# Annual report 2019

CTIVD

Review Committee on the Intelligence and Security Services

# Annual report

# 2019


Review Committee
on the Intelligence and
Security Services

# Preface

## Onwards to 2020

The year 2019 proved in many ways to be a continuation of the previous year and a prelude to 2020, when an evaluation committee will fast-track its review of the Intelligence and Security Services Act 2017 (ISS Act 2017).

A year before, in May 2018, the CTIVD started its investigation into the implementation of the ISS Act 2017 which resulted in 2019 in a second and third progress report. In 2020 that investigatory process will be concluded with a final fourth report. Each time the outcome of the reports has had an impact on the AIVD and the MIVD and has contributed to changes at both services. But it does not end there. The CTIVD will continue to monitor whether the changes are sufficient and do actually yield the intended results, in particular where it concerns the implementation of the services' legal duty of care for the lawfulness and quality of their data processing.

The evaluation of the Act will not only provide an opportunity to address the evolving views and experience gained with the new legislation but also to review the Act in its wider context. I will briefly discuss four important developments.

Previous legal uniformity letters by the CTIVD and the Investigatory Powers Commission (TIB) highlighted the impact of new case law. New rulings from Strasbourg and Luxemburg expected in 2020 may further clarify important issues regarding the protection of the constitutional state. As such, case law forms part of the normative assessment framework and is therefore a standard for the work and assessments by the CTIVD.

One of the principles of the ISS Act 2017 was achieving regulations that were neutral in terms of technology. The public debate focused very much on the prospect that investigation-related interception via the cable would also be allowed. A system of oversight in advance, current oversight and retrospective oversight ('ex ante, ex nunc and ex post') applies to this investigatory power. In 2019, four reports addressed topics regarding investigation-related interception: "The application of filters in investigation-related interception by the AIVD and the MIVD" (report no. 63), "The use of the special investigatory power to select by the AIVD and the MIVD" (report no. 64), "Progress report II" (report no. 62) and "Progress report III" (report no. 66).

Bulk data sets were identified as a significant point for concern, including in the context of investigation-related interception. Bulk data sets include data collections of which the majority of the data cannot be linked to the services' targets. Under the ISS Act 2017, these bulk data sets may be obtained in a variety of ways, including through the use of general and special investigatory powers (in addition to investigation-related interception, that includes measures such as informants, agents, public sources, hacking and the exchange of data with foreign services. Bulk data sets raise questions of their own relating to processing, destruction and retention periods, for which the ISS Act 2017 does not offer specific safeguards, with the exception of investigation-related interception. That already presents new challenges for the legal framework and review.

A further development that merits mention is the ongoing internationalization, which has become more apparent in the AIVD and the MIVD's activities, in particular where it concerns the exchange of data with foreign services. The provision of unevaluated data was the subject of report no. 65. The evaluation of the Act will have to address these international aspects adequately – both the data exchange itself and the oversight of this activity. At the conference for European oversight bodies for the intelligence and security services organized by the CTIVD in December 2019, the participants further discussed the need to strengthen international cooperation between European oversight bodies.

The CTIVD connects the large amount of data and the related automated processes to an enhanced focus on system review and compliance. CTIVD review officers, in particular the IT unit, have already spent a considerable amount of time on this in 2019 – including through baseline measurements of DRS (data reduction systems) and ADA (automated data analysis) – and that is not expected to change in 2020. The aim is, in consultation with the involved stakeholders, to define safeguards that do justice to the interests of legal protection and national security served by that oversight.

The departure of Harm Brouwer and Aad Meijboom as chairperson and committee member respectively, does not signal the end of an era. On the contrary, supported by experienced colleagues and highly motivated staff both gentlemen have plotted a course well worth adhering to in the future. We owe them a debt of gratitude.

