Annual report 2022

CTIVD

Review Committee on the Intelligence and Security Services

Annual report

2022

Review Committee
on the Intelligence and
Security Services

Preface

Transparency about the activities of intelligence and security services is not a matter of course. Confidentiality or limited transparency is part and parcel of the services' activities. The usual legal frameworks such as the Open Government Act or legislation on privacy breaches do not apply. The constitution stipulates that ministers and state secretaries do not need to provide intelligence to parliament if this contravenes the interest of the state.

The CTIVD is not restricted in its access to information from the intelligence and security services. Translating what is secret into what can be shared has the constant attention of the CTIVD, and how to handle confidentiality was already addressed in a report from 2012. The fact remains that state secret information to which the House of Representatives or the CTIVD is privy may not be disclosed.

The CTIVD remains committed to optimizing transparency regarding the activities it oversees. This annual report therefore looks in more detail at the wide range of oversight activities undertaken by the CTIVD in 2022. This is not only prompted by the CTIVD's view of its task but also by the increasing dynamism in the domain of the intelligence and security services. Dynamism that includes technological developments, exponential growth in data, changes to threat perspective and the need for faster action.

The CTIVD increasingly consults with the services before means are used, to contribute to the lawful use of those means. When the CTIVD identifies risks or possible unlawful conduct during its oversight activities, it increases its efforts to mitigate these risks or end the unlawful conduct. The increased oversight of the cable, as described in section 2.2, is a clear example of this. System-based oversight is growing and when the 'Draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme' enters into force, the CTIVD's oversight will take place in near real time. It is to be welcomed that this bill stipulates that, by law, the decisions by the Judicial Division of the Council of State are in principle public, with the exception of the data that are already secret under the Intelligence and Security Services Act (ISS Act 2017).

The CTIVD wishes to provide greater transparency about its oversight activities in the coming period and to further disclose the underlying frameworks through publications, whether or not in modified form. Transparency on decisions and reports based on the application of these frameworks will also be developed further. As an independent oversight body with far-reaching investigatory powers, we feel it is only natural that we are publicly accountable for what we have done and how we went about it. One of our tasks is to contribute to the public debate and accurate perception through our role as an expert. This annual report aims to provide a clear picture of our oversight activities and their impact in 2022 and we look ahead to developments continuing in 2023.

Nico van Eijk
CTIVD Chair

Table of Contents

1

Introduction

As an independent oversight body, the Review Committee on the Intelligence and Security Services (**CTIVD**) oversees the balance between protecting national security and protecting fundamental rights. The CTIVD does so by applying the framework laid down for that purpose in the Intelligence and Security Services Act 2017 (ISS Act 2017).

The CTIVD's oversight activities focus in particular on the lawfulness of conduct by the General Intelligence and Security Service (**AIVD**) and the Military Intelligence and Security Service (**MIVD**). The CTIVD has far-reaching investigatory powers in this area which enable it to conduct in-depth **investigations** into the lawfulness of the services' conduct across the full range of their tasks.

The CTIVD also handles complaints and reports of misconduct on the part of the AIVD and the MIVD. Complaints may be filed by individual citizens or by interest groups working on their behalf. The CTIVD issues binding decisions on complaints. This means that the minister concerned has a duty to implement the **decisions on the complaints**.

Every year, before 1 May, the CTIVD publishes an annual report which is submitted to Parliament and to both the **Minister of the Interior and Kingdom Relations** and the **Minister of Defence**. The annual report accounts for and presents an overview of the work and publications by the CTIVD in the reporting year. Most of the information has already been published on the CTIVD's website (**www.ctivd.nl**). The annual report is a fully public report which is translated into English and made available on the CTIVD's website. This is the 2022 Annual Report.

Structure of the report

The report focuses on the following topics:

- Chapter 2 details the activities carried out by the CTIVD's Oversight Department in 2022. In addition to in-depth investigations and oversight reports, we discuss other oversight activities, such as the enhanced oversight on the cable, information dossiers and the oversight on digital security and reporting of unknown vulnerabilities. This chapter also highlights the publications issued in the context of advice on legislation. Furthermore, it discusses the various consultative and dialogue structures and how the quality and effectiveness of the oversight are guaranteed.
- Chapter 3 details the activities carried out by the CTIVD's Complaints Handling Department in 2022.
- Chapter 4 looks at the preparation for new legislation on investigations into countries with an offensive cyber programme and the role of the CTIVD in those preparations. This chapter also looks in more detail at the publications issued by the CTIVD in the context of advice on the bill.
- Chapter 5 discusses the cooperation with the Investigatory Powers Commission (TIB).
- Chapter 6 addresses the cooperation between the CTIVD and the oversight bodies of foreign intelligence and security services.
- Finally, chapter 7 describes the organization of the CTIVD in 2022.


2

Activities of the Oversight Department

2.1 In-depth investigations

The CTIVD conducts lawfulness investigations into, among other things, conduct by the AIVD and the MIVD when implementing the Intelligence and Security Services Act (ISS Act 2017). The CTIVD sets its own investigative agenda. In particular it looks at the societal context of the AIVD and MIVD's conduct.

The CTIVD's Oversight Department issued two review reports in 2022. The first is review report no. 74 into the use of automated OSINT by the AIVD and MIVD. The second review report is no. 75 into the use of cable interception by the AIVD and the MIVD. An overview of the main findings is given below. The review reports may also be accessed through the CTIVD website.

