

Annual report 2023

CTIVD

Review Committee on the Intelligence and Security Services

Annual report

2023



Review Committee
on the Intelligence and
Security Services


TUNING

Preface

Developments in oversight

A core duty of the Dutch Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD) is to ensure professional and effective oversight. Ensuring the necessary preconditions for proper oversight was a central issue for the CTIVD in 2023. This focus was partly due to the preparation of, and parliamentary debate on, the draft bill for the Temporary Act on investigations by the AIVD and the MIVD into countries with offensive cyber programmes, bulk data sets and other specific provisions (hereinafter: the 'Temporary Act') as well as the government's outline memorandum on revising the current Intelligence and Security Services Act (ISS Act) 2017. The government's outline memorandum describes the key points for revising the ISS Act 2017 and was submitted on 1 September 2023.

Progressive developments in the oversight domain will significantly affect the processes for the Temporary Act and the outline memorandum. Therefore, the CTIVD felt it was important to participate in these processes as well as to provide its input. This concerns only the question of how the AIVD and the MIVD can operate decisively and in a future-proofed manner given all the developments in and challenges to adequately protecting national security, but — correspondingly — also the question of which system of assessment and oversight and what other guarantees are necessary to not only safeguard the fundamental rights of citizens in a democratic legal order, but also to continue ensuring an appropriate system of checks and balances.

The Temporary Act is the prelude to a number of important developments that will strengthen oversight as a counterbalance to the expansion of the AIVD and MIVD's operational capacity in the cyber domain. The Dutch House of Representatives approved the draft bill in November 2023. The Dutch Senate agreed in March 2024. This bill grants the CTIVD binding oversight of certain special investigatory powers used in cyber investigations, such as hacking and automated data analysis. This means that the Minister concerned is obliged, except in the case of appeal to the highest administrative court, to comply with the CTIVD's ruling of unlawfulness, and this can be accompanied by a measure to cease the exercise of a special investigatory power or to destroy acquired data. The Temporary Act does not alter the binding nature of the CTIVD's rulings on complaints.

The Temporary Act also authorises the Dutch Investigatory Powers Commission (Toetsingscommissie Inzet Bevoegdheden, TIB) and the CTIVD to exchange relevant information. Under the current ISS Act 2017, these oversight bodies may only exchange information for legal coherence consultations, which aim to ensure that both parties maintain a consistent interpretation of the Act. The Temporary Act expands the possibilities for exchanging information, which represents a major advancement in inter-organisational cooperation.

In 2023, the CTIVD prioritised the preparations for the implementation of the Temporary Act, including the drafting of assessment frameworks and internal procedures. The committee will continue these preparations in 2024.

The Temporary Act – valid for a period of four years – is seen as a precursor to the previously announced intense overhaul of the ISS Act 2017. The CTIVD and the TIB have indicated that they are in favour of further integrating assessment and oversight by creating a single independent body responsible for end-to-end' oversight. The provisional name for this independent oversight body is the 'National Security Authority' (NSA). In line with this stance, the government's outline memorandum also identifies this 'integrated oversight' as an important option.

The 'single oversight body' model promotes the professionalisation of the system of assessment and oversight and enhances the coordination of the ex-ante testing with the oversight. This will facilitate better adaptation to new developments and risks in the dynamic operational practices of the intelligence and security services, while providing a normative framework for the entire chain. It should be noted that the CTIVD's oversight activities cannot be characterised as purely 'ex post' or 'ex durante'. It is too narrow a view that the oversight activities of the CTIVD only follow the ex-ante testing of a special investigatory power and are aimed at verifying, before and after an operation, whether the intelligence and security services are exercising or have exercised the relevant special investigatory power in a lawful manner. The ex-ante testing represent only one aspect of the comprehensive oversight activities carried out by the CTIVD. Indeed, the CTIVD is charged with monitoring the lawfulness of the implementation of the entire Intelligence and Security Services Act 2017 and the Security Screening Act (Wet Veiligheidsonderzoeken, Wvo). To this end, the CTIVD not only conducts various types of lawfulness investigations and reports on the results, but it also focuses on promoting lawfulness prior to the performance of the intelligence activities. Since the introduction of ISS Act 2017, the CTIVD has endeavoured to maintain a constant dialogue with the intelligence and security services. Increasingly, the CTIVD directly engages the intelligence and security services in 'front-line dialogue' on proposed procedures or activities while providing them with feedback on legal frameworks or policy documents. This proactive approach helps to prevent or reduce the risks of unlawful conduct by the intelligence and security services. The CTIVD's 'end-to-end' oversight activities also provide the relevant context for ex-ante testing.

Developments in oversight, such as the binding oversight stipulated in the Temporary Act, require a significant expansion and further professionalisation of the organisation. This, in turn, requires additional professional development and training for employees. When recruiting new staff for the CTIVD's oversight departments, we look for people who possess wide-ranging knowledge, such as legal expertise and experience, but who also have technical expertise, such as in cybersecurity and IT architecture, and experience in the broader oversight domain. In doing so, the CTIVD is building the balanced, multidisciplinary organisation required to operate effectively within the dynamic environment it oversees.

Developments in oversight translate not only into advances in investigative methodology but also to new oversight instruments. Integrating systemic oversight into the 'palette' of available oversight instruments is a good example of advances in investigative methodology that align with the CTIVD's organisation-wide promotion of lawfulness. This form of oversight relies on the internal control systems and (compliance and auditing) functions of the intelligence and security services. Within this dynamic, the services strive for effective and integrated risk mitigation that entails greater risk awareness and heightened responsibility for risk management. The CTIVD can incorporate this into the risk-based approach to its oversight activities.

As early as 2022, the CTIVD was promised a staff complement of ten full-time equivalents (FTEs) to prepare for the expansion of its tasks under the Temporary Act. Although the promised staff extension made in view of the additional tasks for the CTIVD under the Temporary Act included a commitment to provide the necessary workspace, this has not been realised in 2023. A suitable workspace for the CTIVD, with a sufficient number of workstations, is particularly important now that our staff cannot work from home due to the classified nature of their work. Consequently, the CTIVD has not been able to move forward with the expansion of its organisation. At various moments and meetings throughout 2023, the CTIVD requested greater attention for this urgent issue, eventually expressing this in a letter to the Dutch prime minister. Despite serious attention from the parties involved and certain steps, it remains a difficult process with no prospect for a definitive solution at the time of writing this foreword in the first quarter of 2024. Housing will continue to form a point of concern that requires plenty of our attention in 2024.

On behalf of the CTIVD,
Judith Lichtenberg, Addie Stehouwer and Harm Trip.



Table of Contents

Preface 3

1 Introduction 9

2 Activities of the Oversight Department 11
2.1 In-depth investigations 11
2.2 Validation investigation 13
2.3 Information files 14
2.4 Additional oversight activities 14
2.5 Legal and regulatory advice 18
2.6 Roundtable sessions 19
2.7 Consultations and dialogue 20
2.8 Safeguarding the quality and effectiveness of oversight 21

3 Activities of the Complaints Handling Department 25
3.1 Handling complaints and reports of misconduct 25
3.2 Complaints handled by the Complaints Handling Department of the CTIVD 25
3.3 Complaints about oversight received since 1 May 2018 28
3.4 Interventions in security screening 28
3.5 No reports of suspected misconduct 29
3.6 Complaints and reports of suspected misconduct handled by the AIVD and the MIVD 30

4 New regulations 33

5 Monitoring the legal coherence of the Act and the cooperation with the TIB 39

6 International cooperation 43

7 Organisational development 47

1



Introduction

As an independent oversight body, the Review Committee on the Intelligence and Security Services (**CTIVD**) safeguards the balance between protecting the national security of the country and preserving the fundamental rights of its citizens. In order to maintain this balance, the CTIVD uses the resources provided for by the legislation, while adhering to the prevailing international frameworks.

The CTIVD's oversight tasks and duties focus in particular on the lawfulness of the conduct of the General Intelligence and Security Service (**AIVD**) and the Military Intelligence and Security Service (**MIVD**). This review committee has extensive powers to conduct in-depth **investigations** into the lawfulness of the Dutch intelligence community's activities across the full scope of their tasks.

The CTIVD also investigates complaints and reports of misconduct concerning the AIVD and the MIVD. Complaints can be submitted by citizens directly or on their behalf by interest organisations. The CTIVD issues binding rulings on complaints, which means that the Minister concerned is obliged to implement the committee's **decisions on complaints**.

Every year, the CTIVD publishes its annual report prior to 1 May and subsequently presents it to the Dutch parliament and the relevant Minister of the Interior and Kingdom Relations (**BZK**) and the Minister of **Defence**. The CTIVD's annual report provides an account and overview of its activities and publications in the reporting year concerned. The majority of these activities and publications have already been published on the website of the CTIVD (**www.ctivd.nl**). The annual report is available in full to the public, translated into English and published on the CTIVD's website.

Reader's guide

This annual report addresses the following topics in succession.

- Chapter 2 details the activities of the CTIVD's Oversight Department in 2023. Aside from the in-depth and validation investigations as well as the information files, we discuss other oversight activities, such as various other investigations and the monitoring of the intelligence and security services' reports to the CTIVD. This chapter also briefly highlights the publications we have issued to advise on laws and regulations. We also describe the roundtables we have organised, the consultation and dialogue structures our organisation uses and how we ensure the quality and effectiveness of our oversight.
- Chapter 3 describes the activities of the CTIVD's Complaints Handling Department in 2023. This chapter concentrates on interventions by the CTIVD in the complaints handling process and the security screening.
- Chapter 4 deals specifically with the preparation for the new legislation regarding investigations into countries with offensive cyber programmes and the CTIVD's role in this. This chapter also discusses in greater depth the publications issued by the CTIVD to provide advice on both the draft bill for the Temporary Act and the outline memorandum.
- Chapter 5 discusses the cooperation with the Investigatory Powers Commission (TIB).
- Chapter 6 provides insight into the CTIVD's collaborations with the international oversight bodies of other intelligence and security services.
- Finally, Chapter 7 describes how the CTIVD organisation is structured in 2023.