**Nico van Eijk**
CTIVD chair

# Table of contents

# 1

# Introduction

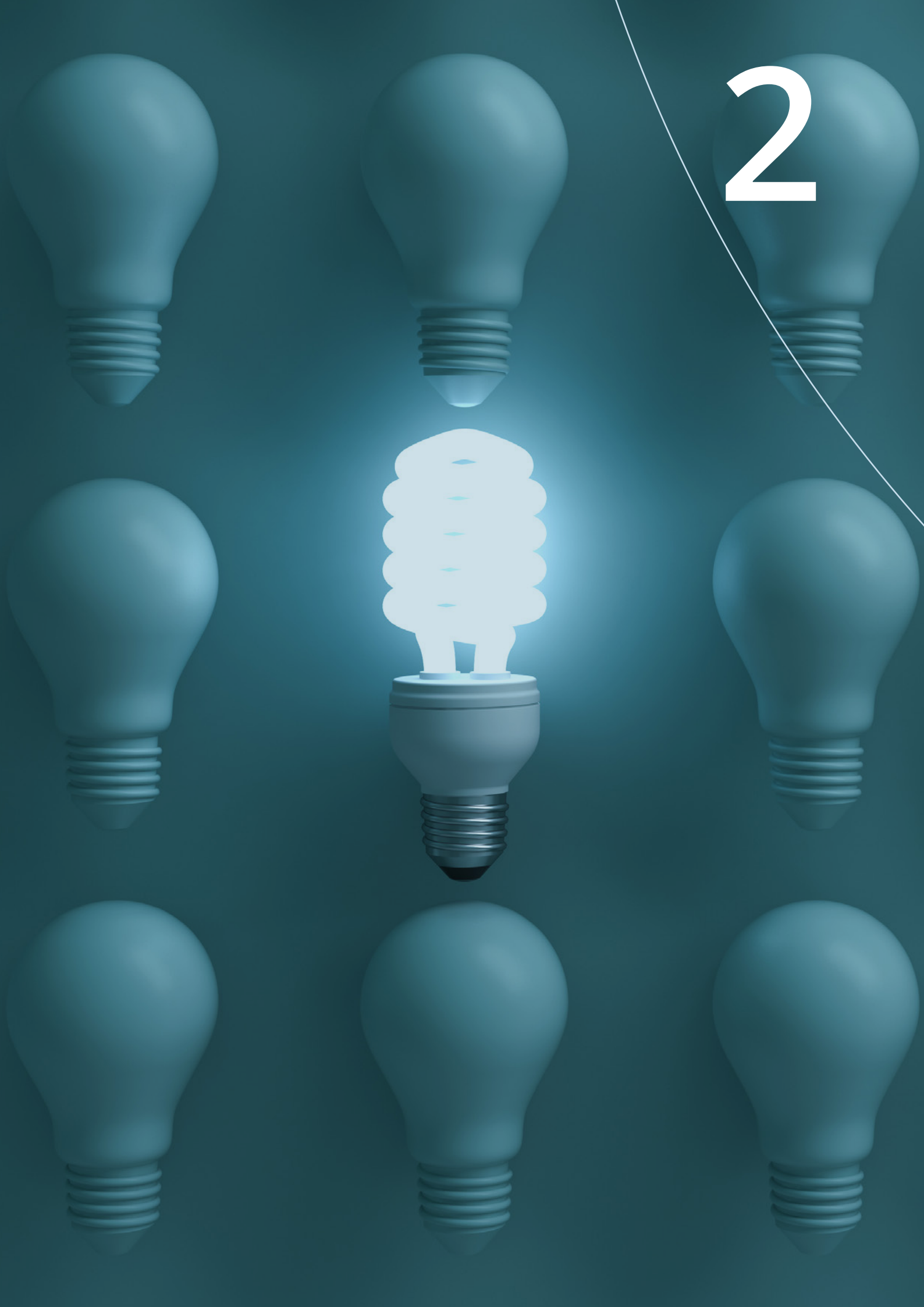
The Review Committee on the Intelligence and Security Services (CTIVD) oversees the lawfulness of the conduct of the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD). The CTIVD has far-reaching investigatory powers to do so which enable it to conduct in-depth investigations **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 is an account and overview of the work and publications by the CTIVD in the reporting year. All the information has already been published on the CTIVD's website. The annual report is a fully public report translated into English and made available on the **CTIVD website**. This is the 2019 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 2019 and lists the items on the agenda for 2020. Section 4 discusses the legal uniformity meetings with the Investigatory Powers Commission (TIB). Section 5 addresses the cooperation between the CTIVD and the oversight bodies of foreign intelligence and security services. Finally, Section 6 describes how the CTIVD's organization developed in 2019.


2

# Activities of the Oversight Department

## 2.1 Oversight of the implementation of the 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 the 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 made a number of specific requests to 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. These 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.

