

Annual report

2021



Review Committee
on the Intelligence and
Security Services

Disclaimer: This is not an official translation. No rights may be derived from this translation and under all circumstances the Dutch text of this report prevails.

Annual report

2021



Review Committee
on the Intelligence and
Security Services

Preface

Oversight of national security is not a given, and nor should it be. Invoking national security means invoking an exception. Under such an exception, far-reaching investigatory powers may be called upon – investigatory powers that are not normally available in criminal law or data protection legislation. Another factor is that anything undertaken within the context of national security is almost always subject to strict secrecy. Those are compelling reasons why national security in a democratic society should be firmly and unambiguously embedded in legislation and subjected to special oversight.

The Intelligence and Security Services Act 2017 (ISS Act 2017) is primarily the mainstay of two specific organizations involved in national security: the AIVD and the MIVD. The tasks and the oversight of both organizations are regulated by that piece of legislation. In a number of areas, the ISS Act 2017 goes further. For example, the Act also regulates the coordination of both services' activities, which overlap with other organizations and tasks in the area of national security. The review and complaint departments of the CTIVD are authorized to review the Security Screening Act and to review the minister of Justice and Security's authority to revoke Dutch citizenship in the interest of national security.

The number of organizations and tasks relating to national security is broader than those covered by the ISS Act 2017. Internationally, this calls for a holistic approach to national security. The lack of such an approach in the Netherlands presents challenges which have recently come to the forefront in public debate. Where it concerns investigatory powers and safeguards, the revision of the ISS Act 2017 and other legislation touching upon national security should be consistent and permanent. During 2021, the CTIVD has regularly called attention to this point of view and will continue to do so in the coming period.

Consistency and permanency also apply to how the oversight itself is set up. For this reason, during the evaluation of the ISS Act 2017, the CTIVD argued in favour of integrated oversight with binding investigatory powers, to satisfy both the interest of national security (the services' effectiveness, protecting the constitutional state) and the fundamental rights.

The CTIVD does not consider its procedure a given, as has become clear over the years. In its review activities, which include in-depth investigations and the resulting publication of reports, there is an increasing focus on oversight that fits in with the larger dynamic required to protect national security. Within the domain of national security, the amount of data that needs to be processed has massively increased and calls for ever faster processing. The CTIVD's efforts are geared towards preventing unlawful conduct in dialogue with the services and towards near-real time review and system review. This annual report explains how those review activities are conducted. The activities include monitoring the weighting process of whether to report unknown vulnerabilities and the service provided to special bodies in the case of digital attacks. A lot of time has been spent on the issues concerning the special investigatory power to collect and process investigation-related data.

In addition, more use is being made of the flexible instrument of so-called 'information files', whereby questions on a specific subject are asked and answered in writing. This ultimately leads to findings being established, after which further agreements can then be made with the services. Another outcome of the information files could be that an in-depth investigation needs to be set up.

A further important development in review is aimed at professionalizing internal compliance. For the services, effective compliance is essential to remaining in control in a growing organization and in the face of increasing complexity. For the oversight body, effective compliance is essential to being able to exercise effective and efficient oversight. By being involved in setting up internal compliance and using random tests to check if the internal rules are actually being adhered to, the services can ensure that the safeguards are indeed effective in practice. We are pleased to note that setting up the necessary preconditions, which we had previously addressed in our progress reports about the implementation of the ISS Act 2017, has not only been given higher priority but is also now being bolstered by additional budgetary resources.

Achieving a consistent approach to national security and the corresponding robust and permanent system of oversight will be necessary to safeguard the interests of the constitutional state and its citizens, particularly in a time when these are being tested.

Nico van Eijk
CTIVD Chair



Table of contents

1	Introduction	7
2	Activities of the Oversight Department	9
2.1	Lawfulness investigations completed in 2021	9
2.2	Ongoing investigations in 2021	11
2.3	Other activities and publications in 2021	12
2.4	Safeguarding the quality and effectiveness of oversight	16
3	Activities by the Complaints Handling Department	19
3.1	Handling complaints and reports of misconduct	19
3.2	Complaints handling by the CTIVD in 2021	19
3.3	Reports on alleged misconduct submitted to the CTIVD in 2021	21
3.4	Complaints and reports of alleged misconduct handled by the AIVD and the MIVD in 2021	22
4	New legislation	25
5	Preserving legal uniformity and cooperation with the TIB	27
6	International cooperation	29
7	Organizational developments	31



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 about the complaints**.