DATA
TECHNOLOGY
2
SECTION

Activities of the Oversight Department

The CTIVD conducts various lawfulness investigations into the conduct of the AIVD and MIVD in the implementation of the Intelligence and Security Services Act 2017 or the Security Screening Act. The CTIVD independently determines (through risk-based oversight and other approaches) not only what it will investigate, but when it will perform these respective investigations. The committee also explicitly considers the societal context of the intelligence and security services' activities.

The CTIVD chooses which investigatory methods and oversight instruments it will deploy based on the nature and purpose of the oversight activity in question. See below for an account of the investigations we completed or conducted in 2023, as well as other activities.

2.1 In-depth investigations

Traditionally, the CTIVD has conducted so-called 'in-depth investigations' into the topics covered by the ISS Act 2017. The CTIVD's findings and recommendations are published in a public oversight report, potentially accompanied by a classified appendix that is sent to the Committee on Intelligence and Security Services (Commissie voor de Inlichtingen- en Veiligheidsdiensten, hereinafter: the CIVD) of the House of Representatives. The Minister or Minister's concerned then forward this public oversight report and their policy response thereto to the parliament.

In-depth investigations completed in 2023



Oversight Report No 76 into the AIVD and MIVD's management of the intelligence services (IDs) of the National Police and the special service (BD) of the Royal Netherlands Marechaussee (Koninklijke Marechaussee, KMar)

Adopted on 21 December 2023. Published on 6 February 2024.

On 23 February 2022, the CTIVD announced it would investigate the AIVD and MIVD's management of the intelligence services (IDs) of the National Police and the special service (BD) of the Royal Netherlands Marechaussee. This investigation was concluded in 2023. The resultant oversight report was adopted on 21 December 2023 and published on 6 February 2024.

The tasks of the intelligence services of the National Police and the special service of the Royal Netherlands Marechaussee are divided into three main processes: the deployment request, the scanning function and the regional investigation. The CTIVD's investigation focused on the scanning function and the regional investigation

conducted by the intelligence services of the National Police and the special service of the Royal Netherlands Marechaussee. Because the Military Intelligence and Security Service (MIVD) exclusively uses deployment requests that have been submitted by the special service of the Royal Netherlands Marechaussee, the report focuses on the General Intelligence and Security Service (AVID). Where relevant, the report's recommendations also apply to the MIVD.

The (IDs) intelligence services' activities (only for the AIVD) and the (BD) special service's activities (for the AVID and the MIVD) are entirely covered by the ISS Act 2017. The intelligence services (IDs) now focus exclusively on national security and no longer on public order. In light of this, the AIVD or the MIVD must provide adequate guidance to, and exercise control over, both intelligence services (IDs and BD). This is particularly important as, administratively, these intelligence services fall under the responsibility of their respective parent organisations (the National Police or Royal Netherlands Marechaussee) ; not the AIVD or the MIVD.

Although with the establishment of the National Police, a separation has been made between their intelligences services (for national security purposes) and the Public Order Intelligence Teams (TOOI) (for public order matters), there is still tension at play between public order and national security. The distinction between the national security and the public order is important because the tasks differ and the investigatory powers that may be used for these two priorities vary. For these reasons, the CTIVD stresses the importance of the AIVD providing sufficient guidance to and control of the intelligence services (IDs).

Our investigation revealed, however, that the AIVD failed to provide sufficient guidance and control in several areas. This mismanagement increases the risks for unlawful or negligent behaviour, which did in fact occur in some instances. The CTIVD made two recommendations in its oversight report in order address these risks and to prevent them in the future.

The Minister of the Interior and Kingdom Relations, on behalf of the Minister of Defence, has endorsed the conclusions from the report and adopted its recommendations. The Ministers sent the report to the House of Representatives on 6 February 2024. In this report, the CTIVD refers to the Ministers' accompanying **policy response**. A classified appendix to this report was sent to the CIVD of the House of Representatives.

Announced and/or ongoing in-depth investigations in 2023

Three investigations into the design and use of the power to deploy agents by the AIVD and MIVD

On **23 May 2023**, the CTIVD announced that it would conduct three investigations into the power to deploy agents elaborated in Section 41 of the ISS Act 2017. All of these investigations concern the AIVD as well as the MIVD.

The investigations probe the following:
- the deployment of virtual agents:
- fulfilling the duty of care regarding agents' mental well-being;
- the deployment of journalists as agents.

The findings of these investigations are slated for publication.

Investigation into the AIVD and MIVD's role in the suspected leaking of state secrets by NCTV employees

On 25 October 2023, the CTIVD decided to investigate the AIVD and MIVD on matters related to the suspected possession and disclosure of state secret information by employees of the National Coordinator for Counterterrorism and Security (NCTV). The CTIVD had previously informed the CIVD of the House of Representatives about this investigation on 1 November 2023. The investigation was publicly announced to the House of Representatives on **19 January 2024**.

The investigation focuses on the following:

- the General Intelligence and Security Service's carrying out of security screenings;
- fulfilling the duty of care with regard to providing state secret information to the NCTV;
- the AIVD's performance of the task as the National Security Authority.

The MIVD will also be involved in the investigation insofar as it touches on the performance of its tasks and duties. The investigation findings will be published.

Investigation request submitted by the CIVD

In October 2023, the CIVD ask the House of Representatives to conduct an investigation into certain aspects regarding Mr Nissi and his relation to the AIVD. The CTIVD has agreed to conduct this investigation. The findings of this investigation will not be released to the general public.

2.2 Validation investigation

Following an (in-depth) investigation, the CTIVD sometimes conducts investigations to ascertain whether recommendations have been followed and in which manner. We refer to this as a 'validation investigation'.

Letter regarding the outcomes of the pilot project to assess the use of OSINT tools

On **11 October 2023**, the CTIVD briefed both of the Ministers concerned on the outcomes of the AIVD and MIVD's pilot project to explore the potential of Open Source Intelligence (OSINT) tools.

As follow up to the recommendations outlined in Oversight Report No 74 (2021) regarding Automated OSINT, the AIVD and MIVD launched a pilot to explore the use of these tools in the intelligence process. In the letter, the CTIVD informed the Ministers concerned about the results of the pilot as well as additional oversight activities.

In the letter, the CTIVD stresses that the use of these tools requires that a risk inventory be carried out and that measures to mitigate the identified risks must be taken for all tools in the intelligence process. Furthermore, a comprehensive record of the tools used should be maintained and periodically updated. The AIVD and MIVD have been requested to implement improvements in the short term.

In their **policy response** of 24 October 2023, the Ministers concerned endorsed the recommendation's premise that the risk inventory should ultimately lead to measures that mitigate the identified risks for all tools in the intelligence process. The intelligence and security services will begin working on this recommendation and will discuss it further with the CTIVD.

2.3 Information files

The CTIVD has been utilising the oversight instrument involving information files for several years now. The underlying rationale for using this instrument is that it allows for faster and more effective responses to the emergent developments within the intelligence and security services. There are a range of triggers for opening an information file, such as an incident report filed by an intelligence and security services, but also observations from in-depth investigations that the main investigation itself did not follow up on. This may be the case, for example, because the incident falls outside the scope of the investigation.

When opening an information file, the CTIVD will typically request additional information, pose questions (in writing) and/or conduct interviews before charting a course of action. This course of action, in turn, take on different forms. Based on the contents of the information file, the CTIVD may decide that no further follow-up is necessary, it may draw up a legal framework to assess the conduct of the intelligence service, it may send an advisory letter to the Minister concerned or it may announce an in-depth investigation.

In 2023, the CTIVD began compiling an information file about the intelligence and security services' cooperation with private parties. In 2023, the CTIVD sent a confidential letter to the directors of the intelligence and security services because the legal basis chosen by the services to justify this cooperation was inadequate. Consequently, the information file was not completed. The CTIVD will continue to keep its finger on the pulse of developments on this file in 2024.

The previously opened information files were continued in 2023. These concern, among other things, aspects of the AIVD's cooperations with non-state actors and the police, as well as the AIVD's task regarding (criminal) undermining. In the interest of these files, the CTIVD has held briefings and discussions with the intelligence and security services. As part of this file, the CTIVD sent a confidential letter to the director of the AIVD concerning the service’s cooperation with the police, pointing out that the ISS Act 2017 does not foresee a legal basis for this cooperation. After receiving this letter, the director of the AIVD terminated its cooperation with the police. Further discussions regarding this file will continue in 2024.

2.4 Additional oversight activities

Exploratory investigation into national partnerships

In August 2023, the CTIVD initiated a preliminary investigation into the AIVD and the MIVD’s participation in national partnerships. The CTIVD considered it important to use an exploratory investigation to gain a better impression of the risks that may arise from cooperations based on covenants with other government bodies, whether these risks are sufficiently understood by the services and whether there are sufficient guarantees. to mitigate such risks. For the CTIVD, exploratory investigations are often the precursor to its in-depth investigations, helping the Committee to learn about certain developments and risks and to make decisions about the focus of the investigation.

As part of this exploratory investigation, the CTIVD held a **roundtable session** on national cooperations and partnerships on 13 October 2023 (see Section 2.6). The roundtable sessions adopted a general focus rather than a focus on specific partnerships. Various experts took part in the discussions on the legal and organisational bottlenecks within the oversight process as well as the domain's unique challenges. These topics were incorporated into the exploratory investigation.