No. 74 | About Automated OSINT
Adopted on 20 December 2021, published on 8 February 2022

Automated OSINT is the automatic collection of data from information sources that are available to everyone using specialist software or web applications ('tools'). The tools have search and network analysis functions which can consult a wide variety of sources in a user-friendly way.

The tools make it possible to consult hundreds of sources at one time in a single search, including location data from mobile devices and leaked data of users of social media services. The tool can then provide a visual representation of the results. Private companies can aggregate these datasets as a single searchable source (a 'composite data set'), which in some instances may contain billions of data points.

OSINT undeniably goes well beyond investigative techniques such as checking telephone directories or using a search engine to access online data. The current practice of automated OSINT involves a more serious violation of privacy than was anticipated when the ISS Act 2017 was drafted. The CTIVD therefore recommended the legislators to create a legal basis with more robust foresight and sufficient safeguards governing the use of automated OSINT, both the tools themselves and the sources that can be accessed using these tools.

Before the tools can be used, the tools' functioning and underlying sources must be scrutinized beforehand in the context of the obligation to 'process data carefully'. This investigation showed that this was not done to a sufficient degree. The CTIVD recommended that both services take mitigating measures to comply with the general provisions in the ISS Act 2017 regarding data processing. In 2022, the CTIVD was in close contact with the services about the follow-up of this recommendation.

This review report contains a classified appendix. This appendix does not contain any reports of unlawful conduct that have not been described in the public review report. However, the classified appendix contains more detailed information that reveals the services' procedure relating to automated OSINT and for that reason had been marked 'classified'.

No. 75 | About Cable interception

Adopted on 26 January 2022, published on 15 March 2022

The investigation focused on the use of the special investigatory power of cable interception and related investigatory powers. Cable interception means that the AIVD and the MIVD may intercept large amounts of cable-bound communication (such as internet traffic) without that interception being aimed at a specific person or organization. The AIVD and the MIVD used cable interception between 1 May 2018 and 31 March 2021 in the form of 'snapshotting': the brief integral interception of certain data flows. The aim of snapshotting is to examine the intercepted data for its potential intelligence value. That interception does not yet have the purpose of using the data for intelligence or other investigations into specific persons or organizations. In the period investigated by the CTIVD, safeguards other than the legal safeguards applied to cable interception in the snapshot phase.

The CTIVD concluded that cable interception was conducted lawfully on key components, but that the legal duty of care had been insufficiently implemented. The duty of care includes the continuous monitoring by both services of how they process data and ensuring that this data processing is and continues to be in accordance with the applicable legal requirements. In the investigation period, compliance with the duty of care was secondary to operational interests. Consequently, unlawful conduct occurred in the interception process or was detected too late.

Based on the findings of that review report, the CTIVD decided in 2022 to oversee cable interception more closely and to report on it in more detail. That means that even after it concluded its investigation, the CTIVD continued to monitor how cable interception was conducted. The starting point here is to engage in dialogue with the services so that any risks of unlawful conduct can be identified at an early stage. Should that yield too few results, the CTIVD could then use the legal measures available to it in the context of its oversight duty. In section 2.2 we look in more detail at the CTIVD's activities and publications in the context of enhanced oversight of cable interception.

The report has no classified appendix.

Ongoing in-depth investigation

Investigation into management by the AIVD and the MIVD of the intelligence services of the police and the Special Service of the Royal Netherlands Marechaussee

On 23 February 2022, the CTIVD announced it would conduct an investigation into management by the AIVD and the MIVD of the intelligence services of the police ('IDs') and the Special Service of the Royal Netherlands Marechaussee ('BD KMar').

From the perspective of careful data processing, protection of fundamental rights of citizens and the guarantee of the legal division between the intelligence and security domain and the crime investigation domain, adequate management by the AIVD and the MIVD is required. All the more so since the IDs and BD KMar employees work at a physical distance from the services' office locations.

This issue is all the more topical now that the AIVD has announced its intention to move into the field of undermining by criminals, because this can pose risks for national security.[1]

The investigation ran into delays in 2022 and will be completed in 2023. Publication of the review is expected in the second half of 2023.

2.2 Enhanced oversight of cable interception

Enhanced oversight by the CTIVD commenced in December 2021 following the findings in review report no. 75 (2022) about cable interception (see section 2.1). This review report looked at the question of whether, in the period from 1 May 2018 to 31 March 2021, the AIVD and the MIVD lawfully operationalized an access location and lawfully exercised the cable interception in the snapshot phase. The main conclusion in report no. 75 was that the duty of care had been insufficiently implemented. The implementation of the duty of care came secondary to operational interests in the investigation period. The duty of care is laid down in Section 24 of the ISS Act 2017.
That duty means that the heads of the AIVD and the MIVD are responsible for applying technical, staffing and organizational measures to ensure data are processed lawfully, by continuously monitoring how the services process data and ensuring that this data processing is and continues to be in accordance with the applicable legal requirements (compliance). That is important because these checks enable the services to prevent unlawful conduct or discover it in time and take mitigating measures. Based on the findings, the CTIVD decided to oversee cable interception more closely and to report on it in more detail.

On 30 May 2022, the Oversight Department of the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations and the Minister of Defence about the first interim findings on the CTIVD's enhanced oversight of cable interception conducted by the AIVD and the MIVD. On 9 June 2022, a **Parliamentary letter** was published with the **response** to the interim findings. In a **separate Parliamentary letter** of 9 June 2022, Minister Bruins Slot (Interior and Kingdom Relations) and Minister Ollongren (Defence) discuss the findings of the CTIVD.

