, and social support, etc.

Reporting an integrity breach is not an individual complaint
An individual who reports an integrity breach takes a fundamentally different position than someone who files a complaint about the actions of an employee of the intelligence services. Whereas a complaint implies that the complainant suffers personal harm as a result of the employee's 'wrongful' conduct, this does not, in principle, apply to whistleblowers who report integrity breaches. Consequently, a situation can be reported and an investigation can be started without the need for repeated exchanges with the person who reported the situation.

3.4. One integrity breach reported

Situations reported to the Committee R/I in 2025 in the context of its role as an external reporting channel were evaluated in accordance with current legislation. This means that the only reports that may be admissible are those related to the activities of the intelligence services not related to national security.[48] In 2025, one case was opened and deemed admissible in connection with a report of an integrity breach. This investigation was still ongoing in 2026.

Are you an employee of GISS or State Security and would like to report an integrity breach? You can report a breach by email (signalement_melding@comiteri.be), by phone (02/286.29.11—ask for the Integrity Cell), or by appointment. You can also submit a report in writing (Committee R/I, Integrity Cell, Leuvenseweg 48, P.O. Box 5, 1000 Brussels).

47 Articles 28 and 29 Whistleblower Act.

48 Breaches committed in the context of national security missions are not admissible (under the protection status of the Whistleblower Act).

THE APPEAL BODY FOR SECURITY CLEARANCES AND SECURITY ADVICE

AN EXCEPTIONALLY HIGH CASELOAD

The Appeal Body is an administrative jurisdictional body with jurisdiction over disputes relating to security clearances and advice. It is a collegial body made up of the (deputy) chairs of the Committee R/I, the Committee P, and the Litigation Chamber of the Data Protection Authority.

The Appeal Body either issues decisions when it receives an appeal relating to security clearances, or provides opinions when it receives an appeal relating to security advice. For the sake of convenience, the term "decisions of the Appeal Body" is used in the following to refer to both the decisions and the advice issued by the Appeal Body.

The Committee R/I chairs and acts as registrar for the Appeal Body. It provides the necessary staff and resources for the operations of the Appeal Body, in particular for updating the registry, organising hearings, drafting official reports, and preparing decisions.

1. GENERAL TRENDS

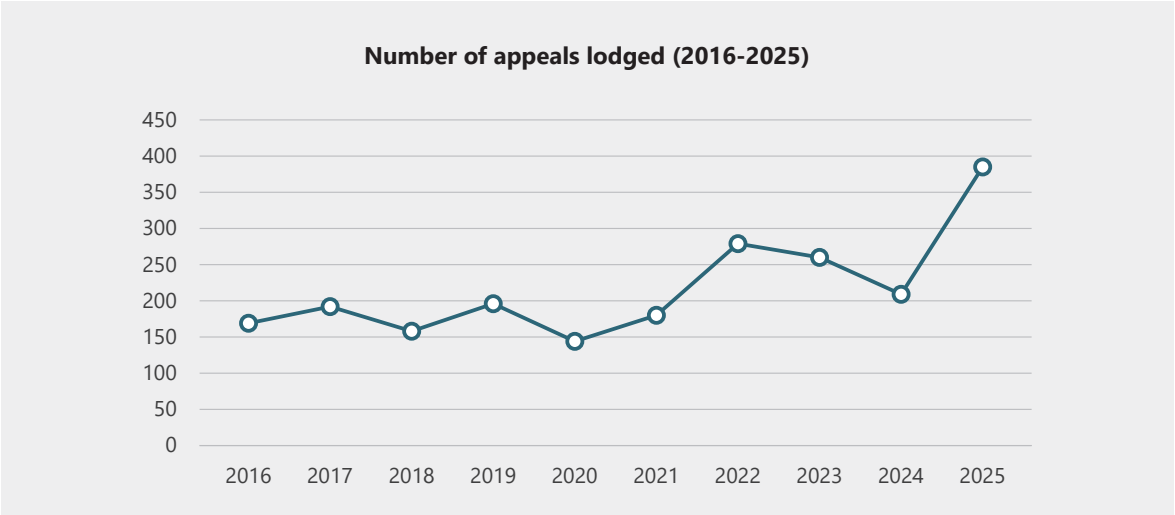
The year 2025 was marked by the large number of appeals lodged with and reviewed by the Appeal Body. The following sections provide an overview of the Appeal Body's activities. They provide a detailed overview of the number of appeals lodged, broken down by the nature of the contested decisions and the language of the proceedings, as well as the number and type of decisions issued by the Appeal Body and the lead times observed.

The figures presented reflect only the disputes handled by the Appeal Body. They do not reflect the total number of decisions or unfavourable opinions issued by the security and verification authorities[49] [50], only a portion of which are subject to appeal. Consequently, the observed trends should not be interpreted as a direct indicator of changes in the activities of the authorities in question. For a complete overview of the number of security clearances and advice granted over the past year, please refer to the activity reports of the various competent authorities.

49 There are three security agencies: the National Security Authority, State Security, and the General Intelligence and Security Service.

50 The term 'verification authority' refers to the government agency that issues security advice. These agencies include, in particular, the Federal Police, GISS, etc.