The exploratory investigation initially focused on two specific partnerships: the Counter-Terrorism Infobox (CTI) and the Cyber Intel/Info Cell (CIIC). The CTIVD believes that there are grounds for a wider investigation into this matter.

The Committee, however, decided to postpone this wider investigation due to its limited capacity to carry it out.

Exploratory investigation into the deployment of hacking powers

This exploratory investigation, which was launched in October 2023, examines the AIVD and MIVD's deployment of hacking powers.

The objective of the exploratory investigation is to inform the CTIVD about the application of the hacking power in preparation for the implementation of the Temporary Act on investigations into countries with offensive cyber programmes, for which aspects of the hacking power, such as the technical risks, are subject to dynamic and binding oversight of the CTIVD.

This investigation will continue into 2024.

Thematic investigation into the data management and IT infrastructure of the AIVD and MIVD

This is a wide-ranging investigation into the design of, and developments in, the individual and collective data management and IT infrastructure of the AIVD and MIVD. The investigation was launched in September 2023. This investigation focused on topics like automated data analysis (ADA), data reduction (DR) techniques, identity access management (IAM), cable interception and the development and functioning of applications.

At this phase, the objective of the investigation is to apprise the CTIVD of the developments and other findings pertaining to the intelligence and security services' data management process. Based on the results of the investigation, the CTIVD also holds quarterly meetings with the CIOs of both services to reflect on the progress and findings thus far. Interim findings may be reported publicly.

This investigation will continue into 2024.

Proactive monitoring of cable interception

Throughout 2023, the CTIVD proactively monitored the emergent developments in the intelligence and security services' cable interception practices. We began doing this in November 2022 as a follow-up to the investigation and the resultant **Oversight Report No 75** that addresses the AIVD and MIVD's use of cable interception.

Since this time, there have been minor changes regarding the collection and filtering of the data obtained via cable interception. The planned expansions for other investigative tasks at the new access sites were not carried out. With one exception, the permission applications approved by the Ministers concerned for the expansion of cable interception and the broader exploration of cable traffic (*snapshotting*) have been declared unlawful by the TIB on various grounds. This is further elaborated in the letter sent to the Ministers.

In the period November 2022 to December 2023, the CTIVD noted that the services continued the central management of, and multidisciplinary approach to, the development and organisation of their cable interception compliance. The services' ongoing efforts for their cable interception compliance ensured that their decision-making process would take all perspectives into account. Further attention must be paid to the additional processing (i.e. analysis) of the data within the interception chain. When incidents do occur, they are reported to the CTIVD according to the previously concluded agreements.

In **a letter dated 23 January 2024**, the CTIVD informed the Minister of the Interior, Kingdom Relations and the Minister of Defence of its findings and explained how the procedure for monitoring these cable interception practices would change. After providing this letter, the CTIVD ceased its proactive monitoring of the service's cable interception. As part of its ongoing monitoring of the data management and IT infrastructure of the intelligence and security services, the CTIVD has decided to focus its oversight on the additional processing of data collected via cable interception. The AIVD and the MIVD have committed to informing the CTIVD of any expansion of their cable interception practices through new access sites or major changes in the cable interception chain, so that the CTIVD can take this into account in its oversight, if necessary. On 14 February 2024, the Minister of the Interior and Kingdom Relations and the Minister of Defence forwarded the CTIVD's letter to the House of Representatives, including **a joint recommendation letter**.

Reports submitted to the CTIVD

Legal reporting obligations
The AIVD and MIVD regularly submit reports to the Oversight Department. On one hand, these are reports required by law. For example, the intelligence and security services are required to report any authorisation granted by a Minister or Ministers to provide unevaluated data to international intelligence and/or security services. The CTIVD must be notified about the deployment of a special investigatory power to facilitate the performance of tasks, such as testing the reliability of a source. Other legal reporting obligations concern the failure (or inability) of the intelligence and security services to fulfil their reporting obligations and the rejection of requests to access data processed by these services. The CTIVD periodically reviews these reports and assesses whether there are grounds for further investigation.

In 2023, the CTIVD drafted internal general working instructions, which, in principle, apply to all the reports to be made by the intelligence and security services. Internal working instructions/review frameworks are also being developed for the specific categories of reports. The intelligence and security services have been informed about the general procedure. Internal consultations are regularly held on the reports made to the CTIVD. Ultimately, this also serves as input for the CTIVD's risk-based approach to its oversight.

Incident reporting obligation
On the other hand, the intelligence and security services also submit reports to the CTIVD that are not (explicitly) required by law. These reports stem from the duty of care both services have regarding confidentiality, security and lawful data processing. These may include, for example, reports of incidents that have occurred or situations in which the legal regulatory compliance (non-compliance) was not met. Throughout 2021 and 2022, there were frequent dialogues with the compliance divisions of both services about further professionalising how they prepare and handle these reports. In 2022, a protocol between the intelligence and security services and the CTIVD set out the agreements for reporting incidents. In 2023, all of the parties gained additional experience with the protocol and the application thereof.

Bulk data sets reporting obligation
The **Temporary Regulation on further processing of bulk data sets** (Tijdelijke regeling verdere verwerking bulkdatasets) entered into force in 2020. This regulation included additional safeguards around the access to, and use of, bulk data sets by the AIVD and MIVD. This was in response to two critical oversight reports the CTIVD drafted on bulk data sets: Oversight Report **No 70 on the use of hacking powers to gather bulk data sets** (i.e. bulk hacks) and Oversight Report **No 71 on the processing of airline passenger data**. The regulation stipulates, among other things, that the AIVD and MIVD must report to the CTIVD the establishment of a (new) access regime for a bulk data set or the refusal thereof by a Minister. The CTIVD oversees the correct classification of bulk data sets into the three access regimes and compliance with the relevant safeguards.

Reporting (vulnerabilities) equities process (*zero days*)
The AIVD and the MIVD weigh the importance of (temporarily) not reporting each unknown vulnerability for the purposes of national security against the benefits that this reporting may serve. The guiding principle here is 'report, unless...'.

The CTIVD maintains constant oversight of the intelligence and security services' deliberation process for unknown vulnerabilities. For the purpose of this form of oversight, the CTIVD dialogues with the intelligence and security services, and, at least every six months, the CTIVD's Unknown Vulnerabilities Research Group performs a random check of the services' systems.

The CTIVD found that the services conducted the deliberation process responsibly throughout 2023. The new (confidential) internal policy represents a significant advancement and has been formally endorsed by the directors of the intelligence and security services who sit on the Committee on Unknown Vulnerabilities (Commissie Onbekende Kwetsbaarheden). The Committee on Unknown Vulnerabilities convened multiple times in 2023. Both services (the AIVD and MIVD) continue to improve their system for reporting unknown vulnerabilities in order to actively promote its further development

Digital security
The AIVD and the MIVD work closely together on digital security. The Joint Sigint Cyber Unit also has an important role in maintaining digital security. The intelligence and security services investigate cyber threats, e.g. attacks on computer systems, originating from state actors targeting Dutch governmental authorities and businesses, with the aim of recognising, identifying and removing these threats. To this end, the intelligence and security services assist these organisations with the detection

and possible mitigation of these attacks. This cooperation is based on agreements elaborated in covenants.

In March 2020, the CTIVD drafted a confidential protocol about this form of cooperation in cases involving special elements of the state.

Separate from the existing covenants, the protocol specifies which requirements the CTIVD must impose on this cooperation under the ISS Act 2017 and how it is to incorporate these activities into its oversight duties.

The protocol also stipulates that this form of oversight not culminate with a public oversight report, but rather that the CTIVD provide its findings to the relevant organisations confidentially and with the intercession of the Ministers concerned for the relevant organisations. This form of oversight is ongoing and the CTIVD will report on it to the relevant organisations at least once a year.

In the fourth quarter of 2023, the CTIVD initiated repeat investigations for these organisations. The reports were adopted in December 2023. The reports were submitted to all of the organisations on a confidential basis. In its reports, the CTIVD concluded that the intelligence and security services acted in accordance with the legal frameworks. The CTIVD had previously identified points for adjustment in the underlying covenants to better reflect the monitoring practices. Once more, the CTIVD has called for additional attention to these points for adjustment. It is up to the organisations that are party to the covenant to follow through on these points. To date, no adjustments have been made to the existing cooperation agreements.

Convenant between the AIVD, MIVD and the Netherlands Bar Association (Nederlandse Orde van Advocaten, NOvA)

On 20 September 2023, the AIVD, MIVD and the Netherlands Bar Association signed the **Covenant on Caller ID and Confidential Numbers** (Convenant inzake Nummerherkenning Geheimhoudernummers).

This covenant sets out the agreements between the parties concerning the intelligence and security services' new number recognition system. With this new number recognition system, confidential numbers can be identified earlier and the associated data can be destroyed if there is no need for further processing.

The services will perform an initial audit of this system six months after its implementation and then test its performance thereafter on an annual basis. Once the CTIVD has received the results of this audit, it will take them into account when deciding which items to include in its oversight agenda.

2.5 Legal and regulatory advice

In 2023, the CTIVD participated in the preparation for, and parliamentary debate on, the Temporary Act on investigations by the AIVD and the MIVD into countries with offensive cyber programmes, bulk data sets and other specific provisions. The various components of the CTIVD's participation regarding the Temporary Act are described in Chapter 4. Further, this chapter explains the CTIVD's role in the preparations for the implementation of this Act. This chapter discusses the involvement of the CTIVD in transitional stipulates to establish a new retention period for the bulk data sets

not covered by the Temporary Act. Finally, we address the outline memorandum, submitted to the House of Representatives on 1 September 2023, for revising the ISS Act 2017 as well as the CTIVD's advisory role on the preparations for this revision.

