Annual report

2020

Review Committee
on the Intelligence and
Security Services

Annual report

2020

Review Committee
on the Intelligence and
Security Services

Preface

In 2020, the CTIVD gave further shape to its oversight role, in addition to publishing three review reports and concluding the process of progress reports on the new legislation, the CTIVD initiated various programmes aimed at professionalizing and diversifying its oversight activities. The lawfulness assessment is as much aimed at encouraging a change in behaviour, as detecting any unlawful conduct as such.

The CTIVD's key responsibility continues to be striking the right balance between the interests of national security – which includes the services' operational strength – and protecting fundamental rights.

The fourth progress report (report no. 69) marks the end of the period of increased oversight on the implementation of the Intelligence and Security Services Act 2017 (ISS Act 2017). Considerable progress has been made. At the same time, converting the legislation and policy into daily practice (work instructions, technical systems, internal control mechanisms) is a concern and will continue to be the CTIVD's focus.

Those concerns also include the matter of bulk data sets, which is the subject of two specific review reports. Report no. 70 covers the collection of bulk data sets using the hacking power and their further processing by the AIVD and the MIVD. Report no. 71 concerns the collection and further processing by both services of airline passenger data. The use of bulk data sets (collections of data, the vast majority of which concerns organizations or people who are not the subject of investigation by the services, nor ever will be) is unavoidable and necessary. However, that use requires solid safeguards due to the severe infringement of fundamental rights it entails.

The CTIVD had previously established that where bulk data sets are concerned, the current legal framework is not consistent with daily practice and lacks the proper safeguards. Consequently, certain bulk data sets are currently being stored in breach of the law for longer than permitted by law. The CTIVD views this with great concern and has communicated to the House of Representatives that the law must be amended swiftly.

Oversight of national security should be in line with principles that apply to other forms of oversight, particularly where it concerns data protection. Processing information is the key task of the intelligence and security services and constitutes a severe infringement of fundamental rights. Effective, independent oversight should ensure that unlawful data processing can be ended. The ISS Act 2017 does not provide for this and that loophole must be closed. In that respect it is vital that the Netherlands ratifies the Council of Europe Convention 108+ promptly and amends the ISS Act 2017 accordingly. Convention 108+ is the first European convention that explicitly regulates the processing of data in the context of national security and provides for safeguards. However, compliance with only the minimum standards in international treaties and case law is not enough. The Netherlands has a reputation to maintain in this matter.

The AIVD and the MIVD play an important role in keeping the Dutch constitutional state safe, among other things by ensuring that digital attacks on special sections of the state are identified and countered. The independence of these organizations' functioning

should be unquestioned. The investigatory powers used by the services are subject to enhanced oversight by the CTIVD. Therefore a protocol was drawn up that ensures regular checks of these activities and reports to the involved organizations. The in-house IT expertise which the CTIVD has gained is proving very useful in this respect.

A further priority for the CTIVD is innovating its oversight – by gradually expanding system oversight and developing new instruments. Those new oversight instruments are in line with what is customary for oversight elsewhere. They represent an incremental professionalization and thus aim to align better with the current challenges for both the services and the oversight.

Needless to say, 2020 with its huge health and societal challenges was an exceptional year for the CTIVD also.

Nico van Eijk
Voorzitter CTIVD

Table of contents

1

Introduction

The Review Committee on the Intelligence and Security Services (**CTIVD**) oversees the lawfulness of the conduct of the General Intelligence and Security Service (**AIVD**) and the Military Intelligence and Security Service (**MIVD**). The CTIVD has far-reaching investigatory powers to do so which enable it to conduct in-depth investigations into the lawfulness of the services' conduct across the full range of their tasks. By means of its independent **investigation**, the CTIVD considers it its duty to provide an understanding of the right balance between the interests of national security and the legal protection of citizens.

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

Every year, the CTIVD publishes an annual report before 1 May, which is submitted to Parliament and 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 translated into English and made available on the CTIVD's website. This is the 2020 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 the Complaints Handling Department in 2020 and lists the items on the agenda for 2021. Section 4 details how the CTIVD participated in the process of evaluating the Act. Section 5 discusses the legal uniformity meetings 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 how the CTIVD's organization developed in 2020.