1.1. Sharp rise in the number of appeals lodged



	2020	2021	2022	2023	2024	2025
NSA	91	86	183	188	77	97
VSSE	0	4	2	0	1	3
GISS	41	84	76	56	65	88
FANC	7	6	12	11	10	14
Federal Police	4	0	1	4	56	182
Local Police	1	0	5	1	0	1
TOTAL	**144**	**180**	**279**	**260**	**209**	**385**

In 2025, the number of appeals lodged rose sharply, from 209 in 2024 to 385 in 2025, representing a rise of 84%. This increase was primarily appeals against security advices, although appeals regarding security clearances also rose significantly (see below).

This trend is also characterised by a rise in the number of cases lodged according to the language of the proceedings. The increase is biggest for appeals lodged in Dutch, i.e., from 76 appeals in 2024 to 195 appeals in 2025, a rise of 156% (see below). The number of appeals lodged in French continues to rise steadily, from 133 in 2024 to 190 in 2025, an increase of 43%.

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
French	99	115	83	101	83	86	201	159	133	190
Dutch	70	77	75	95	61	94	123	101	76	195
German	0	0	0	0	0	0	0	0	0	0

1.2. Breakdown of cases by nature of the contested decisions

	2016	2017	2018	2019	2020	2021	2022	2023	2024	2025
Clearances	50	40	36	51	32	60	83	105	102	145
Advice	101	122	92	115	99	108	157	134	85	234
Certificates	18	30	30	30	13	12	39	21	22	6
TOTAL	**169**	**192**	**158**	**196**	**144**	**180**	**279**	**260**	**209**	**385**

1.2.1. Security clearances

In 2025, the number of appeals lodged in connection with security clearances rose sharply, from 102 cases in 2024 to 145, a rise of 42%. The Appeal Body does not have the necessary elements to determine the cause of the rise in the number of appeals. It is noteworthy that 23% of these appeals (33 out of 145) were lodged because the security authority failed to issue a decision within the legal time limit (or failed to notify the applicant of its decision).

1.2.2. Security advice

The most striking change occurred in security advice, with 234 cases in 2025 compared to 85 in 2024—an increase of 175%. This increase is primarily related to appeals lodged against a negative security advice for performing a job in a port area, considering security screenings are since 2024 required for access to ports. Given the geopolitical situation, it is also likely that the screening process will become more stringent, which in turn could lead to an increase in negative security advice and, consequently, in the number of appeals lodged.

Furthermore, the abolition of security certificates (see below) also contributed to the change in the security advice issued; indeed, an advice is now required for positions and sectors that previously required only a certificate.

1.2.3. Security certificates

Given that the system for security certificates has been abolished (see below), no certificates have been issued since 1 February 2025. Unsurprisingly, this reform has led to a decrease in the number of appeals in this area. Nevertheless, the Appeal Body still handled six cases in 2025 involving refusals of security clearances that had been issued on prior to the abolition of this system.

1.3. Decisions of the Appeal Body

1.3.1. Volume and nature of the decisions

The increase in the number of appeals lodged in 2025 led to an increase in the number of decisions issued by the Appeal Body. It should be noted that some of these decisions relate to cases lodged in 2024, and that some of the appeals lodged in 2025 will only be processed in 2026. The total number of decisions issued by the Appeal Body rose from 261 in 2024 to 357 in 2025, an increase of 37%.

These decisions pertained to:
- 164 security clearances (46% of the total);
- 177 cases of security advice (49.5%);
- 16 security certificates (4.5%).

1.3.2. Overturned decisions and withdrawals

Of all the appeals processed in 2025, the Appeal Body overturned[51] 47 out of 164 (or 28.7%) decisions regarding security clearances, six decisions regarding security certificates out of 16 (or 37.5%), and 62 security advice out of 177 (or 35%). This result bears witness to the effectiveness of the Appeal Body's review process, which conducts in-depth investigations which, in a significant number of cases, lead to the contested decisions being overturned.

Furthermore, it should be noted that a significant proportion of the decisions result in a deed of withdrawal from the appeal: 12.3% of all decisions and advice issued (44 out of 357) and 17.7% of the decisions issued regarding security clearances (29 out of 164). A withdrawal means that the applicant wishes to terminate the proceedings. This usually happens when an appeal has been lodged because a decision has not been issued within the statutory period, and the security or verification authority ultimately issues a decision while the proceedings are still ongoing.

1.3.3. Processing time

In 2025, it took an average of 125.9 days to process cases, or just over 4 months from the time the appeal was lodged. This result shows that the Appeal Body was able to handle a larger number of cases compared to the previous year. This was made possible in particular by the recent expansion of the staff of the Registry (see below), which meant that the growing number of appeals could be processed more efficiently, while maintaining the quality of the decisions and advice issued.

Since mid-2025, the Appeal Body has convened on a weekly basis. However, given the wide range of responsibilities of the Committee and the bodies that together make up the Appeal Body, it is difficult to organise more than one session per week.

51 'Overturning a decision' means that the Appeal Body replaces the initial decision with a new one.

It should also be noted that the processing time does not depend solely on the Appeal Body. This timeframe is also influenced by the (long) periods within which the security and verification authorities forward the applicants' administrative files; this point is explained in more detail below.

1.4. Administrative files delays

The Appeal Body regularly encounters delays in the provision of administrative files by the verification and security authorities. These timeframes have a direct impact on the duration of the appeals process, since the Appeal Body can only render a correct decision if it has the (complete) administrative file at its disposal.

In 2025, the timeframes for providing the administrative files were as follows:

a. As regards security advice:
   - 48 files received within the legal timeframe of 10 days;
   - 71 files received within 11 to 20 days;
   - 37 files received within 21 to 30 days;
   - 77 files were received within a timeframe of more than 30 days, 19 of which were received within a timeframe of more than 100 days.