The CTIVD complied with these requests and in December 2018 published its **first - critical - progress report** on the functioning of the ISS Act 2017. That was included in **CTIVD's 2018 annual report**.

The Oversight Department continued on this road in 2019 and issued two progress reports to provide parliament and society insight into how the AIVD and the MIVD apply the legislation in practice. The outcome of these progress reports may also contribute to the independent evaluation of the legislation to be launched before 1 May 2020 as promised by the cabinet. Mid-2020 the CTIVD adopted the fourth and last progress report. Below is an overview of the main conclusions from progress reports II and III. A detailed description can be found on the **CTIVD website**.


**No. 62 | Progress report II on the introduction of the ISS Act 2017**

*Adopted on 6 November 2019, published on 3 December 2019*

The second progress report deals with the progress achieved by the services in implementing legal safeguards. That includes the services' duty of care to ensure that data is processed lawfully, that data is continuously reduced, that there are safeguards in place for investigation-related interception and for international cooperation. The essence of the second progress report is that the services have partly caught up on the backlog of legal and pledged safeguards aimed at protecting citizens. Those safeguards include the obligation to collect and process data in as targeted a way as possible and the obligation to reduce the collected data to only that data which is relevant for the services' tasks. All non-relevant information must be destroyed as soon as possible, to

guarantee as little infringement as possible of the privacy of those citizens who are not the focus of the investigatory power, but whose data is nevertheless stored.

The services have set out the requirement that data is collected and processed in as targeted a way as possible in their policy and work instructions. However, that needs supplementing in certain areas. The AIVD has now largely implemented the standing obligation to assess the data for relevance as soon as possible and to destroy non-relevant data. The MIVD, however, still has a backlog. It also has a less well-developed IT infrastructure.

The AIVD and the MIVD are fully aware of the necessity of internal control on the lawfulness and quality of their data-processing activities (legal duty of care). The services need to continuously monitor compliance with the law by internal control, which also contributes to effective external review by the CTIVD. Both services have adopted policy and instruments for internal control, including risk analyses and audits. The AIVD has also implemented these instruments in practice. By introducing this legal duty, the AIVD achieved considerable progress in a short time. The MIVD has not yet put these instruments into practice. Both services still need to develop internal control mechanisms in a number of areas.

The CTIVD established a high risk of unlawful conduct by the AIVD and the MIVD in the use of automated data analysis. That is a legal general investigatory power of the services which does not require authorization by the minister or assessment by the TIB. Automated data analysis is subject to legal regulations. The AIVD and the MIVD must set additional internal rules for using automated data analysis in the intelligence process and check the functioning of the technologies involved.

**Full report no. 62 with appendices and ministers' response**


### Nr. 66 | Voortgangsrapportage III over de invoering van de Wiv 2017

*Vastgesteld op 6 november 2019, gepubliceerd op 3 december 2019*

In its third progress report the CTIVD established that the decisive steps that the AIVD and the MIVD must take, or continue to take, consist of converting legislation and policy into internal procedures, specific instructions for staff, technical systems and effective internal control mechanisms. The aim is that things work in practice as they should work and that this is verifiable both internally and externally. The technology-neutral wording of the law means that the AIVD and the MIVD must take the necessary action to implement the legal safeguards to protect citizens in practice.

In order to further specify these legal safeguards, the services must adapt their procedure and technical work environment. That is not easy to achieve at short notice. In practice the services are increasingly faced with the situation that the current set-up of their work processes and systems is insufficiently tailored to the requirements set by the law. Adjusting that requires an extensive overhaul and a change in culture.

The services were therefore unable to continue their upward progress over the past period. The risks referred to in the second progress report remain unchanged in this third progress report.

In one area, the CTIVD established that the conduct reviewed did not only constitute a risk, but was unlawful. This concerns the fact that a number of bulk data sets were declared relevant in their entirety. The ISS Act 2017 does not offer scope for this. The CTIVD acknowledges the fact that there are operational interests to store bulk data sets, in particular to identify unknown threats. However it is inherent to bulk data sets that they contain data, the vast majority of which concerns organizations or people who are not the subject of investigation by the services, nor ever will be.

The CTIVD's IT unit took two samples of the application of data reduction and automated analysis of communication meta data (a special investigatory power) in practice. These samples show that the internal control of the lawfulness and quality of data-processing activities (legal duty of care) is still unsatisfactory.