---

[1] https://www.bnr.nl/nieuws/juridisch/10462265/aivd-gaat-zich-meer-richten-op-aanpak-georganiseerde-misdaad-en-ondermijning.

On 9 November 2022, the CTIVD sent a **second letter** with its findings on the enhanced oversight on cable interception to the Minister of the Interior and Kingdom Relations and the Minister of Defence. In that letter the CTIVD informed the ministers that it would end its enhanced oversight in light of the progress that had been made, the initiatives that had been started and the commitments that had been undertaken.

The AIVD and the MIVD have taken substantial steps to enhance the implementation of the duty of care, including improving the internal check on the lawful processing of data and the technical interception chain. In addition, the services made a number of commitments for implementing cable interception further. The main commitment is that cable interception is extended gradually and that each extension will only be put into practice if the necessary preconditions, including aspects of the duty of care, have been met. The improvements that have been initiated must be embedded in both organizations.

On 2 December 2022, the Minister of the Interior and Kingdom Relations and the Minister of Defence sent the CTIVD's letter to the House of Representatives with a joint **cover letter**.

The CTIVD will continue its consultation on cable interception with the services and will continue to actively monitor this topic in 2023 as well.

2.3 Other oversight activities

Reporting unknown vulnerabilities (*zerodays*)

In 2022, as in 2020 and 2021, the CTIVD again addressed the follow-up of its recommendation to develop policy and procedures on reporting unknown vulnerabilities *(zero days)*, as stated in review report **no. 53** on the use of the hacking power by the AIVD and the MIVD (2017).

The CTIVD established that during 2022, the services had further implemented that recommendation, both in practice through the work of the Committee for Unknown Vulnerabilities and by developing their confidential internal policy further. The Committee for Unknown Vulnerabilities convened a number of times in 2022. Both services are actively involved in further developing a well-considered system to report zero days (responsible disclosure). As regards the services' internal policy, the CTIVD established that the services certainly made progress compared with previous years. A professional decision-making process is being worked out in detail.

Digital security

The AIVD and the MIVD work together closely in the area of digital security. The Joint Sigint Cyber Unit is an important part of that cooperation. The services investigate cyber threats, such as attacks on computer systems by state actors against Dutch authorities and companies, with the aim of identifying, interpreting and removing those threats. The services help those organizations to detect and, if need be, to mitigate the attacks. Agreements made about that cooperation are set out in covenants.

In March 2020, the CTIVD drafted a confidential protocol that applies to this form of cooperation in those cases involving specific sections of the state.

The protocol specifies, irrespective of the existing covenants, which requirements the CTIVD sets regarding this cooperation based on the ISS Act 2017 and how it includes those activities in its review.

The protocol also makes it clear that this form of review will not be published in a public review report, but that the CTIVD will issue its findings to the relevant organizations in a confidential report with the cooperation of the ministers concerned. The CTIVD will report on this ongoing form of review at least once a year to the relevant organizations.

In the fourth quarter of 2022, the CTIVD started its repeat investigations at these organizations. A confidential report will be disclosed to both organizations in 2023.

The CTIVD had already conducted an investigation at one of these organizations in 2020 and 2021. An investigation was conducted at the other organization for the first time in 2021. By early 2022, the CTIVD issued a confidential report on its previous investigations. The CTIVD concluded in its reports that the services acted in accordance with the legal framework, had handled an incident appropriately and had followed up points for improvement regarding their procedure. The CTIVD also identified points for change in the underlying covenants to ensure better alignment with the monitoring practice. It is up to the organizations who are party to the covenant to follow this up. The CTIVD will include this in its repeat investigations.

Information files

In 2020, the CTIVD introduced a new review instrument under the heading 'information file'. This allows for a faster and more effective response to developments within the services. An information file can be initiated for a variety of reasons, including an incident report by one of the services, but also following an observation during an indepth investigation which is not followed up in the investigation itself. That might be the case if the event falls outside the scope of the investigation, for example.

When initiating an information file, the CTIVD will generally request further information, enquire in writing and/or conduct meetings and on that basis plot its subsequent course. That course may take a number of forms. Based on the information file, it may be decided that further follow-up is unnecessary, or that a legal framework should be drawn up against which the established conduct by the service is checked, that an advisory opinion should be sent to the minister or that an in-depth investigation should be announced.

In 2022, the CTIVD commenced three new information files that are still ongoing at the time of publication of this annual report. These relate to matters including the cooperation between the AIVD and the police and the AIVD's task regarding criminal undermining of the democratic constitutional state/rule of law.

Furthermore, in 2022 the CTIVD completed an information file that was started in 2021. Based on the investigation in the context of that information file, the CTIVD found no unlawful conduct. Nor did it see reason to conduct an in-depth investigation into the topic. The CTIVD did make a recommendation that was in line with ongoing initiatives by the services.

Another information file was also ongoing in 2022, which was started in 2020. This information file relates to cooperation by the AIVD with non-state actors. Part of this information file was completed in 2021 with a letter setting the framework for

international cooperation with non-state actors, which was sent to the Minister of the Interior and Kingdom Relations, the Minister of Defence and the CIVD. The services and departments will follow up the set oversight conditions and recommendations. Handling of the remaining part has been delayed and is expected to be completed in 2023.