Every year, before 1 May, the CTIVD publishes an annual report which is submitted to Parliament and to both the Minister of **Internal Affairs 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 2021 Annual Report.

Structure of the report

The report focuses on the following topics: Sections 2 and 3 detail the activities carried out by the CTIVD's Oversight Department and Complaints Handling Department in 2021. Section 4 looks at the preparation for new legislation on investigations into countries with an offensive cyber programme. Section 5 discusses the legal uniformity meetings and cooperation with the Investigatory Powers Commission (TIB). Section 6 addresses the cooperation between the CTIVD and the oversight bodies of foreign intelligence and security services. Finally, section 7 describes the composition of the CTIVD in 2021.

2



Activities of the Oversight Department

2.1 Lawfulness investigations completed in 2021

The CTIVD conducts lawfulness investigations into matters including 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 2021. The first is review report no. 72 into the use of investigatory powers to support a proper execution of the AIVD and MIVD's tasks. The second review report is no. 73 into the provision by the AIVD and the MIVD of personal data to foreign intelligence and/or security services with an increased risk profile. An overview of the main findings is given below. The review reports may also be accessed through the CTIVD website.



No. 72 | Investigation into the use of special investigatory powers to support a proper execution of the AIVD and MIVD's tasks

Adopted on 24 February 2021, published on 15 April 2021

The CTIVD investigated whether in the investigation period (May 2018 - November 2019) the AIVD and the MIVD lawfully applied the investigatory power under Section 28(2) of the ISS Act 2017 and whether they complied with the duty to notify under Section 30(1) of the ISS Act 2017.

The review report focuses on a new element in the Intelligence and Security Services Act 2017: the option to use special investigatory powers to support a proper execution of the AIVD and MIVD's tasks. This could constitute an assessment regarding the necessity of taking special security measures for a service staff member or other person working for the services, or it could be a reliability investigation into a source.

The legislator has included additional safeguards in the law for the use of these special investigatory powers to support the execution of the services' tasks. In brief, these safeguards are: authorization by the minister concerned, the authorization period shortened to four weeks and the requirement that the services immediately notify the CTIVD of any authorization granted by the minister concerned.

The CTIVD concludes that in the investigation period both services applied Section 28(2) lawfully in the cases investigated by the CTIVD. In two cases, both the AIVD and the MIVD used the special investigatory power without basing that use on Section 28(2) while in the CTIVD's opinion that ground was applicable. Nevertheless, the use

of the investigatory powers in those cases was lawful, because it complied with the requirements of necessity, proportionality, subsidiarity and being as targeted as possible.

In the investigation period, the AIVD failed to report 57 of the 98 requests for authorization in the context of Section 28(2) of the ISS Act 2017 to the CTIVD and thus failed to comply with its duty to notify under Section 30(1) of the ISS Act 2017. Both services twice used investigatory powers based on an incorrect legal ground. They therefore failed to comply with the legal safeguards under Section 30(1) of the ISS Act 2017. In the opinion of the CTIVD, not applying all safeguards under Section 30(1) of the ISS Act 2017 is unlawful. Apart from the two aforementioned cases, the MIVD complied with its duty to notify by reporting the granting of six authorizations to the CTIVD.

This review report has no classified appendix.



No. 73 | Investigation into the provision of personal data by the AIVD and the MIVD to foreign services with an increased risk profile

Adopted on 25 August 2021, published on 12 October 2021

In this third investigation into international cooperation by the AIVD and the MIVD under the ISS Act 2017 (following CTIVD reports **no. 60**, February 2019, and **no. 65**, October 2019), the CTIVD focused on international cooperation in practice: the lawfulness of providing personal data to foreign services in specific cases. The investigation looks at those foreign services which, according to the relevant weighting

note, pose a higher risk in relation to one or more of the five legal cooperation criteria, for example respect for human rights or the level of data protection offered. Particularly in those cases where personal data is provided to these types of foreign service, a sound assessment in the specific case is paramount, as is mitigating the existing risks.

The necessity of the current investigation was prompted by the circumstance that the AIVD and the MIVD have not had their weighting notes in order for a long time. Partly because of the criticism expressed by the CTIVD in its review report no. 60 (February 2019), both services singly and jointly initiated a major revision of the process of weighting notes for cooperative relationships with foreign services. That process had not yet been concluded at the time review report no. 73 was published. Particularly in this period, the services should be alert to the process of actually providing sensitive data, such as personal data, to foreign services that do not meet all legal cooperation criteria ('increased risk profile') and the attached authorization and safeguards. The weighting notes – an important base and ground for providing that data – cannot yet provide sufficient substance.