2

Activities of the Oversight Department

2.1 Implementation of ISS Act 2017

Progress reports

Since the **ISS Act 2017** entered into force on 1 May 2018, the Oversight Department of the CTIVD has concentrated its oversight activities on the implementation and functioning of that new legislation, in particular on those themes that commanded the most attention in the political and social debate. As a consequence, during the debate on the Act, both the House of Representatives and the Senate requested the CTIVD to speed up or intensify its oversight activities. The government also asked the CTIVD to rigorously review proper compliance with the legislation in actual practice. Those requests largely correspond with the key points put forward by the CTIVD itself during and after the parliamentary debate on the Act in 2017 and the referendum on the Act on 21 March 2018.

Nr. 69 | Progress report IV on the implementation of the ISS Act 2017

Adopted on 5 August 2020, published on 8 September 2020

In its fourth and concluding progress report, the CTIVD took stock of the results of the process of implementing the ISS Act 2017 since the introduction of this Act more than two years ago. The CTIVD established that although the AIVD and the MIVD have worked hard, they have not yet completed the implementation of the ISS Act 2017. The CTIVD monitored the implementation process closely ever since the Act was introduced. It has been a strenuous process, both for the services having to combine it with their operational practice and for the oversight body having to review a continuously developing implementation process. The services still have their work cut out for them in the period ahead, which places demands on them in terms of focus, direction and capacity. In the coming period the CTIVD will therefore maintain dialogue with the services about the implementation of the ISS Act 2017.

A key factor in the delay of the implementation process and the consequent risks of unlawful conduct by the services is the lack of focus during the drafting of the Act on the impact that the introduction of the ISS Act 2017 would have. The CTIVD stresses the need to avoid a repeat and instead to conduct a realistic impact analysis of the implementation issues when evaluating and amending the current legislation.

The CTIVD concludes that over the past period both services have set course in the right direction. One main aspect is that the legal duty of care for lawfulness and quality of data processing are embedded firmly in the services' organizations, thereby providing a sound basis for the future.

Furthermore, the CTIVD is positive about the far-reaching cooperation between the services in implementing the ISS Act 2017. In the coming years both services will work towards joint data maintenance and a joint IT infrastructure. Once that has been fully achieved, the work processes will consequently be more uniform and that will result in greater joint control and overview.

Converting the legislation and policy into daily practice (work instructions, technical systems, internal control mechanisms) is a concern. Despite their efforts over the past two years, the services have been unable to make sufficient progress. That is particularly the case for investigation-related interception and automated data analysis. That can partly be explained by the fact that this is a time-consuming, complex and wide-ranging process. However, the conversion into practice is at the heart of the implementation process. Ultimately, the legal safeguards are aimed precisely at the operational practice which is where they should have their effect if they are to protect citizens' fundamental rights conclusively. That highlights the importance and need for the services to continue unabated in their efforts to complete the implementation process.

Investigation-related interception via the cable is a significant part of the political and social debate, which has led to questions by Parliament and the ministers to the CTIVD about the use of investigation-related interception via the cable. Due to the fact that this investigatory power has not yet been exercised, those questions cannot be answered. The CTIVD concludes that the efforts made by the services in the process and set-up of the interception of satellite and radio communications as part of investigation-related interception can be reflected onto the cable. From a systems approach, the services are now adequately prepared for bulk interception on the cable.

Secondment of CTIVD review officer to the Netherlands Court of Audit

The Netherlands Court of Audit also assesses the AIVD and MIVD's conduct. Each year, the court conducts an accountability assessment of the expenditure of both services and it issues an annual report to the Committee on the Intelligence and Security Services (CIVD) of the Dutch House of Representatives. The Court of Audit also conducts assessments of efficiency aspects. In its **third progress report** on the implementation of the ISS Act 2017, the CTIVD established that adjusting the work processes and IT systems to comply with the new and existing stipulations of the ISS Act 2017 was more far-reaching than the services initially anticipated. At the time, the CTIVD highlighted the importance of an efficiency assessment of the impact of the new Act on the services to the Court of Audit.