Notifications to the CTIVD

The Oversight Department regularly receives notifications from the AIVD and the MIVD. These include notifications prescribed by law, such as the services' duty to report authorization granted by the ministers for providing unevaluated data. The services must also notify the CTIVD if they use a special investigatory power to support their tasks, for example to check the reliability of a source. Other legal duties to report relate to cases in which the services fail or are unable to exercise the duty to notify and to the rejection of requests to access data processed by the services. The CTIVD examines these notifications periodically and checks if there is reason to conduct further investigation.

However, both services also submit notifications to the CTIVD that are not required by law, but that do ensue from the duty of care that both services have in the area of secrecy, security and lawful data processing. These may include reports of incidents that took place or notifications of actions not taken in accordance with the legal regulation (non-compliance). In 2021 and 2022, the CTIVD frequently consulted with the compliance units of both services about professionalizing the form these notifications should take and how they should be handled.

In 2022, the agreements between the services and the CTIVD about reports were recorded in a protocol. A pilot is currently underway to gain experience with the protocol and its application.

2.4 Advice on legislation

Amendment of the Security Screening Act

On 5 September 2022, the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations in response to the Bill amending the Security Screening Act (WVO) (Persons in Positions involving Confidentiality (Flexible Deployment) Act). The CTIVD was only asked to respond to the bill after it had been submitted for consultation. The CTIVD was therefore not involved in the preliminary process of the bill.

The bill amends the Security Screening Act in a number of respects, i.e. creating a location-specific security clearance (VGB) so that people in that location are able to change jobs more easily, the introduction of an obligation for the employer to register and de-register people in positions involving confidentiality, the introduction of the power to issue a writ of execution, the inclusion of an identification obligation, the introduction of the use of the Citizen Service Number (BSN), the change from criminal enforcement to administrative enforcement in case of non-compliance with Section 14 of the Security Screening Act and, finally, in specific cases, the possibility of being able to conduct a security investigation into a person whose position cannot be designated as one involving confidentiality.

The CTIVD raised questions about or commented on a number of topics and these may need to be amended. Below is a selection, please refer to **the letter** for the complete overview. The CTIVD points out that unwanted administrative confusion might arise from the possibility that some persons in positions involving confidentiality will have two different security clearance certificates for the same position. This is a matter that needs to be looked at in more detail, both for the working practice and the transitional provisions. From an oversight perspective, it is better to avoid the situation with double security clearances where possible.

The CTIVD is in favour of the obligation to register and de-register people in positions involving confidentiality. The AIVD and the MIVD must have the most up-to-date overview possible of active security officials. The CTIVD made several comments on the register to be used by the services for this.

The bill offers scope for ministers to submit a request to the Minister of the Interior and Kingdom Relations to give information about a person who does not or will not hold a position involving confidentiality. That means that a security screening will be conducted but security clearance will not be given. The CTIVD draws attention to a number of ambiguities about this new option in terms of necessity, effectiveness, scope, purpose and impact on the person involved.

Cyber investigations (interim measures) Act

In April 2022, the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations and the Minister of Defence with its response to the draft bill currently in consultation regarding the Draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme. In 2022 also, the CTIVD consulted frequently with the services, the departments and the TIB on the preparations for this draft bill. Chapter 4 deals with the background and substance of this draft bill and the CTIVD's role in that process.

The Processing personal data (coordination and analysis counterterrorism and national security) Bill

The Processing personal data (coordination and analysis counterterrorism and national security) Bill was submitted by the Minister of Justice and Security to the House of Representatives in November 2021. A round-table discussion was held on this bill in the House of Representatives on 31 March 2022. The CTIVD participated in that discussion. In preparation for that meeting, the CTIVD sent its **written contribution** to the House of Representatives, in which the CTIVD argued that the NCTV and/or the tasks assigned to the NCTV in the context of national security should be placed under the ISS Act 2017, so that the customary safeguards for national security and the specialized oversight on them apply and a uniform interpretation of the concept of national security is promoted. Furthermore, that ensures a single, coherent framework that determines who may exercise which tasks and investigatory powers and that cooperation is the starting point. That also entails securing the balance between the necessary scope for action and the fundamental rights at stake.

2.5 Consultation and dialogue

Consultations with Parliament, CIVD, departments and services

The CTIVD issues explanatory notes on its reports to Parliament, generally in the form of a technical briefing. The public reports are usually discussed in public with the parliamentary standing committee of the Interior and Kingdom Relations and/or the parliamentary standing committee of Defence, whereas the classified appendices are discussed behind closed doors in the Committee on the Intelligence and Security Services (CIVD).

In addition to its investigations, the CTIVD holds regular meetings with the departments (the Ministry of General Affairs, the Ministry of the Interior and Kingdom Relations, and the Ministry of Defence) and with the AIVD and MIVD. Periodic meetings are held with the officials in charge of the departments and the heads of the services. The official staff regularly convene meetings with the CTIVD on a range of topics, and the parties hold presentations for each other. For example, the CTIVD contributes to the induction programmes for new employees at the services and the services hold presentations for the CTIVD about new developments. The domain of both services is highly dynamic. A number of the services' programmes and projects are directly connected to the ISS Act 2017, whereby the CTIVD puts forward its point of view in a dialogue with the services.

During 2022, the CTIVD consulted frequently with the departments and services about, and contributed oral and written input to, the draft bill concerning investigations by the AIVD and the MIVD into countries with an offensive cyber programme. That topic is discussed in more detail in chapter 4.