2.6 Roundtable sessions

Roundtable sessions on hacking powers

On 9 May 2023, the Procurator General of the Public Prosecution Office at the Dutch Supreme Court (the Public Prosecutor's Office) and the CTIVD led a roundtable session on hacking powers. The roundtable session was prompted by the reports submitted by the **Justice & Security Inspectorate**, the **Research and Documentation Centre (Wetenschappelijk Onderzoek- en Documentatiecentrum, WODC)**, the **Public Prosecutor's Office** and the **CTIVD** that address hacking powers. Academics (primarily legal experts) who have written about hacking powers were also invited to attend the roundtable session. The aim of the roundtable session was for the attendees to exchange knowledge and learn from each other's experiences with hacking powers.

Roundtable session on intelligence activities

On 9 June 2023, the CTIVD held an **expert's meeting** entitled 'Proliferation of intelligence activities' (Wildgroei aan inlichtingenactiviteiten). This meeting focused on the collection and processing of intelligence by governmental authorities and organisations other than the AIVD and MIVD.

The reason for this meeting was the reporting by the NRC daily newspaper on '**undercover mosque visitations**' and the RTL News' coverage of the **Public Order Intelligence Team (Team Openbare Orde Inlichtingen, TOOI)**. Several reports have appeared on this kind of intelligence activity, such as a **report** by the Van Hulst Committee and the **report** of the Thorbecke Academy of NHL Stenden on intelligence activities on social media. The goal was to discuss this trend with experts and policymakers and to explore the potential measures to be taken.

Emeritus Professor Bob de Graaff (Utrecht University) and Professor Jan-Jaap Oerlemans (Utrecht University and CTIVD) gave introductory presentations to the attendees. After this, the participants — consisting of delegates from municipalities, academia, the Inspectorate of Justice and Security, the Netherlands Institute for Human Rights and a regional ombudsman — engaged in a robust discussion.

The conclusion of the meeting was that there are intelligence activities within a wide range of government bodies that can have a major impact on the parties involved. Participants agreed that intelligence activities should be carried out carefully and within the legal frameworks. This requires professionalism, administrative responsibility and awareness among government officials about the potential for the intelligence activities to impact the fundamental rights of the citizens and, by extension, their lives.

The CTIVD sees two important results from this meeting: it opened the discussion on how intelligence activities can impact citizens and it raised the awareness about this development.

Roundtable session on national security and partnerships

On 13 October 2023, the CTIVD organised an expert's meeting entitled 'National security and partnerships'.

The 'CT Infobox' and the 'Cyber Intel/Info Cell' (CIIC) are examples of the current formalised partnerships in the field of national security. The following parties work together in the CT Infobox and the CIIC partnerships: the AIVD, the Dutch National Police, the National Cyber Security Centre (NCSC), the Dutch Public Prosecution Service and the National Coordinator for Counterterrorism and Security (NCTV). Furthermore, there are other forms of cooperation, such as case discussions on security with parties like the municipalities or the police.

The expert's meeting focused on the tensions that arise when different domains, both legally and organisationally, converge or intersect within a partnership. Dr Constant Hijzen (Leiden University and the Inspectorate of Justice and Security) Prof Dr Jan-Jaap Oerlemans (Utrecht University and the CTIVD) gave introductory presentations for the meeting attendees. After these presentations, the attendees (being experts from diverse organisations) engaged in a wide-ranging conversations. Present at the meeting were lawyers, academics, privacy officers and staff from the National Police, the NCTV, the AIVD, the Public Prosecution Service, the FIOD/Tax and Customs Administration of the Netherlands, De Nederlandsche Bank, the municipality of The Hague and the Rotterdam-Rijnmond Ombudsman.

The legal bottlenecks and challenges for the oversight process were mapped out during the course of this meeting. This provided the CTIVD greater insight into the issues that arise in partnerships around national security. This may also provide focal points for future CTIVD investigations.

2.7 Consultations and dialogue

Consultations between the Dutch parliament, CIVD, departments and intelligence services

The CTIVD provides the Dutch parliament with explanations to its reports, often in the form of a technical briefing. The Standing Committees on Interior Affairs and/or Defence usually receive explanations on public reports during public sessions. The CIVD of the Dutch House of Representatives, however, discusses these confidential appendices in a closed session.

Aside from conducting various investigations, the CTIVD regularly holds consultations with the AIVD and MIVD along with the ministries of General Affairs, Interior Affairs and Defence. The senior officials of the ministries and the directors of the intelligence and security services also join in on periodic consultations. Staff from the CTIVD and intelligence and security services meet regularly to formally discuss a wide range of topics and make presentations to each other. These meetings are mutually beneficial. For example, the CTIVD contributes to and participates in the onboarding process for new recruits of the intelligence and security services, and the services present new developments in their field to the CTIVD. The intelligence and security services operate in highly dynamic fields. Certain programmes and projects of the services have a direct relation with the ISS Act 2017. Given this close connection, the CTIVD dialogues with the intelligence and security services to express its various positions.

Throughout 2023, the CTIVD participated in consultations for and provided oral and written input on the draft bill (for the Temporary Act) that addresses the AIVD and the MIVD's investigations into countries with offensive cyber programmes and the government's outline memorandum for revising the ISS Act 2017. This will be discussed in greater detail in Chapter 4.

Consultation with the Netherlands Court of Audit

The CTIVD held regular consultations with the Netherlands Court of Audit (Algemene Rekenkamer) in 2023. Under the Government Accounts Act (comptabiliteitswet), the Court of Audit is responsible for auditing the central government's revenues and expenditures and presenting its findings to parliament in its annual accountability audit. The president of the Court of Audit audits the classified expenditures of the AIVD and the MIVD. The Court of Audit also investigates the costs and effects (efficiency) of government policies. In 2023, the Court investigated the AIVD and MIVD and included its findings in its **annual report** of the same year. Within the context of this investigation and other areas of attention for the Court of Audit regarding the services' areas of operation, it is important that the CTIVD and the Court of Audit consult on the content and scope of their respective investigations.

Consultations with the Investigatory Powers Commission (TIB)

The TIB is an important conversational partner for the CTIVD. Under the ISS Act 2017, both organisations are tasked with ensuring legal coherence and consistent interpretation of the legal framework. These organisations also collaborate in other ways. See Chapter 5 for an in-depth examination of the ways in which the CTIVD and the TIB worked together in 2023.

2.8 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 organisation.

Internal and external critical input

The CTIVD sets great store by internal and external critical input in its oversight process. All CTIVD investigations are conducted by multidisciplinary teams made up of oversight officials with different areas of expertise. The CTIVD lays the groundwork for internal critical input by having members of staff who are not part of the relevant investigation group critically observe the investigation at hand.

External critical input is, where appropriate, 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.

Reflections from society and 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

After the publication of an oversight report, the CTIVD holds work-place conversations with the intelligence and security services to see how the report's findings and recommendations are received within their respective organisations. These conversations also cover whether the respective oversight report is sufficiently clear for the intelligence and security services' employees and whether the recommendations are feasible. For the CTIVD, these discussions are constructive because they contribute to improving its oversight tasks and the way it prepares its various 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 of the Complaints Handling Department

3.1 Handling complaints and reports of misconduct

Under the ISS Act 2017, the CTIVD's Complaints Handling Department is authorised to handle complaints about the actual or alleged conduct of the AIVD and/or MIVD. Due to this authorisation, the CTIVD's Complaints Handling Department acts as a so-called 'second-line' complaints handler. The ISS Act 2017 stipulates that any complaint against the AIVD or the MIVD must first be handled by the Minister concerned (as the first-line complaints handler). For the AIVD, this is the Minister of the Interior and Kingdom Relations; for the MIVD, it is the Minister of Defence. The AIVD and/or the MIVD carry out the actual complaints handling process. If a complainant is not satisfied with the Minister concerned's handling of his or her complaint, the complainant can file a complaint with the CTIVD's Complaints Handling Department. In some cases, the CTIVD's Complaints Handling Department will directly handle complaints because the complainant cannot reasonably be expected to file his or her complaint with the Minister concerned first.

The Complaints Handling Department is also authorised to handle reports of suspected wrongdoing.

3.2 Complaints handled by the Complaints Handling Department of the CTIVD

The following is a summary of how many complaints the CTIVD's Complaints Handling Department processed in 2023.

CTIVD	Complaints about AIVD	Complaints about MIVD	Other complaints[1]
Pending on 1 January 2023	3	0	-
Complaints received	21	7	16
Declared unfounded	3	0	-
Declared partially well-founded	-	-	-
Declared entirely well-founded	-	-	-
Handled informally[2]	4	4	

[1] For the remaining complaints, it was unclear whether the complaint pertained to the AIVD and/or the MIVD, and the complainant did not provide clarity or additional clarity.

[2] When a complaint is informally settled, this means that the complaint has been resolved to the complainant's satisfaction without the need to conduct a formal investigation of the complaint. This could include, for example, an intervention in which the intelligence service is asked to respond to a message from the complainant or to provide an appropriate solution.

CTIVD	Complaints about AIVD	Complaints about MIVD	Other complaints[1]
Not handled[3]	11	-	16
Forwarded to the Minister[4]	3	3	-
Repealed	-	-	-
Pending on 31 December 2023	3	-	-

In total, the CTIVD's Complaints Handling Department processed four complaints in 2023; three of which it already had under review by 1 January 2023. In three cases, this resulted in a formal decision by Complaints Handling Department, which was subsequently published anonymously on the website of the Review Committee on the Intelligence and Security Services. One complaint that had been handled was not published. In three other cases, the complaints handling had not been completed by 31 December 2023.