**Full report no. 66 with appendices and ministers' response**

### Development of oversight methods

The new legislation also means that the CTIVD's Oversight Department has expanded its oversight methods. That development continued in 2019. The development of oversight methods is an important topic of discussion in the cooperation between the CTIVD and foreign oversight bodies.

With the introduction of the ISS Act 2017, the CTIVD started using baseline measurements for its progress reports. A baseline measurement provides the Oversight Department with a picture of the extent to which the AIVD and/or the MIVD implement the applicable legal framework in their policy, work instructions, processes and systems. A baseline measurement can be compared to a risk analysis and is used by the CTIVD when, for example, a new investigatory power or a new technology is used. Depending on the outcome of a baseline measurement, the Oversight Department sets its priorities and determines the further structure of its oversight activities. A baseline measurement was conducted in 2019 of the general investigatory power of the AIVD and the MIVD to use automated data analysis. The outcomes were included in the second progress report on the introduction of the ISS Act 2017 (see above).

The setting up of internal control mechanisms, such as assessments and audits, by the AIVD and the MIVD should enable the CTIVD to conduct system-based oversight. This type of oversight is aimed at the functioning of a system (or the whole of systems) for data processing by the services. A standard in-depth investigation conducted by the CTIVD focuses in particular on the results of the data-processing activities, for example whether certain data should have been collected and analyzed and whether that data was rightly classified as relevant. System investigation looks at how the data-processing activities that led to the result in question were set up. In the latter case, the Oversight Department assesses the policy, staffing, organizational and/or technical set-up of data processing procedures by the AIVD and the MIVD. Central to this type of investigation is whether the services themselves have sufficiently guaranteed compliance with legal obligations and their internal control of that compliance. It shows to what extent there is a risk of unlawful conduct. The better the internal control mechanisms, the more the Oversight Department will be able to base its oversight methods on them. By

combining system-based oversight (assessment mainly of the process) and samples of practice (assessment of the result), the CTIVD is able to gain a more comprehensive picture of the lawfulness of both services' conduct quicker than in the past. Whether or not system-based oversight can be used depends on the development of internal control mechanisms by the AIVD and the MIVD.

The CTIVD is also conducting more frequent technical investigations, in order to continue to scrutinize the automated data processing activities by the services. A technical investigation consists of checking the functionality of parts of the services' technical systems and may be aimed for example at the functionality of algorithms, log files or the functionality of technical applications in conjunction with each other. Technical investigation is conducted by the CTIVD's IT unit that was expanded in 2019 in the areas of IT architecture and cyber security. Technical samples were taken in 2019 of the use of the special investigatory power of automated data analysis by the services and the functioning of the data reduction system in practice. The outcomes are included in the third progress report on the introduction of the ISS Act 2017 (see above).

Furthermore, the CTIVD explores the use of automated data processing in oversight itself, e.g. by automated comparison of data processed by the services, with the aim of being able to recognize any processed data deviating from the standard. In other words, the CTIVD looks at data-driven forms of oversight that it may apply prior or in addition to its thematic lawfulness investigations and which will enable it to gain a broader overview of any risks of unlawful data processing by the services.

## 2.2 Investigations completed in 2019

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

For some time now, the CTIVD has focused its attention on large amounts of data (bulk data) processed by the AIVD and the MIVD as well as on the application of new automated technologies in that respect. 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, even though the Act does not contain any explicit safeguards to process bulk data as such. To a considerable extent, this data concerns personal data of citizens who are not the focus of either of the services. For this reason bulk processing by both services is an important overall theme in the CTIVD's oversight.

Cooperation with foreign intelligence and security services is another recurring topic of investigation. Not only should the choice to cooperate with a foreign service be thoroughly weighed beforehand, but the actual cooperation in practice – e.g. providing personal data, carrying out joint operations or providing support to a foreign service – must also be accompanied by sufficient safeguards.

The CTIVD's Oversight Department issued four review reports in 2019. Three of those (reports nos. 63, 64 and 65) are part of the above overarching themes of bulk data processing and international cooperation. The fourth report, no. 67, concerns a topical issue that has been the subject of much political and public debate. An overview of the main findings is given below. The review reports may also be accessed through the **CTIVD website**.