In total, more than 75% of the administrative files related to security advice were received after the legal timeframe of 10 days.

b. As regards security clearances:
   - 25 files received within the legal timeframe of 15 days;
   - 48 files received within 16 to 30 days;
   - 52 files received within 31 to 99 days;
   - 17 files received within a timeframe of more than 100 days.

In total, more than 80% of the administrative files related to security clearances were received after the legal timeframe of 15 days. These delays add to the time the Appeal Body needs to process appeals.

2. EVOLUTION OF THE LEGAL FRAMEWORK AND CASE LAW

2.1. New legislation

The Act of 2 June 2024 amending the Act of 11 December 1998 on classification, security clearances, security certificates, security advice and public regulated service entered into force on 1 February 2025. This entailed several significant changes.

2.1.1. Abolition of security certificates

Whereas there were initially three types of screening results (security clearances, security certificates, and security advice), the above-mentioned Act abolished security certificates. As of 1 February 2025, security advice is mandatory for the positions and sectors for which a security clearance was previously required.

2.1.2. Changes regarding security advice

Among the amendments introduced by the above-mentioned Act, Article 36 of the Act of 11 December 1998 ('the Classification Act') introduces two new types of positive security advice: the positive security advice with an individual warning and the positive security advice with an administrative warning.

A positive security advice with an individual warning means that the authority does not have sufficient grounds to issue negative advice, but warns the applicant of the need to improve their conduct with regard to the points raised.

Positive security advice with an administrative warning is issued if the applicant was not residing in Belgium during the five-year period covered by the security verification and the authority does not have sufficient information regarding the individual in question.

Moreover, since 1 February 2025, it has also been possible to lodge an appeal if the verification authority has not issued security advice within the legal timeframe.

2.2. Preliminary question to the Constitutional Court

In 2024, the Appeal Body referred a preliminary question to the Constitutional Court to determine whether Articles 17 and 18 of the Judicial Code, which concern the requirement of an existing and immediate interest in lodging an appeal, are compatible with Articles 10 and 11 of the Constitution. This question specifically concerned the admissibility of an appeal to the Appeal Body in the event of a refusal to grant a security clearance if the applicant had not first challenged the termination of his contract before the competent court.

In this case, the National Security Authority (NSA) had refused to renew the security clearance of the applicant, a NATO employee, and his employment contract was terminated as a result.

In its Judgment No. 36/2025 of 27 February 2025, the Court held that the requirement of an immediate interest, i.e. the fact that the applicant must demonstrate that he or she has lost his or her job, disproportionately infringed upon the right of access to a court. This requirement also undermined the effectiveness of the specific appeal procedure envisaged for decisions on security clearances. The Court therefore upheld an interpretation of the law that allows an appeal to be lodged with the Appeal

Body as of the date of the refusal or revocation of a security clearance or, if there is no decision within the stipulated time limit, without any additional conditions. The ruling therefore upholds a broad interpretation of the right to appeal by rejecting any excessive requirement regarding the interest in starting proceedings, in order to ensure the effectiveness of the appeal.

2.3. Admissibility of the appeal and jurisdiction of the Council of State versus the Appeal Body

The question of the jurisdiction of the Appeal Body arose in connection with a case on which the Administrative Litigation Section of the Council of State ruled in its judgment in early September 2025.[52] In this case, the applicant—a contract employee of the European Commission who had been recruited to work at a post abroad—had applied for "EU SECRET" security clearance, which is required to perform this position.

The National Security Authority (NSA) stated that it "could not approve this request" because it believed that the security review could not be conducted, and it was therefore unable to gather sufficient information to assess whether the applicant provided the required guarantees. More specifically, the NSA referred to the fact that the applicant had held positions abroad for almost the entire investigation period and had not lived in Belgium for many years. The notification stated that, in the event of a dispute, the applicant could file a petition with the Council of State to have this decision annulled.

The applicant's lawyer questioned the jurisdiction of the Council of State and, as a precaution, lodged an appeal with both bodies. She argued that it was indeed a decision to grant a security clearance.

The Council of State upheld this analysis and ruled that, by stating that it could not "approve" the request for security clearance, the NSA had implicitly but unequivocally refused to grant that clearance. However, Article 4, §1, of the Appeal Body Act expressly grants the Appeal Body the authority to review decisions refusing clearances. The Council of State therefore ruled that it could not overturn or suspend such a decision. The Council of State also clarified that the reasons cited by the NSA—namely, the individual's long-term stay abroad and the fact they did not have a place of residence in Belgium—did not change this conclusion. Since it involved a refusal, the Appeal Body was competent, regardless of the reasons cited.

52 Judgment No. 264.054 of 3 September 2025.

2.4. Impossible investigation

The NSA cited "impossible investigation" in other similar cases. Indeed, several cases were brought before the Appeal Body in which the NSA ruled that it was impossible to conduct a security review because the applicant lived abroad. As explained above, the NSA contested the Appeal Body's jurisdiction on the grounds that the contested act did not constitute a "refusal to grant clearance," but rather the simple finding that it was impossible to conduct an investigation.

Following the above-mentioned ruling by the Council of State, the Appeal Body declared itself competent to hear these various cases. It held that the NSA could not systematically invoke the impossibility of conducting an investigation whenever the applicant had a career abroad, given that the position in question required the individual to live abroad.