2.6 Safeguarding the quality and effectiveness of oversight

Expertise

In order to be effective in its oversight of both services, the CTIVD must have expertise in a variety of fields. In addition to a broad legal basis, a range of knowledge areas is important, such as solid technical expertise to be able to fully understand the technological developments and growing technological possibilities for data processing by the AIVD and the MIVD. Another knowledge area is operational context to the various operations, and thus both knowledge and skills in the field of oversight are necessary. To ensure the right composition of its staff, the CTIVD therefore constantly seeks to achieve a balance of these different areas of knowledge and expertise. The CTIVD must adapt to the developments at the services to be able to continue conducting its oversight effectively. Chapter 7 deals with the development of the CTIVD's organization.

Internal and external critical input

The CTIVD sets great store by internal and external critical input in its oversight process. Each investigation is conducted by an investigation group, comprising a Review Committee member in the role of investigation leader and one or more review officers. The investigation may be supported by the IT unit. Internal critical input is given by members of the CTIVD staff not involved in the investigation group taking a critical look at the investigation.

External critical input is provided by the CTIVD's knowledge network involved in its investigations and in important topics concerning oversight. The members of the knowledge network not only reflect on the CTIVD's plans and choice of new investigations but also on its action plans, assessment frameworks, findings from practice and draft reports that the CTIVD draws up. Each of the knowledge network's members has passed a security screening at level A and is permitted to inspect state secret information. The current participants in the **knowledge network** are listed on the CTIVD website.

Apart from contributing to ongoing investigations, members of the knowledge network also participated in a number of meetings in 2022 and shared their views on a number of strategic subjects.

Reflection from society and science

The CTIVD has a broad network of contacts in interest groups, oversight bodies and scientific institutions in the Netherlands. This helps the CTIVD to keep in touch with social and scientific debate around balancing the interests of national security and protecting the public's fundamental rights. It uses that debate to help select its oversight activities.

Reception of reports within both services and follow-up of recommendations

In 2022, as in previous years, the Oversight Department consulted with the services' work floor staff to learn how the findings and recommendations from a review report are received by the services' workforce. During these consultations, the staff of both services are asked if the review report in question is clearly worded and if the recommendations put forward are feasible. The CTIVD finds these consultations constructive and helpful in improving its oversight duty and the way in which it draws up its reports.

Some time after publishing a review report, the Oversight Department requests the minister or ministers concerned to demonstrate how they followed up on the adopted recommendations. Where that leads to questions or obscurities, the CTIVD will consult further or conduct an additional investigation. Where necessary it will inform the minister or ministers how the implementation of its recommendations should be improved.


3

Activities by the Complaints Handling Department

3.1 Handling complaints and reports of misconduct

The Complaints Handling Department of the CTIVD has the authority under the ISS Act 2017 to handle complaints about alleged conduct by the AIVD or the MIVD. In these cases, the Complaints Handling Department acts as a follow-up complaints handler because the ISS Act 2017 stipulates that a complaint about the AIVD or the MIVD should first be handled by the minister concerned, as the primary complaints handler. This is the Minister of the Interior and Kingdom Relations for the AIVD, and the Minister of Defence for the MIVD. The complaints themselves are handled by the AIVD and the MIVD. If a complainant is dissatisfied with how the minister concerned handled their complaint, they can file their complaint with the Complaints Handling Department of the CTIVD. In some cases the Complaints Handling Department will take up a complaint immediately because the complainant cannot be required to first file their complaint with the relevant minister.

Furthermore, the Complaints Handling Department has the authority to handle notifications of alleged misconduct.

3.2 Complaints handling by the CTIVD in 2022

Below is an overview of the number of complaints processed by the Complaints Handling Department in 2022.

CTIVD	Complaints about AIVD	Complaints about MIVD	Other complaints[2]
Pending on 1 January 2022	4	3	–
Complaints received	32	4	17
Declared unfounded	1	1	–
Declared partly well-founded	1	4	–
Declared entirely well-founded	1	1	–
Handled informally[3]	6	1	–
Not handled[4]	22	-	17

[2] In other complaints it was unclear if the complaint related to the AIVD and/or the MIVD and the complainant failed to clarify this further.

[3] When a complaint is handled informally, it means that the complaint could be resolved satisfactorily without a formal complaints procedure being initiated. Examples include an intervention where the service is asked to respond to a message from the complainant or to offer a fitting solution.

[4] There may be a number of reasons why a complaint is not handled, for example, if the complaint was not about the AIVD or the MIVD, the complaint was not about a topic on which the Complaints Handling Department is competent to rule, the complaint was a repeat complaint, the complaint had not yet been handled in a first response by the minister concerned or the complainant failed to respond after the CTIVD asked for additional information.

CTIVD	Complaints about AIVD	Complaints about MIVD	Other complaints[2]
Forwarded to the minister[5]	1	-	-
Repealed	-	-	-
Pending on 31 December 2022	3	-	-

In total, the Complaints Handling Department handled six complaints in 2022, of which it already had four pending on 1 January 2022. In five cases (one complaint involved both the AIVD and the MIVD), this resulted in a formal decision by the Complaints Handling Department which was published in anonymous form on the CTIVD website. One handled complaint was not published. In three other cases the complaint handling had not yet been completed on 31 December 2022.

Decision after investigation

After an investigation into the contents of a complaint, the Complaints Handling Department of the CTIVD decided the complaint was well founded. This complaint, which involved both the AIVD and the MIVD, is discussed below under the heading 'imposing sanctions'.