At the request of the Minister of Defence (at the time also the minister for the AIVD), the Court of Audit decided in May 2020 to conduct an investigation into the incidental and structural effects of the ISS Act 2017 on the operational performance of the AIVD and MIVD's tasks (see pp. 41-42 of the report 'Results of the accountability assessment 2019' at the Ministry of Defence by the Court of Audit (May 2020)). At the request of the Court of Audit, the CTIVD seconded a review officer for the period July - October 2020 to the Court of Audit to share its knowledge about the ISS Act 2017 with the investigative team and to contribute to the investigation. The Netherlands Court of Audit is expected to conclude its investigation in the spring of 2021.

2.2 Lawfulness investigations completed in 2020

Apart from its focus on the implementation of the new legislation in practice, the CTIVD also conducts regular lawfulness investigations. The CTIVD sets its own investigative agenda. In particular it looks at the societal context of the AIVD and MIVD's conduct.

In 2020 as it did in 2019, the CTIVD focused its attention on the large amounts of bulk data processed by the AIVD and the MIVD. This bulk data can be collected through different investigatory powers. For example, large data sets may be obtained on the internet, through informants and agents, with the aid of the hacking power and through the services' new investigatory power of investigation-related interception. Technological developments enable the services to collect ever larger amounts of data and to effectively process it in increasingly complex ways, although the Act in itself does not contain any explicit safeguards to process bulk data. The personal data of citizens who are not the focus of either of the services is a significant factor in all this, making bulk processing by both services an important overall theme in the CTIVD's oversight.

The CTIVD's Oversight Department issued three review reports in 2020. Two of those review reports (nos. 70 and 71) form part of the aforementioned theme of bulk processing while the third report (no. 68) concerns an investigation conducted in the context of the Act Revoking Dutch Citizenship in the interest of National Security. An overview of the main findings is given below. The review reports may also be accessed through the CTIVD website.

Nr. 68 | The AIVD's conduct in the context of revoking Dutch citizenship in the interest of national security

Adopted on 29 April 2020, published on 16 June 2020

The Act Revoking Dutch Citizenship in the interest of National Security entered into force in March 2017. Under this Act the Minister of Justice and Security may revoke Dutch citizenship from individuals who have joined organizations deemed a threat to national security. A decision to revoke Dutch citizenship can be based on public information or information from the Public Prosecution Service, or made following an official message from the AIVD. An official message can thus spark the process in which Dutch citizenship is ultimately revoked.

In its investigation, the CTIVD examined the twelve official messages which the AIVD had issued thus far in the context of revoking Dutch citizenship in the interest of national security. The CTIVD concluded that each time the official messages were all sufficiently substantiated, necessary and proportionate. All twelve official messages were, in the CTIVD's opinion, issued lawfully.

Furthermore the CTIVD made random checks of the cases in which the AIVD decided not to issue an official message. There were a variety of reasons not to do so, for example a lack of sufficient information or operational objections. The CTIVD concluded that in those cases, in which the AIVD decided not to issue an official message, the service had arrived at its decision fairly.

This review report has no classified appendix.

Nr. 70 | On bulk data sets collected using the hacking power and on their further processing by the AIVD and the MIVD

Adopted on 19 August 2020, published op 22 September 2020

Report no. 70 covers the collection of bulk data sets using the hacking power. That is a special investigatory power in the ISS Act 2017. An important safeguard is that the services must assess the data obtained using a special investigatory power for relevance to their investigations as soon as possible. That assessment must be conducted within 18 months otherwise all data, except the data already declared relevant, must be destroyed. That also applies to data in bulk data sets obtained using the hacking power. That safeguard is important because it prevents the services storing non-relevant data for too long, which is particularly important in the case of bulk data sets because the majority of these contain data relating to organizations and/or people who are not the subject of investigation by the services, nor ever will be. The obligation to destroy data after a maximum term has expired is therefore a cornerstone of the data reduction system.

In its review report, the CTIVD established that the legal requirement that data is assessed for relevance 'as soon as possible' is at odds with the nature of bulk data sets. These are large collections of data, and it is difficult if not impossible to determine beforehand which data will be relevant during the assessment period. In addition, because of their specific characteristics, bulk data sets may be of value to the services' investigations for a significantly longer period.

In the face of that issue, the services have declared certain bulk data sets relevant as a whole or for a significant part. The CTIVD assessed this practice as unlawful, as it means that data from people and organizations that are not, nor will be, the subject of investigation is thereby also declared relevant while that data is quite obviously not relevant. A consequence of this abstract method of relevance assessment is that the data can be stored with the services without any definitive destruction period. After all, information declared relevant falls under the heading 'significant' and its destruction is only at issue once the data has lost its significance.