### Nr. 63 | The application of filters in investigation-related interception by the AIVD and the MIVD

*adopted on 17 July 2019, published on 3 September 2019.*

This in-depth investigation was carried out in response to the findings of the **first progress report** on the introduction of the ISS Act 2017, which the CTIVD published in December 2018. In that report, the CTIVD established a high risk of unlawful conduct by the AIVD and the MIVD when using filters in investigation-related interception. This largely new investigatory power allows the services to intercept substantial amounts of bulk communication from either satellite and radio communications or cable and was a key topic during the parliamentary debate and subsequent advisory referendum on the ISS Act 2017.

This investigation focused on whether the AIVD and the MIVD apply filters when using the investigatory power of investigation-related interception and if that use complies with the legal requirements. One of the main requirements is that the services work in 'as targeted a way as possible' when using investigation-related interception, which means that they should collect as little data as possible that is not relevant to their investigations.

For this investigation, the CTIVD assessed the lawfulness of the filtering method in different forms of interception of satellite and radio communications. The CTIVD concludes that the services do filter in practice, but that they failed to sufficiently apply the requirement that they act in 'as targeted a way as possible'. Filtering is mainly based on quantitative factors such as capacity reasons and technical restrictions and not enough on qualitative factors such as preventing unnecessary infringement of citizens' fundamental rights.

Moreover, the CTIVD established that during the period investigated the services themselves did not have a full overview of the functioning of the technical systems used for filtering. In the course of the investigation that overview improved. Internal checks on the composition, functioning and adjustment of the filters, that ensue from the duty of care for data processing, did not take place on a structural basis.

Review report no. 63 has a classified appendix that was submitted to the Committee on the Intelligence and Security Services (CIVD) of the Dutch House of Representatives.

**Full report no. 63 with appendices and ministers' response**


### No. 64 | The use of the special investigatory power of selection by the AIVD and the MIVD

*Adopted on 4 September 2019, published on 15 October 2019*

This in-depth investigation was also carried out in response to the findings of the **first progress report** on the introduction of the ISS Act 2017, which the CTIVD published in December 2018. That report established high risks of unlawful conduct in the compliance with the requirement of 'as targeted as possible' and the duty to reduce data in the system of investigation-related interception.

AIVD and MIVD staff may use the special investigatory power of selection to learn the contents of data obtained with the help of investigation-related interception. The CTIVD established that the AIVD and the MIVD have used the power of selection since 1 May 2018 on intercepted satellite and radio communications. Due to problems in the interception and selection chain, selection at the AIVD partly failed to take place during the investigation period. In September 2018 an incident occurred at the AIVD in which some content data was accessed without the proper authorization. That is unlawful. The AIVD detected this issue itself, reported it to the CTIVD and took appropriate measures.

The requirement of 'as targeted as possible' during selection must be effected by the most specific description possible of the individuals, organizations or topics at which the power of selection is aimed, as well as a substantiation of the corresponding selection criteria. In one of the examined investigations, the AIVD failed to use the power of selection 'in as targeted a way as possible'. The organization at which the selection was aimed had been insufficiently described in the request to use the investigatory power. The substantiation for several individuals linked to that organization by the AIVD was also inadequate. Nonetheless that did not result in an assessment of unlawful conduct, because the selection in this AIVD investigation failed due to technical issues. In other AIVD investigations in which the power of selection was used, the AIVD did duly take the requirement of 'as targeted as possible' into account. The MIVD used the power of selection in 'as targeted a way as possible' in each of the investigations examined.

Data reduction is the obligation to destroy data that is not relevant to the services' investigations ('separate the wheat from the chaff'). To do this, the data obtained must first be examined for relevance. The CTIVD established that the AIVD complied with the data reduction requirement in the two examined investigations where data was actually selected. The MIVD has a well-functioning technical system for selection that ensures the use of selection criteria is accurately registered. However, the way in which the data reduction requirement is implemented needs to be improved. The MIVD wrongfully failed to destroy non-relevant data in two investigations. That is unlawful.

The CTIVD issued recommendations in its review report no. 64 to prevent further unlawful conduct. The review report has a classified appendix that was submitted to the Committee on the Intelligence and Security Services (CIVD) of the Dutch House of Representatives.

**Full report no. 64 with appendices and ministers' response**


## No. 65 | The provision of unevaluated data to foreign intelligence and security services by the AIVD and the MIVD

*Adopted on 11 September 2019, published op 15 October 2019*

When providing unevaluated data, the services have limited knowledge of the actual content and nature of the data. The CTIVD established that in the investigation period (May 2018 - January 2019) the AIVD and the MIVD failed to sufficiently apply the current legal safeguards in their policy and in practice when providing unevaluated data to foreign services.