The CTIVD investigated whether the personal data evaluated was provided lawfully by the AIVD and the MIVD to foreign services with an increased risk profile in the investigation period (1 September 2019 - 1 March 2020) and how that lawfulness was safeguarded.

The CTIVD concluded that the AIVD largely had that process in order. In practice there was some unlawful conduct in the use of overarching authorizations and in a group assessment. The AIVD must quickly develop those topics in policy and work instructions, in line with the prerequisites formulated by the CTIVD. The MIVD did not have this process in order because it did not have a system for providing authorization at an adequate level, and nor did it record the substantiation for the data provided. For the most part the data provided lacked authorization, and in none of the cases was the substantiation recorded. The MIVD must also develop the use of overarching authorization notes to provide personal data in policy and work instructions with due observance of the prerequisites formulated by the CTIVD. The CTIVD will consult with the services on this issue and assess the lawfulness of their actions.

This review report has a classified appendix.

2.2 Ongoing investigations in 2021

The CTIVD announced and conducted two lawfulness investigations in 2021, but the review reports were only published in the first quarter of 2022. The first was an investigation into the use of investigation-related interception on the cable by the AIVD and the MIVD (announced on 19 January 2021, adopted on 26 January 2022); the second was an investigation into automated OSINT by the AIVD and the MIVD (announced on 7 April 2021, adopted on 22 December 2021). These review reports will be included in CTIVD's 2022 annual report. After publication, the review reports will be accessible on www.ctivd.nl

Review report 74 Automated OSINT

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 data leaked from users of social media services. The tool can then provide a visual representation of the results. Private companies can aggregate these data sets 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 recommends that the legislator creates 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 recommends that both services take mitigating measures to comply with the general provisions in the ISS Act 2017 regarding lawful data processing.

Review report 75 Cable interception

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 did not yet have the purpose of using the data for intelligence 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 concludes 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.

In order to reinforce internal control, the services drew up a joint improvement plan in 2021. The CTIVD closely oversees how those measures are implemented. Even after it concluded its investigation, the CTIVD continued to monitor the execution of cable interception and will continue to exercise those oversight activities. The starting point here is to conduct a 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.

2.3 Other activities and publications in 2021

Consultations with Parliament, CIVD, departments and services

As part of its oversight protocol, 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 Internal Affairs 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.

Reporting unknown vulnerabilities (*zero days*)

As it did in 2020, in 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 the year the services had further implemented the recommendation, both in practice by the work of the Committee for Unknown Vulnerabilities (formerly Committee Reporting Vulnerabilities) and by developing the confidential internal policy further. Both services are actively involved in further developing a well-considered system to report *zero days* (*responsible disclosure*). However, due to a variety of circumstances less progress was made in 2021 than expected. The Committee for Unknown Vulnerabilities did convene several times in 2021 and the CTIVD actively followed the associated processes. The CTIVD will continue to address this topic in the coming year.

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 Minister of Defence (at the time also minister for the AIVD) approved this protocol.

The protocol specifies, irrespective of the existing covenants, which requirements the CTIVD sets regarding that 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 second half of 2021, the CTIVD conducted such an investigation relating to two organizations. One of those had already been investigated in 2020, while the other organization was investigated for the first time. Both investigations were concluded at the end of 2021 and a confidential report on the findings was issued in February 2022. The CTIVD concluded in its reports that the services acted in accordance with the legal framework and had handled an incident appropriately. Points for improvement regarding procedure are being addressed. The CTIVD also identified points for change in the underlying covenants to ensure better alignment with the monitoring practice. It is up to the undersigned parties to follow this up.

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 in-depth 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 use that as the basis for 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 2021 the CTIVD concluded a part of the first information file that had commenced in 2020 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 CTIVD's oversight conditions and recommendations. The remaining part of the information file was continued. In that context, a briefing was held in 2021 and written questions were put to the relevant service. At the time this annual report was published, the investigation was still ongoing.

In 2021, the CTIVD commenced one new information file that is still ongoing at the time of publication of this annual report.

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 duties to report relate to the ability or inability to exercise the services' 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. Each of these duties to report is at some point included in a CTIVD in-depth investigation.

On the other hand, both services submit reports 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, 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. The services and the CTIVD aim to set out the agreements in a protocol in the course of 2022.