In the CTIVD's view, this way of assessing relevance is an artifice by which to store and use bulk data sets for longer than permitted by law. It follows from the law that bulk data sets unlawfully declared relevant must be destroyed. The recommendation in the report to destroy that data was not adopted by either minister.

The services apply safeguards in practice beyond those laid down in law, when they further process bulk data sets obtained using the hacking power. The CTIVD finds that to be a sufficient implementation of the requirements that the law sets to proper and careful data processing. Although these general principles provide a basis for the lawfulness assessment, it is advisable to turn to a more inclusive legal regulation of bulk data sets that does sufficient justice to the protection of citizens' fundamental rights and to the operational value of bulk data sets for the services.

As regards the use of the hacking power, the CTIVD concludes in its report that the power was used lawfully, except in a number of operations that failed to comply with the authorization requirements.

This review report has a classified appendix.

Nr. 71 | On the collection and further processing by the AIVD and the MIVD of airline passenger data

Adopted on 19 August 2020, published op 22 September 2020

Review report no. 71 is an in-depth investigation into the further processing by the AIVD and the MIVD of airline passenger data. The CTIVD conducted an investigation into the collection and further processing of Advance Passenger Information (API data). API data is data on passengers of a flight and information about that flight that is stored by the airlines such as name, date of birth, nationality, airport of departure and of arrival. This data is collected routinely and by automated means. The vast majority of this data concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. That means it is actually the collection and further processing of a bulk data set. The data is collected using a general investigatory power (in this case, the investigatory power to use informants). The use of a general investigatory power does not require ministerial authorization or a lawfulness assessment of that authorization by the TIB.

In the investigation period from January 2019 to September 2019, the CTIVD investigated whether the AIVD and the MIVD collected and processed API data lawfully.

The CTIVD concluded that the investigatory power to use informants exercised to collect API data was lawful. Likewise, the requirements of purpose limitation and necessity were met. However, the AIVD and the MIVD failed to classify the data as bulk data sets as required by their own policy. Consequently the safeguards set by law and the services' internal policy, were not or insufficiently applied. That is unlawful. Furthermore, the CTIVD established unlawful conduct in a specific case of data analysis in which the reporting was inadequate. Finally, certain data-processing activities were assessed as unlawful by the Security Screenings Department, because the activities did not fit in with the department's tasks.

The investigation shows that for the collection and further processing of bulk data sets using a general investigatory power, legislation does insufficient justice to the protection of the fundamental rights of people who are not the subject of investigation by the services, nor ever will be. In its report the CTIVD noted that this topic deserves consideration, at the least, in the context of the evaluation of the ISS Act 2017.

This review report has a classified appendix.

2.3 Ongoing investigations in 2020 and planning for 2021

Investigation into the use of investigatory powers to support a proper execution of the AIVD and MIVD's tasks

The services may, after authorization by the relevant minister, use special investigatory powers in certain cases to support their work, for example to establish whether special measures are necessary to guarantee the safety of an agent or to assess the reliability of an informant. That legal regulation was introduced in the ISS Act 2017.

Given the fact that this procedure differs from the principle that the use of investigatory powers must be necessary for the services to carry out their tasks properly, the ISS Act 2017 stipulates that the CTIVD be informed immediately when authorization is granted. The investigation is aimed at assessing the lawfulness of the application of Section 28(2) of the ISS Act 2017, which regulates the cases in which special investigatory powers can be used to support a proper execution of tasks. The investigation also attempts to answer the question whether the services notify the CTIVD of the granted authorization in all cases required by law.

This investigation was announced on 9 October 2019 and will be published in April 2021.

Investigation into the provision of personal data by the AIVD and the MIVD to foreign intelligence and security services with an increased risk profile

In this third investigation into international cooperation of 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 that pose a higher risk according to the relevant weighting note 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 speciffic case is paramount, as is mitigating the existing risks.

This investigation was announced on 25 June 2020 and will be published mid 2021.