The services' policy and work instructions regarding the provision of unevaluated data to foreign services fall short in a number of areas. That relates to the definition of the terms evaluated and unevaluated. The CTIVD sets a more specific context for these terms in its review report, in accordance with the legislator's definition. The CTIVD also makes recommendations about amending or supplementing policy and work instructions on the internal registration/recording of unevaluated data provided and where necessary filtering that data beforehand, for example for Dutch technical characteristics and technical characteristics of lawyers and journalists.

In the investigation period, the AIVD and the MIVD only provided unevaluated data to foreign services with which they have a long-term strategic operational cooperation. IThis investigation concerns ten cooperative relationships of the AIVD and twelve cooperative relationships of the MIVD, in the context of which they supplied unevaluated data of a similar nature once or more often. However, both services failed to comply fully with the legal requirements. The CTIVD established several incidents of unlawful conduct in procedure or content at both the AIVD and the MIVD. Several times unevaluated data was provided without authorization by the relevant minister and in some cases the underlying request for authorization failed to comply with the legal requirements for substantiation. Significant improvement is also required of the legally compulsory registration/reporting when supplying unevaluated data (record obligation). Moreover the AIVD failed to comply in all cases with the legal duty to report to the CTIVD. The MIVD did comply with this duty to report in all cases, except where it undertook 'selection on behalf of a foreign service' and the data was classed wrongly as evaluated. The CTIVD made recommendations for improvement.

Review report no. 65 has no classified appendix.

**Full report no. 65 with appendices and ministers' response**


## No. 67| The exchange of data by the AIVD on the Cornelius Haga Lyceum school

*Adopted on 20 November 2019, published on 6 December 2019*

From December 2018, the AIVD issued four reports on the school and on the individuals involved within a short period of time: a state secret intelligence analysis in December 2018, an official message in January 2019 and an official message and simultaneously a state secret intelligence report with financial information, in February 2019. These notices were issued to inter alia the Inspectorate of Education, the ministry of Education, Culture and Science, the city of Amsterdam, the ministry of Social Affairs and Employment, the National Coordinator for Security and Counterterrorism, and the Public Prosecution Service.

The CTIVD finds that issuing the intelligence analysis (December 2018) and the official message (January 2019) was necessary and proportionate given the established threat that pupils of the school could be influenced by the antidemocratic and anti-integration ideology of Salafist leaders. The majority of the content is underpinned by sound intelligence and was carefully phrased, including the information essential to assess the threat.

However, the reports issued by the AIVD also contained a number of substantial deficiencies, that lead to unlawful conduct in part. Parts of the reports were either not properly substantiated or phrased inaccurately. Sentences about links between individuals involved in the school and terrorist groups and about the Salafist nature of the policy and doctrine at the school were therefore provided unlawfully. These elements in the AIVD's reports influenced the image that the outside world has of the school and of the individuals involved. According to the CTIVD, the AIVD should also have been clearer in its reports and communication with the recipients about what the service did not know. Up until that point the intelligence investigation had not established that a Salafist ideology – and the associated anti-democratic or anti-integration message – was being imparted to the pupils at the school. Had that been clear, the recipient government bodies could have assessed the degree of urgency of the reports better. This lack of clarity on the part of the AIVD was negligent.

The CTIVD established that sending the official message containing financial information to the Public Prosecution Service was lawful. However a legal basis was lacking for the financial official message sent to other government bodies and the issued intelligence message with financial information. That information was thus provided unlawfully.

The AIVD held firmly to the legal boundaries in its oral communication with other government bodies about the school and the individuals involved and no information was provided apart from the written messages. In the meeting with the recipients, the AIVD refrained from participating in any decision-making on the measures to be imposed. There is no evidence that the AIVD made any attempts to influence or manipulate.

Review report no. 67 has no classified appendix.

**Full report no. 67 with appendices and ministers' response**

## 2.3 Ongoing investigations in 2019 and planning for 2020

### Progress report IV

With a view to the early evaluation of the ISS Act 2017 intended to start from May 2020, the CTIVD will issue its fourth and concluding progress report mid-2020 on the topics that were raised during the parliamentary debate on the Act and that were submitted to the CTIVD for investigation. In that context, a number of technical samples will be taken of the functioning of the data reduction system and the use of the general power of automated data analysis.