Decision after investigation

Decision of 1 May 2023

The complainant had filed a complaint against the AIVD, alleging that he had been followed by individuals on different occasions, whom he believed were from the AIVD, and who were collecting information about him that was being passed on to other parties. The complainant was given an opportunity to explain his complaint orally. In the course of handling this complaint, the Minister noted that the AIVD could not disclose whether special investigatory powers (e.g. surveillance) had been deployed in his case. This observation, however, was not communicated to other parties who had complained about the use of the special investigatory powers. The Minister points out that if a person does not engage in activities that could harm national security, the General Intelligence and Security Service will not pay attention to him or her. In the complainant's view, the AIVD had not conducted the investigation into his complaint properly. After reviewing the AIVD's complaints file, the CTIVD concluded that its investigation had been thorough, contained no erroneous information and that everything in the file had been meticulously documented. The complaint is unfounded.

Decision of 2 August 2023

The complainant filed a complaint about the contacts between the complainant and the employees of the Internal Security Service (Binnenlandse Veiligheidsdienst, BVD), the predecessor to the AIVD. The complaint has been declared unfounded. The complainant's relatives filed a complaint with the Complaints Handling Department because, based on the recently disclosed file on the complainant, they believed that BVD staff had more contact with the complainant during the complaints handling process than the AIVD had assumed. During the investigation, the Complaints Handling Department found no indications that there had been other contacts between BVD employees and the complainant beyond those identified in the complaints

[3] There are various reasons for not taking a complaint into handling. Examples include, but are not limited to, the following: the complaint does not pertain to the AIVD and/or the MIVD, the complaint does not concern a subject which the Complaints Handling Department is authorised to adjudicate, the complaint is a repeat complaint, the complaint was not addressed first by the Minister concerned, or the complainant failed to respond to the CTIVD's request for additional information.

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

investigation conducted by the AIVD and documented in the complainant's personal file. The complaint is unfounded.

Decision of 22 November 2023

The complainant filed a complaint against the AIVD. This complaint has been declared unfounded. The letter states, as in the case that led to the 1 May 2023 decision, the Minister cannot disclose whether special investigatory powers were deployed in his case. This observation, however, was not communicated to other parties who had complained about the use of the special investigatory powers. The Minister points out that if a person does not engage in activities that could harm national security, the General Intelligence and Security Service will not pay attention to him or her.

The complainant filed a complaint with the Complaints Handling Department alleging that the AIVD had carried out attacks on his life and harassed him by hacking into his computer.

Upon investigation, the Complaints Handling Department found no evidence to suggest that the information contained in the Minister's letter was incorrect. The Complaints Handling Department has ruled that the complaint regarding attacks upon a person's life is manifestly unfounded because the AIVD does not use this method and there is no doubt about that conclusion. The decision also states that the AIVD did not deploy special investigatory powers (e.g. hacking) unlawfully.

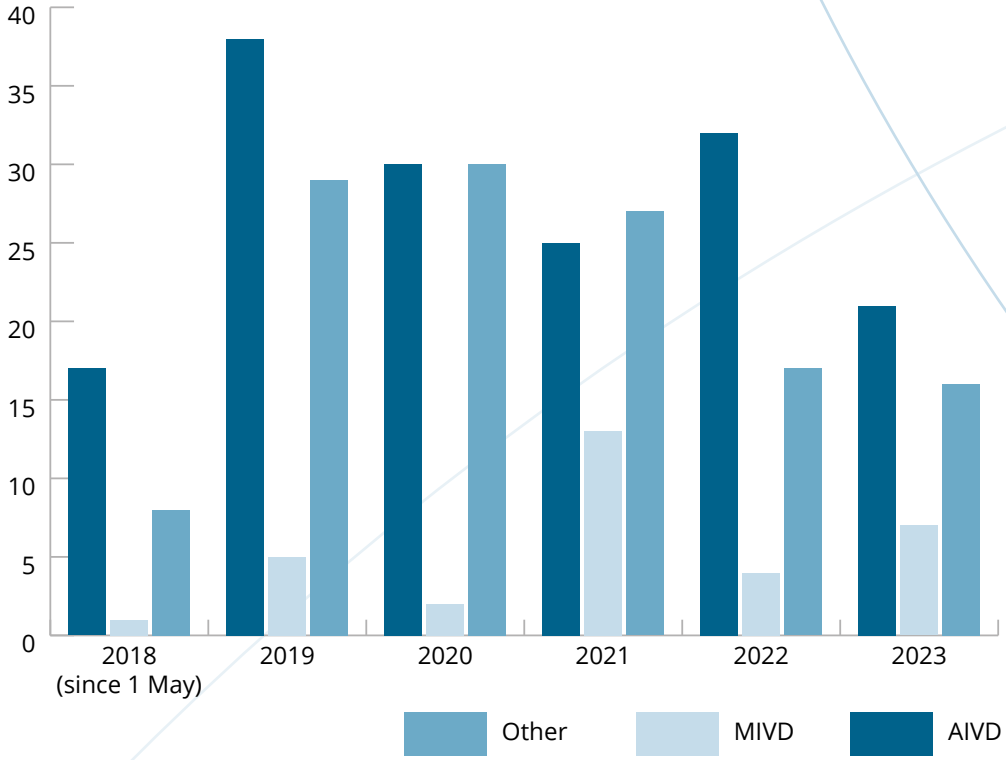
The complaint decisions are anonymised and made available for consultation on the CTIVD website.

Complaints handled informally

Finally, the CTIVD's Complaints Handling Department was able to informally settle four complaints filed against the AIVD and four against the MIVD. The majority of the complaints concerned the processing times of security screening. Through informal channels, the Complaints Handling Department has urged timely communication to those involved regarding the lengthy processing times and, where possible, expedited the completion of the security screening. In all cases, this was handled to the complainant's satisfaction. Therefore, further consideration of the complaint was no longer necessary.

3.3 Complaints about oversight received since 1 May 2018

Since the introduction of the ISS Act 2017, the CTIVD has received a fairly stable number of complaints.



3.4 Interventions in security screening

The Complaints Handling Department has intervened several times to find solutions for complainants who have had to wait for prolonged periods or for an excessive length of time, for their security screening to be completed. There have been delays of more than a year.

The interventions involved requesting the respective service, the AIVD or the MIVD, to contact the individual under investigation. The Complaints Handling Department had proposed deadlines of up to two weeks for contacting this individual. Furthermore, the Department requested that thereafter, in case of further security screening delays, the person in question should voluntarily be kept regularly informed. On a number of occasions, the Department has insisted that a decision be issued quickly. This was also a negative decision (refusal of the security clearance, in Dutch: verklaring van geen bezwaar, VGB), but it gave the individual and opportunity to initiate an objection and appeal procedure.

In 2023, the services' joint Security Screening Unit (Unit Veiligheidsonderzoeken, UVO) sent a letter to those waiting on their security screening, informing them that the screening would take another nine months. Initially, the relevant individuals only received that letter after the deadline for the screening (eight weeks) had already been greatly exceeded (by up to five months). Due to that, these individuals inferred from that letter that the screening process would take more than a year.

The lengthy duration also affected the relationship between these individuals and their employer (in many cases, the Ministry of Defence). Several individuals who had filed a complaint with the CTIVD reported that, as a result, they had been unable to undergo training or to start a new (promotional) position, with some even facing suspension as employees.

On **1 November 2023**, the Complaints Handling Department raised concerns with the Defence Minister about the processing times of the security clearance requests. In response, the Minister stated that measures had been taken.

On 21 December 2023, the chair of the Complaints Handling Department spoke with the director of the Security Screening Unit and the deputy director for an overview of the nature and extent of the issues with turnaround times of the screening. The UVO itself was found to have received only two complaints during the period from 1 January 2023 to 1 December 2023.

These consultations led to follow-up discussions in 2024 with the UVO and the complaints officers of both services. The intelligence and security services, which do receive complaints, and the UVO now have frequent contact about resolving and possibly preventing the complaints. The UVO reports that they are doing everything possible to reduce the backlog.

3.5 No reports of suspected misconduct

The ISS Act 2017 contains a procedure for reporting suspected misconduct to one of the intelligence and security services or to the Coordinator of the Intelligence and Security Services. These kinds of reports can also be submitted to the Complaints Handling Departments of the CTIVD. Anyone who is or has been involved in the implementation of the ISS Act 2017 or the Security Screening Act can report suspicions of misconduct to the Complaints Handling Department. Before contacting the Complaints Handling Department, the party reporting the suspected misconduct must first notify the relevant intelligence service. If the service in question fails to handle this report properly or within a reasonable timeframe, the reporting party may contact the Complaints Handling Department of the CTIVD.

If the Complaints Handling Department finds indications for suspicions of misconduct, it will proceed with the report in question. The Department will then assess whether there are plausible grounds for the misconduct described. The reporting party and the Minister concerned are given an opportunity to explain their position. Following its investigation, the Complaints Handling Department will write a report. The Department will communicate its ruling to the reporting party and the Minister concerned, and may provide recommendations to said Minister. Next, the Minister will explain how he or she will respond to the Department's ruling and within which time frame. The Minister concerned then sends the Complaints Handling Department's ruling together with his or her response to this ruling to parliament. The CTIVD publishes an anonymised report about the alleged suspicions of misconduct it reviewed on its website.

In 2023, no reports of suspected misconduct were filed with the CTIVD's Complaints Handling Department. No suspicions of misconduct were reported in previous years either. Two reports of suspected misconduct were filed at the beginning of 2024.