Investigation into the use of investigation-related interception on the cable by the AIVD and MIVD

In 2021 the CTIVD is conducting an investigation into the use of investigation-related interception on the cable. The AIVD and the MIVD conducted exploratory activities on the cable and used investigatory powers that obligate communication providers to issue information on request and to cooperate with both services (known as the duty to assist and provide information). The services expect the actual interception of data on the cable to take place in 2021.

The exploratory activities consist of taking what is known as snapshots – short integral recordings of data flows. These recordings are then used to examine whether a data flow can be important for the services' investigation assignments. Based on that investigation, the actual interception will be carried out in as targeted a way as possible. The CTIVD opted to investigate the initial phase of the interception process first. A follow-up investigation will be carried out once the services have started the interception.

This investigation was announced on 19 January 2021 and will be published in the second half of 2021.

2.4 Other activities

Consultations with Parliament, departments and services

As part of its oversight protocol, the CTIVD issues explanatory notes regarding 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, 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 give presentations to each other. The CTIVD contributes for example to the introduction 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 2019, the CTIVD in 2020 again addressed the follow-up of the 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). Both services gave a verbal explanation of their activities in a meeting.

The CTIVD established that during the year the services 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). An evaluation of the internal policy has been scheduled and will be completed by both services in 2021. In the coming year the CTIVD will continue to address this topic.

On 12 June 2020, the CTIVD published **a public response** to the Bill Zero Days Assessment process, in which it explained the zero days issues and clarified its position on the bill.

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 to that cooperation based on the ISS Act 2017 and how it includes those activities in its review.

The protocol also sets out that this form of review will not be published in a public review report but that the CTIVD will issue its findings to the organizations involved in a confidential report and through the ministers involved. The CTIVD will report on this ongoing form of review at least once a year to the relevant organizations. In the second half of 2020, the CTIVD conducted such an investigation, the results of which were included in a report at the beginning of 2021.

Bulk data

Bulk data was once more an important overall theme in the review by the CTIVD (see also Sections 2.1 and 2.2). The CTIVD discussed this topic with the ISS Act 2017 Evaluation Committee chaired by Ms Renee Jones (see Section 4). The CTIVD underscores the need to set out a solid legal framework for acquiring and further processing bulk data sets in order to justify both the operational necessity of using bulk data sets and the corresponding necessary safeguards.

The ongoing evaluation of the act does not change the fact that in the meantime the fundamental rights of individuals who are not or should not be the focus of the services must be adequately protected. In its review reports no. 70 and no. 71 (see Section 2.2), the CTIVD made the recommendation to both services to develop an overall policy that provides for safeguards on dealing with bulk data sets. Partly in response to that, the services and the departments involved worked on policy in the form of the Temporary regulation for further processing bulk data sets ISS Act 2017. That was published in the Government Gazette on 5 November 2020. During the development of the regulation, the CTIVD and the services conducted a dialogue in a number of ways including in several meetings.

On 5 November 2020 the CTIVD published **a response** to the temporary regulation on its website, in which it states that the policy does not reverse the fact that the provisions of the ISS Act 2017 remain fully applicable to the processing of bulk data sets. That not only applies to the general requirements for data processing but also for the requirement that data obtained using a special investigatory power must be assessed for relevance within a maximum term of 18 months.

Information files

In 2020 the CTIVD introduced a new review instrument under the heading information file. That allows for a faster and more effective response to developments within the services. Initiating an information file can be prompted 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 on that basis plot its subsequent course. That course may take a number of forms. Based on the information file, it may be decided that further follow-up is unnecessary, or that a legal framework should be drawn up against which the established conduct by the service should be checked, that an advisory opinion should be sent to the minister or that an in-depth investigation should be announced. At the end of 2020 the CTIVD initiated its first information file that is still ongoing at the time of drafting this annual report.

2.5 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 are 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. This also includes operational context to the various operations and both knowledge and skills in the field of oversight are necessary. For 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 has to adapt to the developments at the services to be able to continue conducting its oversight effectively. Section 7 deals with the development of the CTIVD's organization.

Under Section 108 of the ISS Act 2017 the CTIVD may also attract expertise from outside the organization. Thus the CTIVD is able to draft an expert opinion – a theoretical analysis or an indepth study of a specific issue. In 2020 the CTIVD availed itself of the knowledge network and the Council of Europe's secretariat to check its position on the implications of the Council of Europe's Convention 108+ for oversight of the intelligence and security services. The CTIVD and the TIB sent a letter on this topic to the House of Representatives in February 2021.