### Ongoing investigation into the acquisition of bulk data sets using the hacking power

The use of the hacking power is an important aspect in the broader theme of bulk processing by the AIVD and the MIVD. The investigation focuses on the question whether there are sufficient safeguards for the use and application of hacks with which large amounts of bulk data may be obtained and processed further. Bulk data sets include data collections of which the majority of the data cannot be linked to the services' targets. Moreover the investigation is important in light of the evaluation of the ISS Act 2017.

### Ongoing investigation into the processing of airline passenger data

The services' use of airline passenger data has led to public debate as it involves a large amount of data (bulk). The CTIVD previously conducted an investigation into the acquisition of bulk data sets offered on the internet (**report no. 55, 2018**) in which it became clear that further investigation into the use of a general investigatory power by the AIVD and the MIVD was important, because general powers are usually equipped with fewer safeguards than special investigatory powers.

The in-depth investigation therefore concerns the question whether there are sufficient safeguards for the acquisition and further processing of large amounts of bulk data based on a general investigatory power, such as the investigatory power to use informants.

### Ongoing investigation into the use of investigatory powers to support a proper execution of tasks

The investigation focuses on 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, 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 regulation is a new element of the ISS Act 2017 and deviates from the principle that the use of the investigatory power must be necessary for the services to properly carry out their tasks.

The investigation also answers the question whether the services notify the CTIVD of the granted authorization in all cases required by law. That duty to report was introduced in the ISS Act 2017.

### Ongoing investigation into the AIVD's conduct in the context of revoking Dutch citizenship

On 1 March 2017 the Netherlands Nationality Act was amended with the addition of Section 14(4), to create a new power for the Minister of Justice and Security. In essence that power means that, for a period of five years after the legislative amendment, the minister may revoke Dutch citizenship of individuals leaving the country voluntarily to join a terrorist organization which poses a threat to the national security. That measure can be taken following an official message by the AIVD or the MIVD. Thus an official message may be the starting for the Minister of Justice and Security to use the power to revoke citizenship.

The emphasis of the investigation is therefore on the lawfulness of the AIVD's conduct. An assessment is also made in that context whether the grounds of the services' decision to issue or not to issue an official message are sound.

### Planned in-depth investigation into cooperation with foreign services in practice

In essence, weighting notes are a written justification for the decision to cooperate with a foreign service within certain limits. In 2020 the CTIVD started an investigation into the functioning of those weighting notes in practice.[1] A key question of that investigation is whether the AIVD and the MIVD remain within the boundaries of the weighting notes in the specific cooperative activities, such as the exchange of personal data and whether these cooperative activities also comply with the requirements of the ISS Act 2017.

## 2.4 Safeguarding the quality and effectiveness of oversight

### Expertise

Technological developments enable the AIVD and the MIVD to collect ever larger amounts of data and to process it in increasingly complex ways. The technological aspect of data processing has become more important. The CTIVD has to adapt to this development to continue to be able to conduct its oversight effectively. The CTIVD reinforced the technological expertise of its staff in 2019 by appointing an IT architect and a cyber security specialist to its IT unit. In addition the CTIVD strengthened its investigatory staff by attracting review officers with operational knowledge and experience in the area of intelligence and security. Section 6 deals with the development of the CTIVD's organization.

[1] The starting date of the investigation had not been announced at the time of concluding the annual report. The CTIVD has already announced an investigation into this topic in its **letter of 26 April 2018 to the House of Representatives on its oversight activities** after the introduction of the ISS Act 2017.

The CTIVD may also attract expertise from outside the organization, under Section 108 of the ISS Act 2017. Thus the CTIVD is able to draft an expert opinion – a theoretical analysis or an in-depth study of a specific issue. The CTIVD did not make use of this option in 2019.

### 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 takes the form of CTIVD staff uninvolved in the investigation group in question taking a critical look at every step of 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 selection 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 each in-depth investigation in 2019. The current participants in the knowledge network are listed on the website of the CTIVD. The CTIVD aims to expand its knowledge network in 2020.