3.6 Complaints and reports of alleged misconduct handled by the AIVD and the MIVD

Complaints handled by the AIVD and the MIVD

Complaints can be submitted to the Minister concerned. For the AIVD, this is the Minister of the Interior and Kingdom Relations; for the MIVD, it is the Minister of Defence. The actual complaints handling resides with the AIVD and the MIVD. If the complainant is not satisfied with the outcome of the internal complaints handling process, he or she can file a complaint with the CTIVD's Complaints Handling Department. The first step in filing a complaint is to submit it to the Minister concerned, unless this cannot reasonably be expected of the complainant.

Below is an overview of the numbers of complaints processed by both services in 2023.[5]

Intelligence and security services	AIVD	MIVD
Pending on 1 January 2023	4	6
Complaints received	26	40
Declared unfounded	8	4
Declared partly well-founded	4	-
Declared well-founded	-	11
Handled informally[6]	8	1
Not handled[7]	4	1
Repealed	-	12
Referred[8]	-	7
Pending on 31 December 2023	6	10

Reports of alleged misconduct handled by the AIVD and MIVD

No alleged misconduct was reported to either intelligence service in 2023. The lack of reports of alleged misconduct in recent years has caught the attention of the CTIVD's Complaints Handling Department. The CTIVD's Complaints Handling Department had requested additional attention for this issue in 2022. The Complaints Handling Department continues to draw attention to this. Two reports of alleged misconduct were filed with the CTIVD at the beginning of 2024.

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

Since the introduction of the ISS Act 2017, the Legal Affairs departments of the AIVD and the MIVD (as first-line complaints handlers) and the CTIVD (as a second-line complaints handler) have held regular consultations about the procedures for and the implementation of the complaints procedure in practice. The implementation

---

5 The figures were submitted by the AIVD and the MIVD.

6 'Informally settled' means that a satisfactory solution has been found for the complainant without the need for a formal complaints handling procedure.

7 This situation may arise, for example, if the complaints body is not authorised to handle the complaint or if an objection or appeal procedure is simultaneously pending before the court on the same issue.

8 Referred complaints involve the submission of a complaint to the wrong body. In consultation with the complainant, the complaint will be forwarded to the appropriate body.

is assessed, ex officio or otherwise, by the Complaints Handling Department when dealing with complaints filed with the department. In addition, attention is paid to trends in the numbers and nature of complaints received. Both services provide periodic lists of the complaints that they have or have not taken into handling. This is how the Complaints Handling Department monitors both the developments in front-line complaint resolution and reporting procedures and how they are implemented in the intelligence and security services.

4



New regulations

Temporary Act on investigations by the AIVD and the MIVD into countries with offensive cyber programmes, bulk data sets and other specific provisions

In 2023, the CTIVD was also intensively involved with the draft bill concerning the AIVD and MIVD's investigations into countries with offensive cyber programmes (known in full as the Temporary Act on AIVD and MIVD investigations into countries with offensive cyber programmes, bulk data sets and other specific provisions, hereafter : 'Temporary Act', [Parliamentary Paper 36 263]), which lay before the Dutch House of Representatives at the time and the corresponding amendment memorandum.

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 characterised 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*.

Any legal framework that affords the intelligence and security services greater leeway for coping with the dynamic and unpredictable nature of cyber threats requires an oversight system that effectively monitor this their activities, without scaling down the associated safeguards. The relevant legislation should provide for a system of *checks and balances* that respects both the interests of national security and the protection of fundamental rights.

A draft bill for the Temporary Act went into public consultation on 01 April 2022. In April 2022, the CTIVD sent a **letter** to the Minister of the Interior and Kingdom Relations containing its response to the draft bill. From the perspective of oversight, the CTIVD agreed with the principles of the Temporary Act, apart from a few concerns. The draft bill was submitted to the Dutch House of Representatives in December 2022.

By 2022's end, a draft amendment memorandum had been prepared that addressed two amendments to the draft bill. The amendments concerned a regulation for the so-called 'silent tap' (a special investigatory power for collecting *real-time* traffic and location data, i.e. not the content of the communications) codifying case law of the European Court of Justice and a regulation for assessing the extension of the retention period for bulk data sets collected by exercising special investigatory powers. The draft proposal of the Temporary Act already contains a regulation for assessing bulk data sets, in so far as these fall within the scope of the Temporary Act. The draft amendment memorandum also contains a regulation for bulk data sets. This regulation, however, is largely identical to that of the Temporary Act, albeit with a broader scope of application, to wit, all of the special investigatory powers (excluding investigation-related interception).

The CTIVD attended meetings about the memorandum of amendment being prepared. On 16 January 2023, the CTIVD dispatched a **letter** to the Minister of the Interior and Kingdom Relations in response to the draft amendment memorandum released for consultation in December 2022. The draft amendment memorandum was submitted to the Dutch House of Representatives in September 2023.

In its response, the CTIVD stated that it considers the two proposed changes in the amendment memorandum a positive development and that it supports them. These amendments to the Temporary Act will strengthen the oversight system and render it far more effective. They will also rectify a number of imperfections in the ISS Act 2017 that were previously flagged by the CTIVD. The result will be enhanced protection of both national security interests and fundamental rights.

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.

On 30 March 2023, the CTIVD and TIB participated in a technical briefing on the draft bill before the Dutch House of Representatives.

On 29 August 2023, the CTIVD sent a **letter** to the House of Representatives' Parliamentary Standing Committee on Interior Affairs.

This letter expressed the CTIVD's concerns about the progress made thus far on the Temporary Act. Based on its findings, the CTIVD has stressed on several occasions that a more tailored exercise of existing investigatory powers (the draft bill does not create new powers as such) is necessary to adapt to the dynamic practices in the cyber domain and thus ensure national security. The draft bill provides for a much better balance between the importance of national security and the importance of safeguarding fundamental rights. As regards data processing, where the risks are greatest, the bill also provides for the oversight body to issue binding decisions on the lawfulness of said processing. Moreover, the court has been assigned an independent

role and its decisions will, in principle, be public. In its letter, the CTIVD calls on the House of Representatives to consider the proposed Temporary Act as soon as possible.

The House of Representatives passed the draft bill for the Temporary Act in November 2023. After which, it was submitted to the Senate for consideration. In December 2023, the CTIVD took part in a technical briefing on the draft bill before the Senate. The Senate passed the draft bill in March 2024.

The transitional stipulates for bulk data sets in the Temporary Act

The ISS Act 2017 stipulates that data collected by exercising a special investigatory power should be examined soon as possible, but no later than within eighteen months for their relevance to the investigation for which they were collected. Once this period has expired, any data declared irrelevant must be destroyed. The MIVD and the AIVD possess bulk data sets whose relevance assessment period is nearing expiration, and upon the expiration of this period, these sets must be destroyed.

There are a very small number of these bulk data sets (relating to investigations abroad) for which the services consider that there are urgent national security reasons for prolonging the use of these data sets. The current legal framework, however, does not foresee a basis for prolonging the use of these sets. The CTIVD, the Evaluation Committee on the ISS Act 2017 and the Court of Audit have previously recognised the issues associated with assessing the relevance of bulk data sets and prolonging their usage.

During the House of Representative's parliamentary debates on the draft bill for the Temporary Act of 16 October 2023 (Parliamentary Paper **36 263, No 35**), MP Rajkowski (VVD party) was promised that there would be a meeting with oversight bodies about a potential solution for bulk data sets, of which, in short, the legal period for the relevance assessment expires prior to the possible entry into force of the Temporary Act.

In a **letter** (Parliamentary Paper 36 263, No 36), the Minister of the Interior and Kingdom Relations and the Minister of Defence informed the House of Representatives about the results of their consultation with the CTIVD, as the issue at hand primarily concerns the CTIVD's general oversight of lawfulness. The TIB was informed at a later stage about the agreements that had been concluded with the CTIVD.

During these discussions, the CTIVD stated that, on the basis of its review task, it considers it acceptable, under certain conditions and taking into account the need for national security, to process the relevant bulk data sets in accordance with the provisions of the Temporary Act. In so doing, the CTIVD took into account that the Temporary Act offers concrete prospects for a legal regulation that will ensure sufficient safeguards for the handling and processing of these bulk data sets. Bulk data sets that, in the context of national security, are no longer necessary, will be destroyed after the expiry of the deadline.

This regulation entails, in brief, that the director of the relevant intelligence service may, with a view to urgent reasons of national security, submit a substantiated request to the Minister concerned to establish a new deadline, of no more than a year, for using the bulk data set, and that the CTIVD can then judge whether this new deadline has been justified. The Ministers will then comply with the CTIVD's ruling. It is not possible to lodge an appeal with the Administrative Jurisdiction Division of the Council of State before the Temporary Act enters into force.

Agreements have been made with the CTIVD about the following additional safeguards:

- The House of Representatives will be informed immediately after the Minister concerned has established a new deadline for a bulk data set and the CTIVD has exercised binding oversight.
- Once the Temporary Act has entered into force, the director of the intelligence service concerned will re-submit a request to the respective Minister to establish a new deadline for the use of the bulk data set. From that moment forward, a single regime will be established for the lawful use of bulk data sets collected through the use of a special investigatory power.
- Should the Senate not pass the draft bill, the bulk data sets that have been assigned a new deadline will still be immediately destroyed.