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. 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 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. The expertise of the members of the knowledge network was put to good use in in-depth investigations in 2020 also.

In April 2020 the cabinet approved the appointment of Prof. Bart Jacobs as a member of the independent committee which evaluated the Intelligence and Security Services Act 2017 (ISS Act 2017). His membership of the knowledge network was suspended

following this appointment. In 2020 Ms Quirine Eijkman joined the knowledge network. Ms Eijkman is a prominent human rights lawyer and deputy chair for the Netherlands Institute for Human Rights. The current participants in the **knowledge network** are listed on the website of the CTIVD.

Reflection from society and science

The CTIVD has a broad network of contacts in interest groups, oversight bodies and scientific institutions in the Netherlands. These help it to keep in touch with the social and scientific debate on weighing the interests of national security against the protection of citizens' fundamental rights and it takes these factors into account when selecting its investigations.

The CTIVD cooperated with Utrecht University in creating the endowed chair in Intelligence and Law. From 1 February 2020 Jan-Jaap Oerlemans, working at CTIVD as a senior review officer, was appointed endowed professor. The endowed chair was created by the CTIVD to promote research and the transfer of knowledge about the legal aspects in the field of intelligence and national security. The Ministry of the Interior and Kingdom Relations and the Ministry of Defence have allocated a budget to appoint a PhD supervised by the chair holder.

On 16 November 2020, Prof. Oerlemans held his inaugural lecture entitled: "Setting limits to the hunger for data. Protecting national security in a democratic constitutional state." In his lecture, Oerlemans proposes creating explicit legal grounds for collecting bulk data sets from other government parties.

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 duty of the services to report authorization granted by the minister(s) 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. The CTIVD started an investigation into this topic at the end of 2019 (see Section 2.3). Other legal duties to report relate to cases in which the services fail or are unable to exercise the duty to notify and to the rejection of requests to access data processed by the services. The CTIVD reviews these notifications and assesses whether there is reason to conduct further investigation. Each of these duties to report can at some point be included in an in-depth investigation by the CTIVD. That was the case with the previous review reports **no. 65** (unevaluated data), **no. 58** and **no. 54** (requests to access data) and **no. 51** (duty to notify). In 2020 an investigation was conducted into the use of investigatory powers to support a proper execution of tasks and the review report was drafted. That report will be published in April 2021.

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. That may include reports of incidents that took place or notifications of actions not taken in accordance with the legal regulation. In those cases the CTIVD makes thorough inquiries with the services and where necessary independently conducts further investigation, for example by way of an in-depth investigation or an information file. See also Section 2.4.

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

As in previous years, the Oversight Department consulted in 2020 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 involved to demonstrate the extent to which the recommendations adopted have been followed up on. Should this lead 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

Since the introduction of the ISS Act 2017, regular meetings are held between the services' legal affairs departments (as primary complaint handlers) and the CTIVD (as follow-up complaints handler) about the procedures and 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. In addition, trends in the nature and number of the complaints filed are also addressed. On a periodic basis, both services submit lists of the complaints they handled or decided not to handle. The Complaints Handling Department can thus follow the developments in primary **complaints handling**, the notification procedures and how these are used by both services.

3.2 Complaints and reports of misconduct in 2020

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.

Hieronder wordt een overzicht gegeven van de aantallen klachten die in 2020 door de beide diensten zijn verwerkt.[1]

Complaints	AIVD	MIVD
Pending on 1-1-2020	7	–
Complaints received	25	5
Declared unfounded	3	–
Declared partly well-founded	1	–
Declared well-founded	–	1
Handled informally[2]	3	–
Not handled[3]	20	1
Repealed	1	–
Referred[4]	2	2
Pending on 31-12-2020	2	1

Complaints handled by the Complaints Handling Department of the CTIVD

Below is an overview of the number of complaints processed by the CTIVD in 2020.