Other publications

Response to ECW report

The ISS Act 2017 Evaluation Committee (ECW) published its evaluation report on 20 January 2021. At that time, the CTIVD posted an initial **critical response** to the report on its website. The CTIVD concluded that there was an imbalance in the ECW's report between the operational interests of the services for the purpose of protecting national security and the interests of protecting the fundamental rights of citizens. In 2021 the CTIVD continued its efforts to clarify its position on the points for improvement in the ISS Act 2017 to the services and the departments.

Letter about the implications of Convention 108+

On 17 February 2021, in a **joint letter** with the TIB to the House of Representatives, the CTIVD stated its position on the implications of the Council of Europe's Convention 108+ for oversight of the intelligence and security services. The Convention 108+ is a renewal of the existing Convention 108 about the protection of people as regards the automatic processing of personal data. In **their letter**, the TIB and the CTIVD detailed the implications of Convention 108+ for oversight on the processing of personal data in the context of national security. Given the great importance of the proposed amendments in the treaty, the TIB and CTIVD call for the Convention 108+ to be ratified as soon as possible.

Letter about the bill to revoke Dutch citizenship

On 2 November 2021, the CTIVD expressed its opinion on the bill to Amend the Netherlands Nationality Act and the Intelligence and Security Services Act (ISS Act) 2017 (*Parliamentary documents* 35934) in a **letter** to the president of the House of Representatives. A copy was sent to the Senate and to the States of Aruba, Curaçao and Sint Maarten. The CTIVD's view included the position that because of the proposal, the CTIVD's oversight of the authority which the Minister of Justice and Security has to revoke Dutch citizenship will result in a gap in oversight. The CTIVD also called attention to the importance of oversight of an unambiguous definition of the term 'national security'. Rather than making the minister's authority permanent, the legislator decided to extend it by five years and to retain the oversight by the CTIVD, but to limit that oversight to the unambiguous interpretation of the term 'national security' and no longer to include the efficacy and proportionality of the application of that authority. This Act entered into force on 28 February 2022. (*Parliamentary documents I* 2021/22, 35 934, D; *Bulletin of Acts and Decrees* 2022, 84).

Letter about the NCTV bill

On 22 July 2021, the CTIVD sent a **letter** to the Advisory Division of the Council of State about the bill regarding legal grounds for processing personal data by the National Coordinator for Security and Counterterrorism (NCTV). 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 on 9 November 2021. The CTIVD takes the position that from the perspective of lawfulness and rule of law, it would be better to incorporate the NCTV's activities into the Intelligence and Security Services Act 2017 (ISS Act 2017). The CTIVD points out that the bill lacks essential elements.

2.4 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, as is knowledge and skills in the field of oversight. 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. Section 6 looks in more detail at 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 investigation 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 those 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 the 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 investigation but also on its action plans, assessment frameworks, findings on practice and draft reports that the investigation groups draw up. Each of the knowledge network's members has passed a security screening at level A and is permitted to inspect state secret information. In 2021 Prof. Bart Jacobs returned to the knowledge network after completing his work for the ISS Act 2017 Evaluation Committee. The current participants in the **knowledge network** are listed on the CTIVD website.

Apart from the ongoing investigations, members of the knowledge network also participated in a number of online meetings in 2021 and shared their views on a variety 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 citizens' fundamental rights. It uses that debate to help select its investigations.

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

As in previous years, in 2021 the Oversight Department consulted with the 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. It emerged

from the consultations that the CTIVD's review reports lead to real changes in the work practice of both services.

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. That is the Minister of Internal Affairs and Kingdom Relations for the AIVD and the Minister of Defence for 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 reports of alleged misconduct.

3.2 Complaints handling by the CTIVD in 2021

Below is an overview of the number of complaints processed by the Complaints Handling Department in 2021.

CTIVD	Complaints about the AIVD	Complaints about the MIVD	Other complaints ¹
Pending on 1 January 2021	3	-	-
Complaints received	25	13	27
Declared unfounded	2	1	-
Declared partly well-founded	1	1	-
Declared entirely well-founded	-	-	-
Handled informally ²	8	2	-
Not handled ³	13	5	27

¹ 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.

² 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.

³ 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 the AIVD	Complaints about the MIVD	Other complaints ¹
Forwarded to the minister ⁴	-	1	-
Withdrawn	-	-	-
Pending on 31 December 2021	4	3	-

In total, the Complaints Handling Department handled 23 complaints in 2021, of which it already had three pending on 1 January 2021. In four 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. In five cases (two of which involved both the AIVD and the MIVD), the complaint had not been handled conclusively by 31 December 2021. Compared to previous years, the complaints handled in 2021 are more complex in nature.