Implementation of the Temporary Act

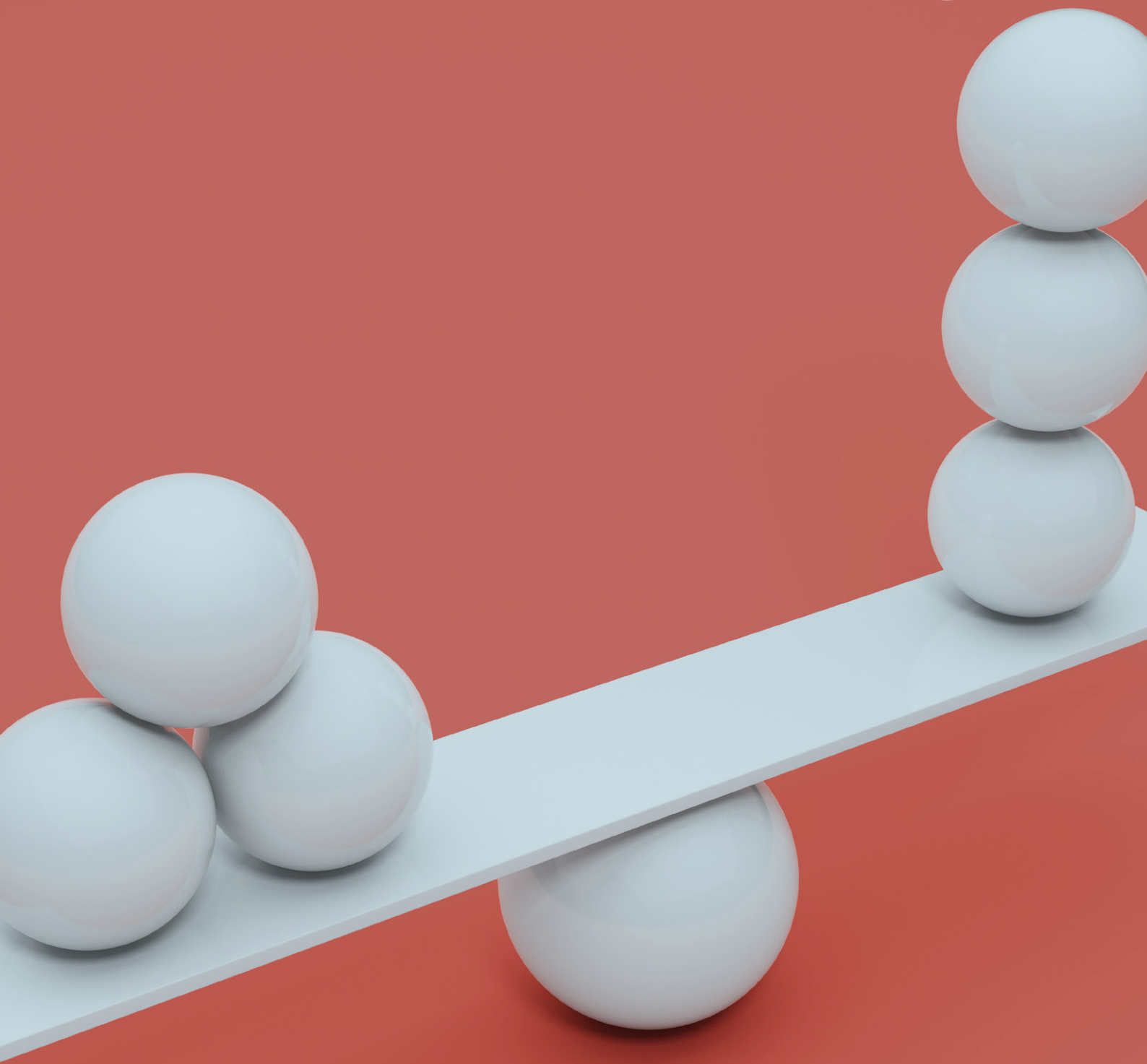
Not only did the CTIVD's participation in the preparation and handling of the draft bill for the Temporary Act require significant attention in 2023, the preparation for the implementation of the draft bill pertaining to the CTIVD's own procedures and working methods given priority and thus required considerable capacity. The CTIVD thus anticipated parliamentary approval of the draft bill; however, given the expansion of its range of tasks, the anticipated impact on the organisation and the required preparation time, the CTIVD could not wait until the Act came into effect. It became clear in March 2024, however, that the Senate had approved the draft bill. The Act will enter into force on a date to be determined.

The CTIVD has established an internal steering group that is structurally responsible for preparing the implementation of the Act. This preparation involves drafting assessment frameworks, procedures for internal decision-making and external escalation, procedures for reporting, justification and the appeals process before the court. The work to prepare for the implementation of the Act will continue in 2024.

Review of the ISS Act 2017

2023 also saw the CTIVD participating in discussions about the preparation of the government's outline memorandum on revising the ISS Act 2017. The outline memorandum describes the general framework and principles for this legislative revision. On two separate occasions, the CTIVD has submitted extensive views in writing on the draft versions of the outline memorandum to the Ministry of the Interior and Kingdom Relations, which has a leading role for this revision. This input was partly followed up in the final **outline memorandum** submitted to the House of Representatives on 1 September 2023.

5



Monitoring the legal coherence of the Act and the cooperation with the TIB

Legal coherence consultation

The TIB and CTIVD hold regular consultations to harmonise their legal interpretation of the ISS Act 2017. They refer to this as the 'legal coherence consultation'. In accordance with the legislative history, both of these bodies have the task of seeking coordination where necessary and monitoring legal coherence. The legal coherence consultation prevents the same legal provision from being interpreted in different ways. This not only serves the legal certainty of citizens, providing them with greater insight into the scope and application of the AIVD and the MIVD's use of special investigatory powers, It also provides the AIVD and the MIVD with clarity about the legal framework that applies to the performance of their tasks.

The legal coherence consultation, however, did not result in the issuance of a so-called 'legal coherence letter' in 2023. Both bodies have regular consulted one another about the respective topics from the ISS Act 2017 that impact them.

Draft bill: Temporary Act on investigations by the AIVD and the MIVD into countries with offensive cyber programmes, bulk data sets and other specific provisions

Just like previous years, the Temporary Act continued to be an important topic in 2023 (see Chapter 4). At several points in 2023, the CTIVD and the TIB consulted departments and the intelligence services on this draft bill for the purpose of parliamentary debate. Both bodies (the CTIVD and TIB) have had close contact and consultation on the Temporary Act.

Joint letter concerning rapid ratification of Convention 108+

On 13 July 2023, the TIB and the CTIVD drafted a **joint letter** about Convention 108+ to the Minister of the Interior and Kingdom Relations (with a copy provided to the Defence Minister and the chairs of the Dutch Senate and House of Representatives).

In this letter, the TIB and the CTIVD call for the Approval Act for this treaty to be presented to parliament as soon as possible and for the treaty to be ratified. They request that the Ministers act in accordance with the Treaty until this law has been passed.

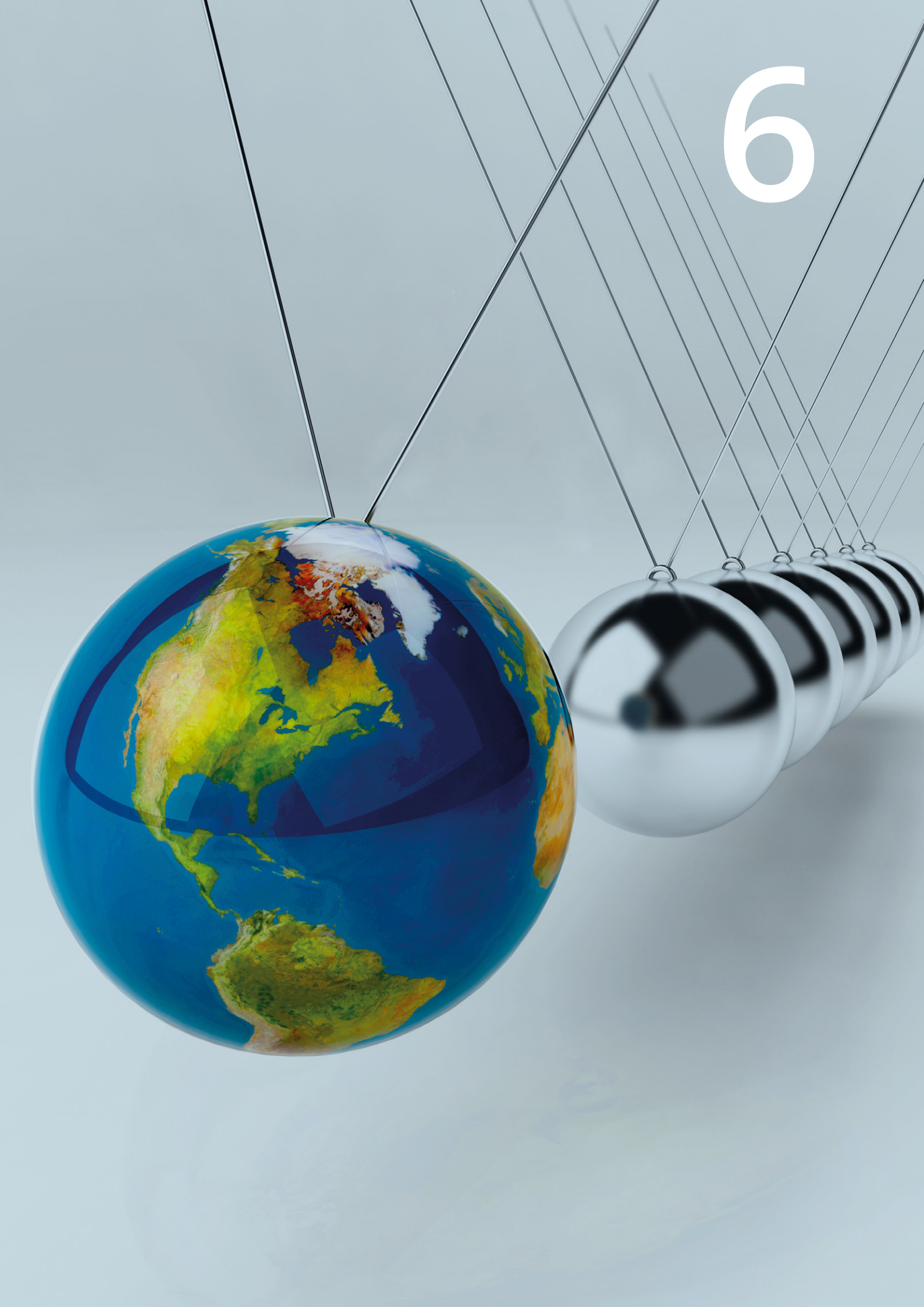
Convention 108, a 1981 Council of Europe treaty, laid the foundation for the protection of personal data. **Convention 108+** will renew this earlier treaty. The treaty does not provide an exception for national security, unlike, for example, the European Union's General Data Protection Regulation.