CTIVD	Complaints about the AIVD	Complaints about the MIVD	Other complaints[5]
Pending on 1-1-2020	3	–	–
Complaints received	30	2	30
Declared unfounded	4	–	–
Declared partly well-founded	–	–	–
Declared entirely well-founded	–	–	–
Handled informally[6]	1	1	–
Not handled[7]	24	1	30
Forwarded to the minister	–	–	–
Repealed	1	–	–
Pending on 31-12-2020	3	–	–

In total the CTIVD handled 7 complaints in 2020. In 4 cases that resulted in a formal decision by the Complaints Handling Department who published the complaint in anonymized form on the CTIVD's website. In 3 cases the complaint handling had not yet been completed on 31 December 2020.

1 The numbers were provided by the AIVD and the MIVD.
2 Handled informally means that a solution was found to the complainant's satisfaction without a formal complaints procedure being initiated.
3 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 an objection or appeal proceedings.
4 Complaints filed with the wrong body are referred. The complaint is forwarded to the correct body in consultation with the complainant.
5 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.
6 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.
7 There may be a number of reasons why a complaint is not handled, for example the complaint was a repeat complaint, the complaint had not yet been handled in a primary response by the minister involved or the complainant failed to respond after the CTIVD asked for additional information.

Unfounded complaints

The four complaints ruled unfounded by the CTIVD related in each case to the alleged use of investigatory powers by the AIVD against the complainants.

The CTIVD ruled two of those complaints to be 'apparently unfounded'. That means that the content of the written complaint itself already showed the complaint was unfounded. In the case of those two complaints, the CTIVD did not conduct any investigation into the complaints.

The other two complaints were ruled unfounded by the CTIVD. That means that the CTIVD conducted an investigation into the complaint and assessed it on its contents. In those complaints the AIVD's conduct was not found to be improper. However, for one complaint the CTIVD did assess the complaints handling procedure at the AIVD on its own initiative. The Complaints Handling Department of the CTIVD commented on the identification of complaints by the AIVD.

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

Informally handled complaints

The CTIVD was able to handle one complaint about the AIVD informally. That complaint concerned a claim for compensation from the AIVD by the complainant. The complainant failed to agree to the AIVD's offer, after which the AIVD withdrew the offer. The complainant then filed a complaint about that and wanted to reopen talks about the amount of compensation. Through an intervention that complaint was then resolved by the AIVD to the complainant's satisfaction.

Accessibility of the complaints process

Special investigatory powers are used covertly by both services. That means citizens will generally be unaware if an investigatory power is being used against them. In a complaint, the complainant does not have to further substantiate the alleged unlawful use of investigatory powers against him or her. Submitted complaints about one service that possibly relate to the conduct of the other service are forwarded. 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 digitally (through a website) with the AIVD, the MIVD and the CTIVD. In that sense, every attempt is made to make it easy to file a complaint.

Imposing measures

The Complaints Handling Department issues binding decisions on the ministers involved and may impose measures 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 measure 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 department in 2020. So far all the recommendations made by the Complaints Handling Department have been followed. For example a recommendation made by the department in 2019 resulted in 2020 in an improved internal procedure for both services in conducting security screenings.

Reporting misconduct

The ISS Act 2017 contains a procedure on 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. Every 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 CTIVD will process the report if it believes that it concerns a report of alleged misconduct and will then investigate whether it is likely for misconduct to have occurred. The reporter and the minister concerned are both granted 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. Next, the minister informs the CTIVD on 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 report on the report on its website.

In 2020 no alleged misconduct has been reported to either service or the Complaints Handling Department of the CTIVD.

3.3 Pending complaints

In the course of 2020 the Complaints Handling Department received three complaints where the complainant was represented by a lawyer. Two of those complaints were investigated and the reports will be published in 2021. The third complaint was first handled by the relevant minister.

4

Evaluation of the Act

On 1 May 2020 the evaluation committee chaired by Ms R.V.M. Jones commenced its evaluation of the Intelligence and Security Services Act 2017 (ISS Act 2017). That is an implementation of a coalition agreement to initiate the evaluation of the ISS Act 2017 within two years of its introduction on 1 May 2018. Bringing forward the evaluation was prompted by the outcome of the advisory referendum on the ISS Act 2017, in which 49.44% of participants voted against and 46.53% voted in favour of the ISS Act 2017.

The cabinet asked the evaluation committee for the ISS Act 2017 (hereinafter: ECW) to investigate the following: (1) whether the Act delivered what the legislator intended; (2) whether the Act has proved to be a viable tool in practice for the services' tasks; and (3) what bottlenecks and points for concern were raised in daily practice.