Unfounded complaints

Three complaints were ruled to be unfounded by the Complaints Handling Department (two of which were in fact the same complaint, one about the AIVD and the other about the MIVD). The ruling 'unfounded' means that the Complaints Handling Department investigated the complaint and assessed it on its merits. No improper conduct by the AIVD or the MIVD was found in these complaints. Each of these complaints was about alleged conduct in the sense of the use of special investigatory powers by the AIVD or the MIVD against the complainants.

The Complaints Handling Department ruled the two other complaints to be partially founded. The parts in the complaints that were ruled to be founded both concerned procedure, for example an application for access to data in the personnel file that was not provided expeditiously enough. The Complaints Handling Department found that to be improper.

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

Complaints handled informally

Finally, the Complaints Handling Department of the CTIVD was able to handle eight complaints about the AIVD and two about the MIVD informally. A number of the 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

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 only refuse a complaint on a limited number of grounds. A complaint may be filed

⁴ 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.

digitally (through a website) 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. There was no unlawful use of a special investigatory power in the complaints handled by the Complaints Handling Department in 2021, and so far all the recommendations made by the Complaints Handling Department have been followed.

3.3 Reports on alleged misconduct submitted to the CTIVD in 2021

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 2021.

3.4 Complaints and reports of alleged misconduct handled by the AIVD and the MIVD in 2021

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 2021.⁵

Service	AIVD	MIVD
Pending on 1 January 2021	5	-
Complaints received	19	23
Declared unfounded	3	2
Declared partly well-founded	-	1
Declared well-founded	-	-
Handled informally ⁶	7	1
Not handled ⁷	6	15
Withdrawn	2	-
Referred ⁸	1	3
Pending on 31 December 2021	4	1

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. The Complaints Handling Department will address this issue in its meeting with the services.

Dialogue between the CTIVD and the AIVD and MIVD about complaints handling and reports of alleged 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 follows the developments in primary complaints handling and the handling of reports of alleged misconduct by the services.

⁵ The numbers were provided by the AIVD and the MIVD.

⁶ Handled informally means that a solution was found to the complainant's satisfaction without a formal complaints procedure being initiated.

⁷ 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.

⁸ Complaints filed with the wrong body are referred. The complaint is forwarded to the correct body in consultation with the complainant.



4

Failed

Protected

Cyber Attack

348FJDKFWOEFIK

Protected

New legislation

In the second half of 2021 the CTIVD consulted frequently with the services, departments and the TIB. Those consultations were 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 dynamic 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 the 'AIVD and MIVD Investigations into Countries with an Offensive Cyber Programme (Interim Measures) Act' was put out for public consultation on 1 April 2022.



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 2021 the CTIVD and the TIB consulted with the departments and the services about drafting a more detailed legal framework for the topic of 'organizations' in requests for authorization. This resulted in a classified legal framework.

In line with the legal uniformity consultations, the CTIVD and the TIB also consult on matters relating to the oversight of the intelligence and security services. In 2020, talks were held on the implications of the Convention 108+ of the Council of Europe for oversight. Those talks resulted in a **joint letter** to Parliament in February 2021. In December 2021, the CTIVD shared its draft review report no. 75 with the TIB – at the TIB's request and with the consent of the departments and services – with the CTIVD providing an oral explanation of its findings.



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*, and since 2018 a conference is organized annually in December for oversight bodies.

After a period of close cooperation in 2019, international cooperation with foreign oversight bodies was severely hampered in 2020 due to Covid. In the second half of 2021, a first step was taken towards resuming cooperation within the *Intelligence Oversight Working Group* by means of an online meeting. That cooperation has stepped up again in 2022.

Following the conference in The Hague in December 2019, the CTIVD participated in the annual conference of European oversight bodies for the intelligence and security services held in Rome in October 2021. The chair of the Complaints Handling Department gave a presentation about the state of affairs of the right of complaint in a number of European countries.

7



Organizational developments

Composition of the CTIVD

In 2021 the CTIVD consisted of Nico van Eijk (chair), Marylène Koelewijn (member), Harm Trip (member) and Addie Stehouwer (member and chair of the complaints handling department).

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

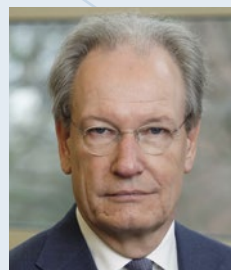
Oversight Department



Nico van Eijk
Chair



Marylène Koelewijn
Member



Harm Trip
Member

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.

Facilities developments

Administratively, the CTIVD falls under the Minister 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 (2021).



P.O. Box 85556
2508 CG The Hague

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