In 2021, the TIB and the CTIVD drafted a joint **memorandum** outlining the treaty's implications for the monitoring of personal data processing in the context of national security.

The TIB and the CTIVD made this appeal partly in response to the recommendations recently issued by the PEGA Committee of the European Parliament. The PEGA Committee investigated the use of Pegasus and similar spyware. Based on these investigation findings, the European Parliament's **recommendations** urge all member states to promptly ratify the treaty and transpose its standards into national law, acting accordingly in the field of national security.

The chairs of the TIB and the CTIVD have both been heard by the PEGA Committee (see the hearings of the **TIB** and **CTIVD** and the transcript of the input from the **TIB** and the **CTIVD**).

6



International cooperation

The cooperation between the intelligence and security service is not only intensifying, it is also becoming more innovative. International cooperation is a vital tool for these intelligence services to protect the national security of their respective countries. There is also growing cooperation when it comes to oversight.

Oversight Working Group (IOWG)

The CTIVD works closely with seven other European oversight bodies in a partnership known as the *Intelligence Oversight Working Group* (IOWG), which shares best practice in oversight and consults on topical issues affecting all the bodies. The IOWG meets twice a year.

In late May 2023, the CTIVD organised and hosted a conference in The Hague with the participating oversight bodies from the IOWG.

In early November 2023, the CTIVD held discussions among the administrative officials and chairs of the participating oversight bodies from the IOWG. The conference meetings were held in Oslo, Norway.

European Intelligence Oversight Conference (EIOC)

Following the meetings of the IOWG in November 2023, the annual *European Intelligence Oversight Conference* was also held in Norway. This edition of the conference was organised by the oversight body of the Norwegian Parliament, together with the oversight bodies from Sweden and Denmark.

International Intelligence Oversight Forum (IIOF)

In late November 2023, the CTIVD participated in the annual *International Intelligence Oversight Forum* (IIOF) held in Washington, DC. The IIOF is organised by Prof Joseph Cannataci, former UN rapporteur on the right to privacy and former rapporteur for the Council of Europe under Convention 108+.

The IIOF aims to be a platform for international oversight bodies that monitor intelligence and security services and privacy and data protection, as well as other stakeholders, such as intelligence and security services, to discuss national and international developments and sector *best practices*.

The CTIVD combined this conference with working visits to several organisations in the intelligence and oversight community of the United States and Canada.

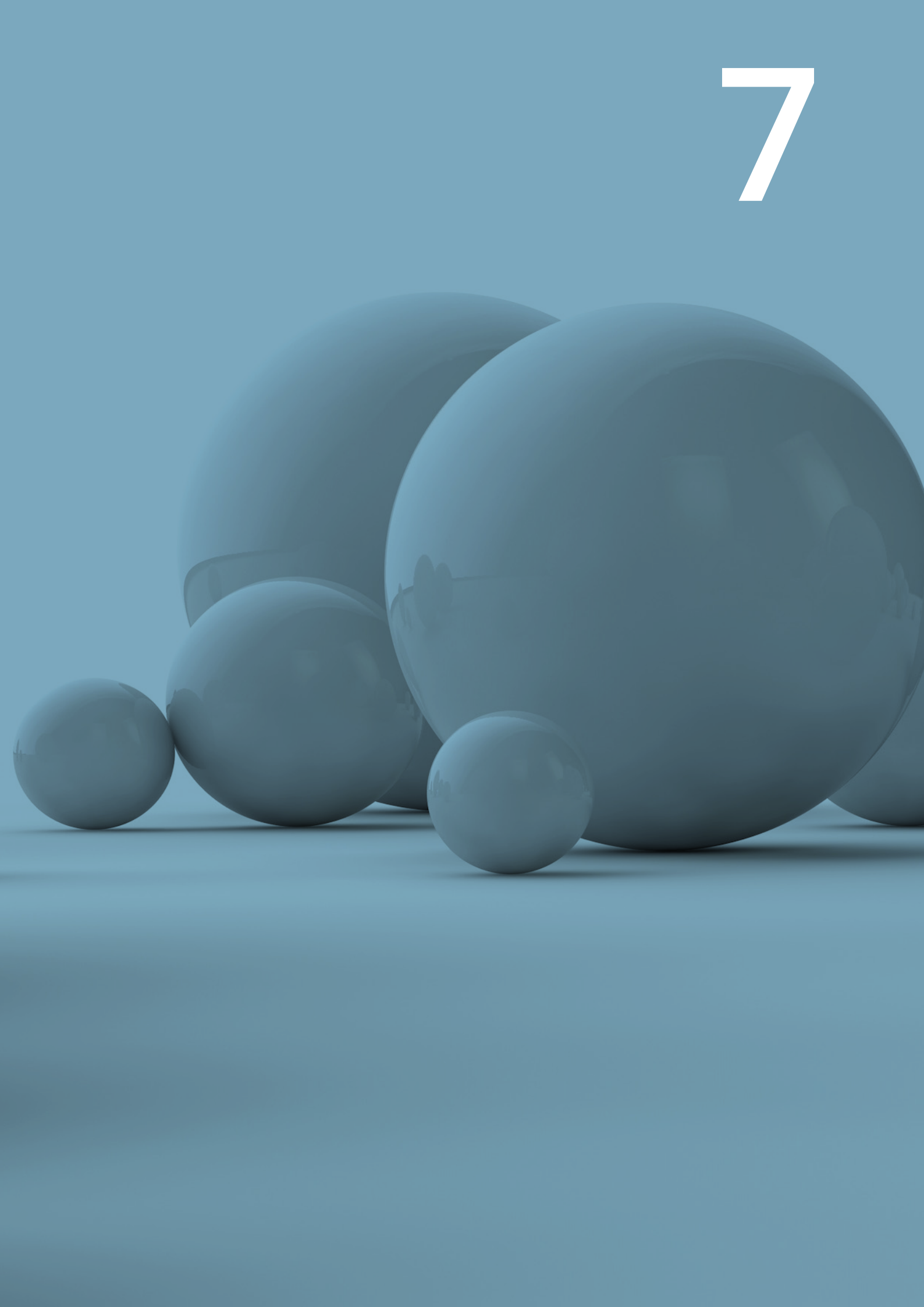
Other contacts

The CTIVD also maintains various bilateral contacts with other oversight bodies.

In September 2023, at the request of the Norwegian oversight body, CTIVD staff gave an online presentation on conducting interviews as an investigative methodology.

In October 2023, the CTIVD participated in a meeting, hosted by the AIVD, for delegates of the **European Union Advisory Mission** for Civilian Security Sector Reform in Ukraine - Civilian Mission (EUAM Ukraine). The mission delegates are a group of international experts from Europe, established at the request of the Ukrainian government in 2014, to advise it on reforming government and law enforcement agencies.

7



Organisational development

Organisational structure of the CTIVD

The CTIVD is divided into two different departments. In 2023, the Oversight Department consisted of Nico van Eijk (chair), Harm Trip and Judith Lichtenberg. That same year, the Complaints Handling Department consisted of Addie Stehouwer (chair), Hermine Wiersinga (committee member up to 1 December 2023), Anne Mieke Zwaneveld (committee member up to 1 April 2023), Erik Kok and Peter Muijen (committee member starting on 1 November 2023). Nico, Harm, Judith and Addie are also members of the CTIVD. As of 4 March 2024, Nico van Eijk has **stepped down** as committee chair and Herman Bolhaar has been appointed as the interim chair.

Both departments are supported by the secretariat. The CTIVD staff is managed by the secretary-director and consists of legal, technical and operational supervisors and two support staff.

Expansion of personnel

Since 2022, the CTIVD has been promised additional staffing (10 FTE) to prepare for the expansion of its duties under the Temporary Act on investigations by the AIVD and MIVD into countries with offensive cyber programmes, bulk data sets and other specific provisions (see Chapter 4 for additional information). Due to insufficient office space, the CTIVD is unable to accommodate the expansion of its personnel .

The offices of the CTIVD

Although the promised staff extension made in view of the additional tasks for the CTIVD under the Temporary Act included a commitment to provide the necessary workspace, this has not been realised in 2023. Since 2022, the CTIVD has been in intensive talks with the parties concerned about the necessary expansion of its current offices and explorations into relocating the organisation. This process continued through 2023 but did not result in a solution, so it will continue in 2024.

Facility developments

Administratively, the CTIVD is under the purview of the Dutch Ministry of General Affairs (Ministerie van Algemene Zaken). This means that the CTIVD can rely on the Ministry for such services as financial management, ICT and human resources.

The CTIVD itself, however, decides on the expenditure of its financial resources. The CTIVD has a budget of approximately €4 million.



P.O. Box 85556
2508 CG The Hague

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