In another complaint involving both the AIVD and the MIVD, no decision was issued on the element of the complaint about the AIVD (included in the table as unfounded) but the complaint was deemed well founded as regards the element of the complaint about the MIVD. That decision was not published because it had been classified as state secret.

The Complaints Handling Department ruled the four other complaints about the AIVD and the MIVD respectively, to be partially founded. The founded elements of the complaints related to the duration of the security screening and in three cases to how the complaint had been handled.

The above **decisions on complaints** are available on the CTIVD website in anonymous form.

Complaints handled informally

Finally, the Complaints Handling Department of the CTIVD was able to handle six complaints about the AIVD and one about the MIVD informally. A number of these complaints were about the AIVD or the MIVD failing to handle a complaint. After the Complaints Handling Department intervened, the complaints were handled.

Accessibility of the complaints process

Special investigatory powers are used covertly by both services. This means that citizens will generally be unaware if an investigatory power is being used against them. A complainant therefore does not need to provide substantiation for the alleged use of investigatory powers against them in their complaint. The legislator has chosen to make it easy to file a complaint, even in the case of covert situations, to ensure the legal remedy is effective. In other respects, few formal or substantive requirements are set to a complaint and the services or the CTIVD's Complaints Handling Department may

[5] If a complainant has not yet filed the complaint with the minister concerned, the Complaints Handling Department may refer the complaint to the minister at the complainant's request.

only refuse a complaint on a limited number of grounds. A complaint may be filed digitally with the AIVD, the MIVD and the CTIVD. In that sense, every attempt is made to make filing a complaint easy.

Imposing sanctions

The Complaints Handling Department issues binding decisions on the ministers concerned and may impose sanctions in that context, such as terminating an ongoing investigation of the services, terminating the use of special investigatory powers or removing and destroying data processed by the services. The Complaints Handling Department may impose such a sanction if it ruled, for example, that the use of the special investigatory power was unlawful.

Since the Complaints Handling Department was tasked with handling complaints about the AIVD and the MIVD with the introduction of the ISS Act 2017, it issued **a binding decision** for the first time in 2022, stating that data processed by the services needed to be removed and destroyed. This concerned five bulk data sets. The interest group Bits of Freedom had complained that the AIVD and the MIVD failed to destroy the bulk data sets on time and that they stored them for longer than permitted by law. The Complaints Handling Department looked at how the ministers implemented the temporary ministerial regulation on bulk data sets. The Complaints Handling Department ruled that the complaint was well founded and determined that the relevant bulk data sets had to be removed and destroyed. The Minister of the Interior and Kingdom Relations and the Minister of Defence subsequently removed and **destroyed** the data.

3.3 Reports of alleged misconduct submitted to the CTIVD in 2022

The ISS Act 2017 contains a procedure for reporting alleged misconduct by one of the services or by the Coordinator of the Intelligence and Security Services. Such reports may be submitted to the CTIVD's Complaints Handling Department. Any person who is or has been involved in implementing the ISS Act 2017 or the Security Screening Act may report alleged misconduct to the Complaints Handling Department. The reporter must first report the alleged misconduct to the service concerned. Should the internal report not have been properly handled within a reasonable term, the reporter may turn to the CTIVD's Complaints Handling Department.

The Complaints Handling Department will process the report if it believes that the report alleges misconduct, and will then investigate whether misconduct is likely to have occurred. The reporter and the minister concerned are both given the opportunity to explain their positions. The Complaints Handling Department will draw up a report on the basis of its investigation. It informs the reporter and the minister of its decision and may include recommendations to the minister. The minister then informs the CTIVD of how and within which term he or she will follow up on this decision. The decision of the Complaints Handling Department and the minister's response are submitted to Parliament by the latter. The CTIVD will publish an anonymized review of the report on its website.

No alleged misconduct was reported to the Complaints Handling Department of the CTIVD in 2022.

3.4 Complaints and reports of alleged misconduct handled by the AIVD and the MIVD in 2022

Complaints handled by the AIVD and the MIVD

Complaints may be filed with the minister concerned. The minister concerned is the Minister of the Interior and Kingdom Relations for the AIVD and the Minister of Defence for the MIVD. Complaints are handled de facto by the AIVD and the MIVD. If the complainant is dissatisfied with the results of the internal complaints handling, they may file their complaint with the Complaints Handling Department of the CTIVD. This first requires filing the complaint with the minister concerned, unless this cannot be reasonably expected of the complainant.

Below is an overview of the number of complaints processed by both services in 2022.[6]

Service	AIVD	MIVD
Pending on 1 January 2022	4	1
Complaints received	15	37
Declared unfounded	6	–
Declared partly well-founded	1	–
Declared well-founded	–	5
Handled informally[7]	6	–
Not handled[8]	1	16 (combined with referral)
Repealed	–	11
Referred[9]	1	Combined with not handled
Pending on 31 December 2022	4	6

Reports of alleged misconduct handled by the AIVD and the MIVD

No alleged misconduct was reported to either service. The lack of reports on misconduct over the years is striking, according to the CTIVD's Complaints Handling Department. In 2022, the Complaints Handling Department raised this issue specifically and held meetings with both services about this topic. The Complaints Handling Department will continue to address this issue in the coming year.