In these cases, the Appeal Body pointed out that the intelligence and security services have broad powers to take various steps in the context of a security review, including outside Belgian territory.[53] It also argued that a security authority must make reasonable efforts to conduct its investigation. For example, the Appeal Body believes that it is possible to take the applicant's professional evaluations into account, arrange an interview with him or her, take into account their ties to Belgium, contact the regional security officer, or even consider mitigating measures. In light of the above, the Appeal Body concluded that it was possible to initiate an investigation into these various cases.

2.5. Screening as a covert human resources measure

The Appeal Body has confirmed that screenings are regularly concluded with negative results for reasons that are not in accordance with the legal provisions. The cases reviewed show that security clearances are sometimes denied or negative security advice is issued on grounds that do not pose a threat to the democratic rule of law or national security. This is an erroneous application of the applicable legal provisions.

Security clearance is required only if the individual needs access to classified information. The person in question must therefore provide sufficient assurances regarding integrity, loyalty, and discretion. Security clearance may be denied only if there is concrete evidence that the individual in question poses a risk to national security. The Appeal Body must verify whether the security authority's decision meets the legal criteria.

53 See Articles 18 and 19 of the Act of 11 December 1998 on classification, security clearances, security advice and public regulated service.

2.6. Screening based on a regulatory decision

Despite a significant increase in security screenings, the Appeal Body must remain vigilant to ensure that these screenings are always conducted in accordance with the regulations. For example, a screening was conducted on participants in an information session on "working for the local police," which took place at a local police zone. The Appeal Body first ascertained which regulatory decision formed the basis for the verification. However, in this situation, the screening was required only for individuals who would be temporarily performing a duty or function within the infrastructure of the local Police. The Appeal Body ruled that attending an information session does not in any way fall under the category of "performing a function or assignment." Consequently, the person in question was wrongfully denied the opportunity to attend the information session; moreover, all participants in the information session were *de facto* wrongfully screened.

It goes without saying that, especially given the rising number of screenings, there must be a permanent focus on ensuring that these are conducted in accordance with the law. It is crucial to ascertain whether security screening is necessary in certain cases and whether the screening actually achieves its purpose.

2.7. Application of Article 5, § 3 of the Appeal Body Act

In accordance with the right to a defence, the applicant must be given the opportunity to know the reason or grounds for the denial of security clearance or negative security advice. There may be cases where certain information cannot or should not be disclosed due to the risk of infringing on other interests: personal information about third parties, the operations of intelligence and security services, the progress of a judicial investigation, or the protection of sources.

Pursuant to Article 5, §3 of the Appeal Body Act, the security authorities or verification authorities may request the Appeal Body not to allow the applicant or their lawyers to inspect certain information for the reasons stated above. At that point, a decision must be made to ensure that the applicant is at least given a genuine opportunity to defend him or herself and to seriously challenge a negative decision or advice. Specifically, this means that not all requests to place information under embargo are automatically granted.

3. APPEALS LODGED WITH OTHER COURTS

3.1. Appeal to the Council of State

In 2025, three appeals were lodged with the Court of Cassation against decisions of the Appeal Body. One case was declared inadmissible due to a lack of admissible grounds. The other two cases were still pending at the end of 2025. Finally, a 2024 case was dismissed by the Council of State in 2025. The reason given for dismissing the appeal was that no violation of the statutory provisions had

been identified. The applicant had argued that his right to a hearing had been violated, as had the obligation to state reasons. Both remedies were dismissed.

3.2. Petition to the European Court of Human Rights

A petition was also lodged with the European Court of Human Rights. It was an appeal against a negative security advice.

The applicant invoked Article 6 of the European Convention on Human Rights and claimed that the fact it was not possible to access decisive evidence submitted to the Appeal Body and the lack of a clear statement of reasons for the Appeal Body's decision constituted a violation of his right to a fair trial. He also invoked Article 8 of the Convention and argued that the negative security advice constituted an infringement of his right to privacy, in particular with regard to his professional life. The case had not yet been concluded by the end of 2025.

4. INTERNAL ORGANISATION AND FUNCTIONING OF THE REGISTRY

4.1. Internal organisation and staff

The increase in the number of appeals lodged in 2025 (see above) had a direct impact on the organisation of the hearings and the workload of the Appeal Body.

Since the spring of 2025, two sessions have been held each month for French-language cases, whereby 12 to 15 cases could be reviewed per session.

Since mid-2025, due to the significant rise in the number of cases lodged in Dutch, the same schedule of two monthly sessions was implemented for Dutch-language cases, with an equivalent number of cases reviewed.

The activities of the Appeal Body place a particularly heavy workload on the Committee R/I, even though this is only one of the many tasks entrusted to the Committee. To cope with the increase in the number of disputes and the growing volume of administrative tasks, two staff members were recruited in September and October 2025 to bolster the registry of the Appeal Body. Thanks to this reinforcement, reasonable processing times were ensured, despite the increase in activity relating to disputes. Processing these cases currently requires the equivalent of two legal experts (one French-speaking and one Dutch-speaking) and four full-time administrative staff members. The Committee's chairwoman and member devote about 20% of their working time to it.

4.2. Digitisation and modernisation of the procedure

In 2025, a comprehensive review was launched regarding the digitisation of the appeals process within the Appeal Body. The objective is to reduce the workload of the registry and make it easier for citizens to lodge an appeal.