The CTIVD was fully involved in the evaluation process. On 11 August 2020 it sent a **detailed letter** about various topics to the ECW. In that letter, the CTIVD stressed that developments in case law and international treaties require a restructuring of the oversight system towards integrated oversight, with the option for the CTIVD to issue a binding decision on the lawfulness of dataprocessing activities. The CTIVD also contributed the suggestion that a regulation for bulk data sets is necessary and that the regulation for automated data analysis should be amended. On 2 December 2020, the CTIVD sent a **final letter** in which it listed its main opinions on the oversight.

On 12 October 2020, the CTIVD sent **a letter** about complaints handling. In that letter the CTIVD explained that in its view, the ISS Act 2017 did not require any amendments concerning complaints handling or handling of reports of misconduct.

The CTIVD also had several in-depth meetings with the ECW in which it held presentations about a number of topics including the oversight system, complaints handling and reports on alleged misconduct, international cooperation by intelligence and security services, automated data analysis, the hacking power and the processing of bulk data by the services.

The 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 will continue its efforts to clarify its position on the points for improvement in the ISS Act 2017.


5

Preserving legal uniformity

The Investigatory Powers Commission (TIB) and the CTIVD regularly meet to ensure 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. That 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.

The legal uniformity consultations held between the TIB and the CTIVD in 2020 focused on topics including the acquisition and further processing of bulk data sets.

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 that the Convention 108+ of the Council of Europe has for oversight. That resulted early 2021 in a **joint letter** to Parliament.


6

International cooperation

Intelligence and security services are cooperating more closely and in new ways. International cooperation is essential for those services in order to protect the national security.

However, cooperation between oversight bodies is still in its infancy, although since 2015 more and more initiatives have been taken in this area. For example, the CTIVD established a cooperative partnership with five other oversight bodies, the Intelligence Oversight Working Group, and since 2018 a conference is organized annually in December for oversight bodies. The first conference was held in Paris in 2018, the second in The Hague in December 2019. In 2020 the European Intelligence Oversight Conference was supposed to have been organized by the Italian oversight body, but following a period of close cooperation in 2019, COVID-19 severely limited any international cooperation with foreign oversight bodies.

As a result of the COVID-19 restrictions, few activities were able to take place in 2020 either. The scheduled European Intelligence Oversight Conference in Rome had to be cancelled. Whether the conference can take place in 2021 is being considered. In 2020 various online meetings were held to discuss this with a number of foreign oversight bodies and a delegation of the CTIVD visited the Italian oversight body in July 2020 to discuss the schedule and programme of the coming conference.

7

Organizational developments

Composition of the CTIVD

In 2020 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. On 1 January 2020 Harm Trip was appointed committee member of the Oversight Department. On 1 June 2020 Erik Kok was appointed committee member of the Complaints Handling Department. Both departments are supported by the CTIVD's secretariat. Kristel Koese has been the general secretary since 1 July 2020.

Oversight Department

Nico van Eijk
Chair

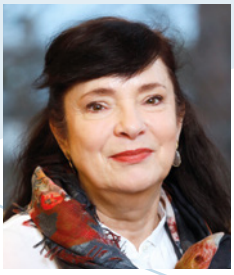
Marylène Koelewijn
Member

Harm Trip
Member

Complaints Handling Department

Addie Stehouwer
Chair

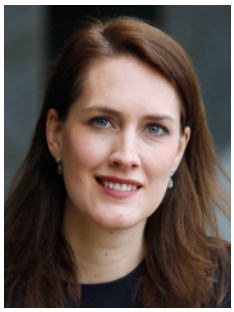
Hermine Wiersinga
Member



Anne Mieke Zwaneveld
Member

Erik Kok
Member

Staf



Kristel Koese
General Secretary

The CTIVD is supported by the general secretary, review officers with expertise in legal, policy and technical matters, a member of the support staff and a secretary.

Facilities developments

Administratively, the CTIVD falls under the Minister of General Affairs. That 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 in 2020 was 2.5 million euros.

Oranjestraat 15, 2514 JB The Hague
P.O.Box 85556, 2508 CG The Hague

T +31 (0)70 315 58 20
E info@ctivd.nl | www.ctivd.nl