Dialogue between the CTIVD and the AIVD and MIVD about complaints handling and suspicions about reports of misconduct

Since the ISS Act 2017 entered into force, there has been regular consultation between the Legal Affairs departments of the AIVD and the MIVD (as primary complaints handlers) and the CTIVD (follow-up complaints handler) about the procedures and the implementation of the complaints mechanism in practice. That implementation is assessed, either on request or on its own initiative, by the Complaints Handling Department when handling complaints filed with them. Trends in the nature and number of the complaints filed are also addressed. On a periodic basis, both services submit lists of the complaints they handled or decided not to handle. The Complaints Handling Department can thus monitor the developments in primary complaints handling, the notification procedures and how these are used by both services.

---

6 The numbers were provided by the AIVD and the MIVD.
7 Handled informally means that a solution was found to the complainant's satisfaction without a formal complaints procedure being initiated.
8 This situation may occur if the complaints body is not authorized to handle the complaint or if the same matter is being handled by a court in objection or appeal proceedings.
9 Complaints filed with the wrong body are referred. The complaint is forwarded to the correct body in consultation with the complainant.


4

New legislation

As it did in 2021, in 2022 the CTIVD took part in frequent consultations with the services, the departments and the TIB about the draft bill on investigations by the AIVD and the MIVD into countries with an offensive cyber programme and the subsequent memorandum of amendment.

That draft bill was prompted by the view of the services and the departments that the ISS Act 2017 offers the services insufficient scope to oppose the threat coming from countries with an offensive cyber programme. That cyber threat is characterized by a great deal of dynamism and unpredictability. A country can use infrastructure across the entire world, with or without the knowledge of the owner of that infrastructure. For the services, that means an attack by an actor of this kind can come from any corner of the world, including the infrastructure within its own borders. In addition, these actors operate at top level with high-tech equipment and network *redundancy*.

A legal framework providing the services with more scope to deal with the dynamism and unpredictability of those cyber threats calls for oversight that ties in effectively, without any safeguards being scaled down. The relevant legislation must provide for a system of *checks and balances* that does justice to both the interests of national security and the protection of fundamental rights.

The proposal for a 'Draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme' was put out for public consultation on 1 April 2022. In April 2022, the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations with its response to the draft bill. Apart from several areas of concern, the CTIVD is able, from an oversight perspective, to concur with the principles of the interim measures. The draft bill was submitted to the House of Representatives in December 2022.

At the end of 2022, a draft memorandum of amendment to the submitted draft bill was prepared, which provides for two amendments to the draft bill. These amendments relate to a regulation for 'real-time interception' (a special investigatory power to intercept traffic and location data in *real time* and not the contents of the communication itself) to codify the case law of the EU Court of Justice and a regulation to assess the extension of the retention period of bulk data sets obtained through special investigatory powers. The draft bill for interim measures already contains a regulation on assessing bulk data sets in so far as these are covered by the interim measures. The draft memorandum of amendment contains a regulation for bulk data sets that is largely identical, albeit with a broader scope of application, i.e. all special investigatory powers excluding investigation-related interception.

The CTIVD attended meetings about the memorandum of amendment being prepared. On 16 January 2023 the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations in response to the Memorandum of Amendment to the Draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme that was put to consultation in December 2022.

In its response, the CTIVD stated that it considered the two proposed amendments in the memorandum to be a positive development and that the CTIVD supported the amendments because oversight is thereby strengthened and significantly more effective. These amendments to the interim measures repair a number of imperfections in the ISS Act 2017, which the CTIVD had pointed out in the past. Thus, the interests of national security and fundamental rights are better protected.

The CTIVD points out that the draft memorandum of amendment provides more safeguards for bulk data sets obtained through the use of investigatory powers than is currently the case in the ISS Act 2017. The CTIVD had already raised the issue of bulk data sets in relation to Section 27 of the ISS Act 2017 in 2019 in its reports on the implementation of the ISS Act 2017. The CTIVD considers it a positive development that the draft memorandum of amendment regulates a final deadline of one year in which to assess the relevance of data in a bulk data set, after which the minister must make a reassessment for the necessity of retaining the relevant bulk data set for another year. The draft memorandum also provides for a binding assessment by the CTIVD of the necessity, including the proportionality, of an extension of the assessment period by one year, whereby a bulk data set must be destroyed if the extension is denied. This makes it possible to take individual measures in a dynamic system and limit the amount of extensions. Furthermore, provisions are made to strengthen the rule of law by the option of appeal to an independent court if the minister disagrees with a binding assessment by the CTIVD.

The CTIVD makes several comments in its response, including on the fact that the review of the ISS Act 2017 should be taken up with minimum delay. The CTIVD also establishes that the regulation for the retention of bulk data sets in the draft memorandum relates to bulk data sets obtained through a special investigatory power, but not to bulk data sets obtained by other means. The CTIVD is of the opinion that ‘bulk is bulk’ regardless of how it was acquired. That principle implies that there should be a universal regime for bulk data sets.


5

Preserving legal uniformity and cooperation with the TIB

The Investigatory Powers Commission (TIB) and the CTIVD regularly meet to ensure they use the same interpretation of the ISS Act 2017. These meetings are called legal uniformity consultations. Both bodies have the duty pursuant to legislative history to consult where necessary and preserve legal uniformity. The legal uniformity consultations prevent the same legal provision being interpreted in different ways. This not only serves the legal certainty of citizens, who can then better understand the scope and application of the investigatory powers used by the AIVD and the MIVD, but also clarifies to both services the legal framework that applies to the performance of their tasks. In 2022, that did not result in a legal uniformity letter or other joint publication.