This project includes a functional analysis of the various stages of the procedure, IT development, and a review of the rules governing the lodging and processing of appeals. This is a long-term process that will continue into 2026 due to the necessary in-depth technical and regulatory changes.

Ultimately, the aim is for applicants to be able to choose for an electronic procedure. This development should lead to a significant decrease in the amount of registered mail sent by the Appeal Body and should help reduce the associated costs (currently estimated at approximately €50 per case in the simplest cases). Digitisation would also ensure better traceability of exchanges, shorter deadlines for submitting documents, and a simplification of the registry's work.

(INTER)NATIONAL COOPERATION

SHARING KNOWLEDGE AND EXPERTISE

1. INTERNATIONAL EXCHANGES

In these times of ever-increasing international cooperation (including the exchange of information) among intelligence and security services, the Committee R/I is convinced of the need for more extensive international cooperation among review bodies. Whether this takes the form of bilateral meetings or in the context of broader, multilateral working groups, such cooperation makes it possible to identify best practices for reviewing intelligence services, find ways to strengthen these reviews, and subsequently adapt to current challenges.

In 2025, artificial intelligence, the acquisition of bulk data, and Convention 108+[54] were the main topics at the international forums in which the Committee R/I participated.

Meeting with the Review Committee on the Intelligence and Security Services, 2 April 2025, Brussels

A delegation from the Dutch Review Committee on the Intelligence and Security Services (CTIVD) visited the Committee R/I in April 2025. This meeting provided an opportunity to exchange views on the specific characteristics of each review body as well as on the common challenges that need to be addressed. The fight against organised crime and the acquisition of bulk data, among other topics, were the focus of the discussions. This visit laid the foundation for enhanced bilateral cooperation between the two review committees.

European Intelligence Oversight Network, 20 May 2025, Brussels

In 2025, the European Intelligence Oversight Network (EION)[55] workshop focused on the use of data obtained from commercial sources by intelligence and security services. The discussions were an opportunity to take stock of the current regulations as well as the day-to-day oversight of the activities of the intelligence services. Convention 108+ and the opportunities it offers for enhanced international cooperation among oversight bodies were also discussed.

54 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

55 The EION brings together representatives from the oversight bodies of Belgium, Canada, Denmark, Germany, France, Lithuania, the Netherlands, Norway, Serbia, the United Kingdom, the United States, Sweden, and Switzerland.

Intelligence Oversight Working Group, 21-23 May 2025, Copenhagen

A technical meeting of the *Intelligence Oversight Working Group* (IOWG)[56] took place in Copenhagen in late May 2025. Following the customary round of questions about recent developments at each of the national oversight bodies, the participants discussed oversight of the use of artificial intelligence by intelligence services and the management of databases. The technical meeting was followed by a staff meeting, where the IOWG members discussed the challenges they face during their reviews. For example, the discussion focused on human resources management, the sometimes lengthy timeframes for conducting investigations, the communication strategy, and access to the intelligence services.

Intelligence Oversight Working Group, 4-5 November 2025, Zurich

The IOWG members met again in Zurich at the end of 2025. The discussions at this meeting focused primarily on the use of cryptocurrencies by intelligence services, the knowledge and expertise management within oversight bodies, and training for their staff. The technical and staff meetings were followed by a Chair meeting, during which the Canadian oversight body, namely the National Security and Intelligence Review Agency (NSIRA), which had previously been participating as observer, was officially admitted as a full member of the IOWG. Following the conclusions reached at the events in May and November 2025, two working groups were set up: the AI Oversight working group monitors the use (and oversight) of artificial intelligence in the context of national security, while the Oversight Gap working group explores possible solutions for international cooperation among oversight bodies.

Seminar: "'National Security' and the Politics of Security Screenings in a Globalized World," 5 November 2025, Oslo

In November 2025, the Committee R/I was invited to share its expertise in the context of a seminar dedicated to the issue of security screenings, organised by Oslo Metropolitan University (Oslomet). Among other things, the discussion focused on the challenges of security investigations conducted at the national level in a globalised world, as well as the analysis methodology used by the intelligence services to assess individual threats.

European Intelligence Oversight Conference, 5-6 November 2025, Zurich

In November 2025, the Committee R/I participated in the European Intelligence Oversight Conference (EIOC). The EIOC was started in 2018 with the aim of creating possibilities for meetings and discussions for both oversight bodies and representatives from civil society. In 2025, the discussions focused specifically on bulk data and gaps in oversight of the intelligence and security services.

56 The IOWG brings together oversight bodies from Belgium, Canada, Denmark, the Netherlands, Norway, the United Kingdom, Sweden, and Switzerland.

International Intelligence Oversight Forum, 18-19 November 2025, Austin

The International Intelligence Oversight Forum (IIOFF) also took place in November 2025 in Austin, Texas. The presentations, organised around the theme "Intelligence Oversight in Complex Security Environments", addressed the relationships between oversight bodies and the intelligence services they oversee, the use of artificial intelligence tools in the context of national security, and Convention 108+.The Committee seise the opportunity of its trip to Austin to meet with members of the Strauss Centre for International Security and Law at the University of Texas.

Meeting with the Investigatory Powers Commission, 27 November 2025, Brussels

In November 2025, the Committee R/I hosted a delegation from the Dutch Investigatory Powers Commission (TIB) in Brussels. In the Netherlands, this commission is responsible for the *a priori* review of the intelligence methods used by the General Intelligence and Security Service (AIVD in Dutch) and the Military Intelligence and Security Service (MIVD in Dutch). At the meeting, both institutions discussed their legal obligations and practices in the area of communication, the use of artificial intelligence by the intelligence and security services, and the internal oversight they organise.

2. THE BELGIAN OVERSIGHT COMMUNITY

Besides international cooperation, the Committee also forges contacts and exchanges with its Belgian partners. Indeed, to ensure effective oversight of the intelligence and security services, close cooperation is essential among all actors in the 'oversight community', which goes beyond the Committee R/I alone.

2.1. Joint meetings with the Committee P

Article 52 of the Review Act provides for at least two meetings per year between the Committee R/I and the Committee P. In 2025, the committees did actually meet twice (in July and December). They discussed the progress of several joint dossiers, the draft revision of a protocol agreement on the exercise of the oversight bodies' powers regarding the processing of personal data, as well as the cases and operations of the Appeal Body.

At the same time, there were numerous exchanges with Committee P, specifically in the context of joint review investigations and the joint handling of complaints.

2.2. The Human Rights Consultation Platform

Since 2015, all institutions with a human rights mandate have undertaken to exchange practices and working methods, explore common issues, and promote mutual cooperation.[57] These exchanges take place within the Human Rights consultation platform.

In 2025, seven meetings were held under the chairmanship of the Flemish Institute for Human Rights and subsequently of the Federal Institute for the Promotion and Protection of Human Rights (FIRM). The discussions at these meetings focused specifically on the federal coalition agreement, mental health care in prisons, the reception crisis, the European regulation on artificial intelligence and, more generally, the challenges related to the use of artificial intelligence by public services, as well as policy developments concerning the European Court of Human Rights.

57 Protocol Agreement dated 13 January 2015 between the institutions with a full or partial mandate to ensure respect for human rights.

INTERNAL FUNCTIONING

WORKFORCE EXPANSION

COMPOSITION OF THE COMMITTEE R/I

Vanessa Samain and Séverine Merckx continued to serve in their respective roles as Chairwoman and French-speaking member of the Committee R/I in 2025. Linda Schweiger was replaced by Filip Vanneste, a judge on the Antwerp Court of Appeal, who was sworn in as a Dutch-speaking member on 22 April 2025. During the plenary session of the Chamber of Representatives on 6 November 2025, he was appointed to serve another six-year term.[1]

The Investigation Services, headed by Frederic Verspeelt, had seven commissioner-auditors. The administrative staff, led by Chief Executive Frédéric Givron, was bolstered thanks to the recruitment of a secretary, a clerk, a jurist, and a *Chief Information Security Officer* (CISO). At the end of 2025, there were 22 administrative staff members in service.

INTERNAL REORGANISATION

The reorganisation of the Committee's internal structure, implemented in consultation with the staff, was started in January 2025. In addition to the support functions (secretariat, IT, accounting, human resources), the administration is now divided into two sections: *Legal,* which handles legal matters and analyses, and *Perspective & Analysis,* which serves as a documentation and expertise centre. At the same time, transversal working groups (WGs) were set up, consisting of staff from various services within the Committee, with the aim of fostering a multidisciplinary approach to the Committee's tasks and responsibilities (WG Special Intelligence Methods, WG Internal and External Communication, WG Horizon 2030, etc.).

With this new organisational structure, the Committee aims to clarify the tasks and responsibilities of each team, especially since the expansion of the workforce. Moreover, the reform also addressed several recommendations of the Court of Auditors in its 2024 audit.

The reorganisation was evaluated during two team-building sessions: one in June 2025 for members of the Investigation Service and the other in October 2025 for the administrative staff. These seminars made it possible to identify specific avenues for action and define new work processes. The discussions also provided broader input for the drafting of the Committee R/I's future strategic plan.

1 At the same time, Vinciane Boon and Isabelle Goes were appointed as the first and second French-speaking substitute members of the Committee R/I, respectively.

A NEW VISUAL IDENTITY

The Committee also revamped its visual identity in 2025. This was part of the efforts to strengthen trust, underscore professionalism, and reflect the fundamental values and principles that guide the work of the Committee. Legality, integrity, independence, transparency, and rigour: these principles, the cornerstones of the Committee's operations, deserve an image that reflects and reinforces them.

As an institution eligible for funding from the Chamber of Representatives, the Committee reports to members of parliament and communicates with political leaders on a daily basis. However, they are not the Committee's only target audience; the Committee's work is also intended for the broader oversight community, which consists of institutional partners, civil society, and the press. But above all, the Committee wants to resolutely focus its efforts on citizens. Indeed, given the complex and multifaceted missions it performs on the periphery of the confidential sector of national security, the Committee remains largely unknown to the general public. Nevertheless, the work of the Committee, which is essential in a state governed by the rule of law, can have a direct impact on citizens (and their rights)—for example, through the handling of complaints. The Committee's new visual identity is therefore intended to enhance the visibility of the Committee as well as that of the oversight of the intelligence services.

The new logo symbolises several metaphors that echo the Committee's identity. The metaphor of the tree represents an organisation that, through its history, is rooted in a solid foundation of values. The trunk embodies stability and reliability, while the branches illustrate the diversity of its missions. The Committee's various tasks are carried out independently, but remain inextricably linked.

The subtle reference to the national colours alludes to the democratic principles on which the Belgian state is founded. It refers to the Committee's responsibility to act independently, impartially, and transparently, in the interest of every citizen.