An important theme in 2022 was the Cyber investigations (interim measures) Act (see chapter 4). During 2022, the CTIVD and the TIB participated frequently in preparations for this draft bill and both bodies consulted closely and frequently with each other on this topic. The CTIVD and the TIB decided to issue their written points of view separately. In April 2022, the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations with its response to the draft bill. In January 2023, the CTIVD sent **a letter** to the Minister of the Interior and Kingdom Relations in response to the Memorandum of Amendment to the Draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme that was put to consultation in December 2022.

6

International cooperation

Today's intelligence and security services are cooperating more closely and in new ways. International cooperation is essential for those services to protect national security.

Although cooperation between oversight bodies is still in its infancy, more and more initiatives have been taken in this area since 2015. For example, the CTIVD has joined with five other oversight bodies to establish a cooperative partnership, the *Intelligence Oversight Working Group* (IOWG), and since 2018 a conference is organized annually in December for oversight bodies.

After a period of close cooperation within the IOWG in 2019, international cooperation with foreign oversight bodies was severely hampered in 2020 due to COVID-19. That cooperation was resumed in 2021.

In 2022, cooperation within the IOWG was stepped up. In March 2022, an administrative delegation of the CTIVD visited the Swiss oversight body. In October 2022, the CTIVD spoke with the participating oversight bodies in the IOWG at administrative and chairperson level. At that time, two Swedish oversight bodies, the *Swedish Foreign Intelligence Inspectorate and the Swedish Commission on Security and Integrity Protection*, officially joined the IOWG, after a period of being observers.

In October 2022, the CTIVD took part in the annual *European Intelligence Oversight Conference* held in London and organized by the British oversight body IPCO.

In November 2022, the CTIVD took part in the annual *European Intelligence Oversight Forum* (IIOF) in Strasbourg. The IIOF was organized by Professor Joe Cannataci, former UN rapporteur on the right to privacy and currently rapporteur for the Council of Europe in the context of the Convention 108+. In 2021, the CTIVD and the TIB published **a memo** on the implications of Convention 108+ for oversight on the processing of personal data in the context of national security. The IIOF aims to be a platform for international oversight bodies in the field of intelligence and security services, privacy and data protection and other parties involved such as the intelligence and security services, to discuss national and international developments and best practices.

A CTIVD delegation, together with fellow oversight bodies, participated in a conference in Berlin in June 2022 organized by the German knowledge centre *Stiftung Neue Verantwortung*.

In addition, the CTIVD maintains bilateral contacts with other oversight bodies. In May 2022, the Canadian oversight body visited the CTIVD. In September 2022, the CTIVD hosted a visit by the parliamentary oversight body of Finland.


7

Organizational developments

Composition of the CTIVD

In 2022 the CTIVD consisted of Nico van Eijk (chair), Marylène Koelewijn (member, until 1 Feb 2022), her successor Judith Lichtenberg (member, from Aug 2022), Harm Trip (member) and Addie Stehouwer (member and chair of the complaints department).

The CTIVD is divided into two departments, both of which are supported by the CTIVD's secretariat.

Oversight Department

Nico van Eijk
Chair

Marylène Koelewijn
Member

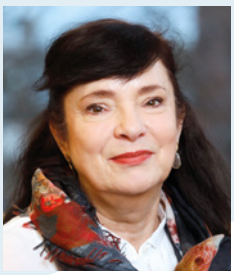
Harm Trip
Member

Judith Lichtenberg
Member
(from Aug 2022)

Complaints Handling Department

Addie Stehouwer
Chair

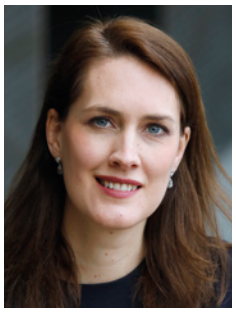
Hermine Wiersinga
Member



Anne Mieke Zwaneveld
Member

Erik Kok
Member

Staff



Kristel Koese
General Secretary

The CTIVD staff is headed by the General Secretary and consists of 12 legal, technical and operational review officers, two supporting staff members and one IT adviser. The staff supports both departments.

Extension of staff

During 2022, the CTIVD invested in extending the number of review officers. That was prompted by the Draft bill for the implementation of interim measures governing AIVD and MIVD investigations into countries with an offensive cyber programme (see chapter 4 for more details). That bill implies an extension of the CTIVD's task to strengthen review of the AIVD and the MIVD. An additional headcount of 10 FTE was therefore promised to the CTIVD in anticipation of the entry into force of the interim measures. Initially, the bill was intended to be submitted to parliament during 2022 and possibly come into force in the same year. The draft bill was ultimately submitted to the House of Representatives in December 2022. Five new review officers were appointed in 2022. Partly due to turnover in the existing workforce, it has not yet been possible to fill all vacancies in 2022. That process will be continued in 2023.

Accommodation

Commitments made in the context of the interim measures on the additional workforce at the CTIVD also included a commitment to provide the necessary working space. During 2022, the CTIVD consulted closely with the parties involved about extending the current housing and exploring options for new accommodation. That process will be continued in 2023.

Facilities developments

Administratively, the CTIVD falls under the Ministry of General Affairs. This means that the CTIVD can call on the Ministry's financial management, IT and HR services.

The CTIVD makes its own decisions about spending its financial resources. The CTIVD's budget amounts to around €2.5 million. That budget was increased temporarily in 2022 in connection with the interim measures. From 2023, the budget comes to about €4 million. That increase is permanent.

P.O. Box 85556
2508 CG The Hague

T 070 315 58 20
E info@ctivd.nl
I www.english.ctivd.nl