Together, these graphic elements form a fingerprint that symbolises the Committee's unique identity as a body *sui generis*. This image reflects the institution's unique character, authenticity, and dependability, while also reminding us of the importance of confidentiality and the rigour that guides its missions.

PARLIAMENTARY MONITORING COMMITTEE

The Chairman of the Chamber, Peter De Roover (N-VA), is also chair of the Parliamentary Monitoring Committee for the Standing Police Services Monitoring Committee and the Standing intelligence services Review Committee (the Monitoring Committee). In 2025, the voting members were Paul Van Tigchelt (Anders), Sammy Mahdi (CD&V), Stefaan Van Hecke (Ecolo-Groen), Benoît Lutgen (Les

Engagés), Denis Ducarme (MR), Benoît Piedboeuf (MR), Peter Buysrogge (N-VA), Christoph D'Haese (N-VA), Maaike De Vreese (N-VA), Khalil Aouasti (PS), Eric Thiébaut (PS), Greet Daems (PVDA-PTB), Francesca Van Belleghem (VB), Marijke Dillen (VB) and Brent Meuleman (Vooruit).

During the course of 2025, the Monitoring Committee held two meetings, with the discussions focusing on a review investigation, the 2024 Activity report, several ongoing cases, and the internal operations of the Committee R/I.

OPEN TO OUTSIDE EXPERTISE

The Committee R/I also foster internal discussions regarding broader, contemporary challenges related to intelligence, security, or democratic oversight. To this end, the Committee relies on external experts, who are invited to share their insights during thematic lunches.

Two such sessions were organised in 2025. In June, Bernard Siman (Egmont Institute/VUB) presented a paper on hybrid warfare and developments in the field of war and peace practices. At its second session in September, the Committee welcomed Pascal Petry, advisor to the Federal Police and chair of the Coordination Committee on Intelligence and Security, who gave a presentation on the day-to-day, practical operations of this platform, which plays a central role in Belgium's security architecture.

BUDGET

The Committee R/I's budget for 2025 was set at €6,393,778, an increase of 1.6% compared to 2024, which corresponds to the indexation and the increases in staff salaries based on the salary scale.

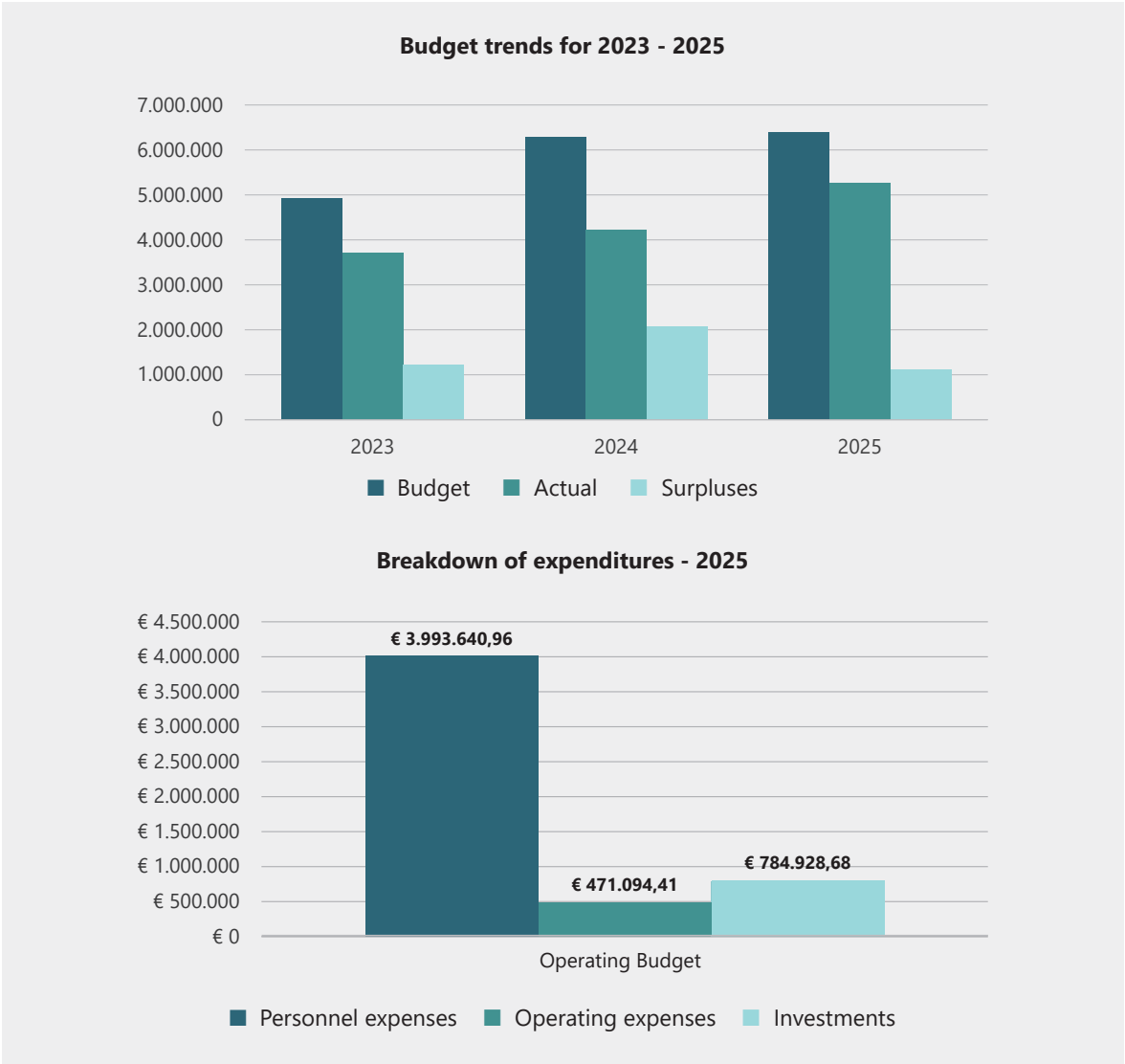
The funding allocated by the Chamber of Representatives is composed as follows: 81% as a grant—the sole contribution to net cash—and a 19% surplus from 2023. This is the Committee's sole source of funding, but it is enough to cover the costs of all its activities.

The implementation of the 2025 budget resulted in an accounting surplus of €1,125,013, which is the difference between the approved budget and the actual expenditure. The accounting surplus is divided equally between personnel and operating expenses. Two factors may explain these substantial surpluses.

- The Committee had requested exceptional funding for a three-year period in 2024 to digitise its processes and modernise its IT infrastructure. The implementation of this project is subject to the security verifications inherent in the nature of the Committee's work (the necessary security clearances for companies and personnel, which are granted following security investigations that take an average of 9 months), as well as the objective of optimising resources. As a result, there are often delays in identifying potential suppliers, available framework agreements, evaluating bids, and awarding contracts, which prevents the full utilisation of the available funds.

› In recent years, the sharp increase in the Committee's oversight remit, the emergence of new and highly diverse responsibilities resulting from legislative changes, as well as the increased workload from managing the Appeal Body, prompted the Committee to recruit new staff. During the fiscal years 2023, 2024, and 2025, several new recruitments or replacements were implemented. Due to the length of the recruitment process, the time required to obtain the necessary security clearances, and any applicable notice periods, more than a year may elapse between the call for applications and the actual start date of the employee in question. This timeframe is automatically recorded in the financial results for the year in which the recruitment takes place. The Committee is aware of this challenge and is making additional efforts to shorten the duration of the recruitment process, at least with regard to the parameters it can control.

It is therefore expected that recruitment of new employees in 2026 and even 2027, as well as the completion of the digitisation project, will lead to a new balance between the approved budget and actual expenditures, as well as a reduction in surpluses.



DIGITISATION

At the end of 2023, the Chamber of Representatives allocated a specific budget to the Committee R/I to implement a large-scale digitisation project aimed at modernising its operations.

Following the significant investments in *hardware* and *software* made in 2024, the projects in 2025 focused on digitising work processes. Among other things, modernising the operations of the Appeal Body's registry will make it possible to streamline administrative tasks. At the same time, the Committee is putting the finishing touches on the development of a digital library designed to facilitate modern and intuitive management of its documentation.

A hardware security solution has also been implemented to enable one-way data transmission between two networks. Specifically, the transfer of files from the online network to the Committee's secure network now takes place almost in real time, with strict adherence to security standards.

These IT developments are crucial to ensuring a balanced allocation of the Committee's resources across its remit. Furthermore, it means employees have modern and flexible tools at their disposal while ensuring an appropriate level of security.

In addition, several projects have been launched to modernise the Committee's classified network; a Chief Information Security Officer (CISO) has also been appointed.

The website of the Appeal Body, which is managed by the Committee, was also redesigned in 2025. Its content was revised following several significant legislative changes involving security clearances and security advice. In 2026, the Committee R/I will also have a new website.

ABBREVIATIONS

CCIV	Coordination Committee on Intelligence and Security
CDB T.E.R.	Common Database Terrorism, Extremism, Radicalisation process
COC	Supervisory body for police information
Committee P	Standing Police Services Monitoring Committee
Committee R/I	Standing Intelligence Agencies Review Committee
Convention 108+	Convention no. 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data
CSA	Competent Supervisory Authority
CUTA	Coordination Unit for Threat Analysis
CUTA Act	Act of 10 July 2006 on threat analysis
DP Act	Act of 30 July 2018 on the protection of natural persons with regard to the processing of personal data (Data Protection Act)
DPA	Data Protection Authority
DPO	Data Protection Officer
ECHR	European Convention on Human Rights
ETIAS	European Travel Information and Authorisation System
FIRM	Federal Institute for the Protection and Promotion of Human Rights
GISS	General Intelligence and Security Service
IOWG	Intelligence Oversight Working Group
ISA	Act of 30 November 1998 governing the intelligence and security services
LISC—R	Local Integrated Security Cells on Radicalism
LTF	Local Task Force
Monitoring Committee	Special committee entrusted with the parliamentary oversight of the Standing Police Services Monitoring Committee and the Standing Intelligence Agencies Review Committee
NSA	National Security Authority
NSC	National Security Council
NSIP	National Strategic Intelligence Plan
PFCECT	Platform Counter Extremism & Counter Terrorism
PNR	Passenger Name Record
Review Act	Act of 18 July 1991 governing the review of the police and intelligence services and the Coordination Unit for Threat Analysis
SIM	Special Intelligence Methods
SIM Commission	Administrative commission responsible for monitoring the specific and exceptional methods of information collection by the intelligence and security services
Strategy T.E.R.	Strategy Terrorism, Extremism, Radicalisation process
VSSE	State Security