### 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 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 2019 in creating the endowed chair in Intelligence and Law. That endowed chair aims to promote scientific research and the transfer of knowledge relating to legal issues in the field of intelligence and security. The endowed chair will start in 2020 and is facilitated in part by the ministry of Internal Affairs and Kingdom Relations and the ministry of Defence. Jan-Jaap Oerlemans, review officer at the CTIVD, has been appointed to the endowed chair for one day a week from 1 February 2020.

### 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 duties to report relate to cases in which the services fail or are unable to carry out the duty to notify and to the rejection of requests to access data processed by the services. The CTIVD examines these notifications periodically and checks if there is reason to conduct further investigation. Each of these duties to report is included in an in-depth investigation of the CTIVD at some point. See **review report no. 65** (unevaluated data), **review report no. 58** and **review report no. 54** (request to access) and **review report no. 51** (duty to notify).

On the other hand, both services submit reports to the CTIVD that are not required by law, but 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 conduct which is not in accordance with the legal regulation (non-compliance). In those cases the CTIVD makes thorough inquiries at the services and where necessary independently conducts an exploratory investigation.

### Reception of reports within both services

As in previous years, in 2019 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 and the way in which it draws up its reports. It emerges from the consultations that the CTIVD's review reports lead to real changes in the work practice of both services.

### Follow-up of recommendations

Sometime 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.

In 2019 the CTIVD expressly addressed the follow-up of the recommendations in **review report no. 53** on the use of the hacking power by the AIVD and the MIVD (2017). The CTIVD has a positive view of the way in which the recommendations were followed up by the services. That goes in particular for the recommendation on developing policy and procedures to report unknown vulnerabilities ('zero days') in the context of responsible disclosure. In the current investigation into the acquisition of bulk data sets using the hacking power, certain aspects of the services' practice have been reviewed in light of the new legislation.

The CTIVD also focused on the implementation of the recommendations from **review report no. 56** on the multilateral exchange of data on alleged jihadists by the AIVD (2018). In its review report no. 56, the CTIVD made a snapshot, as it were, of the development at that time within several multilateral cooperative relationships in which the AIVD takes part. The recommendations in that report mainly concern reinforcing the safeguards for the legal protection of citizens in joint standards and multilateral agreements within those cooperative partnerships. That includes achieving appropriate and effective oversight on international cooperation. The Oversight Department will continue to deal with this topic and at some point take a second snapshot. In the meantime, the department is exploring how the oversight on international cooperation can be developed further (see also Section 5).


3

# Activities by the Complaints Handling Department

## 3.1 Handling complaints and reports of misconduct

Shortly after the ISS Act 2017 entered into force in May 2018, the CTIVD conducted a baseline measurement into the set-up and procedures for the primary handling of complaints and reports of misconduct at the AIVD and the MIVD, as set down in policy and work processes. Prior to that and also in 2019, the CTIVD held various meetings with the services' legal affairs departments and the ministries about the implementation of the complaints mechanism in practice. The implementation is also assessed, either on request or at the initiative of the CTIVD, when handling complaints filed with the Complaints Handling Department. In addition, developments in the nature 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 2019

### 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 2019.[2]

| Service | AIVD | MIVD |
|---|---|---|
| Pending on 1 January 2019 | 4 | 1 |
| Complaints received | 30 | 15 |
| Declared unfounded | 6 | 1 |
| Declared partly well-founded | – | – |
| Declared well-founded | 1 | 1 |
| Handled informally [3] | 7 | 3 |
| Not handled[4] | 8 | 4 |
| Repealed | 7 | 5 |
| Referred[5] | – | 2 |
| Pending on 31 December 2019 | 5 | 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 2019.

| CTIVD | Klachten t.a.v. AIVD | Klachten t.a.v. MIVD | Overige klachten[6] |
|---|---|---|---|
| Pending on 1 January 2019 | 1 | – | – |
| Complaints received | 38 | 5 | 29 |
| Declared unfounded | 4 | – | – |
| Declared partly well-founded | 1 | 2 | – |
| Handled informally[7] | 3 | – | – |
| Not handled[8] | 22 | 1 | 29 |
| Forwarded to the minister | 6 | 2 | – |
| Repealed | – | – | – |
| Pending on 31 December 2019 | 3 | – | |

[2] The starting date of the investigation had not been announced at the time of concluding the annual report. The CTIVD has already announced an investigation into this topic in its letter of 26 April 2018 to the House of Representatives on its oversight activities after the introduction of the ISS Act 2017.

[3] The numbers were provided by the AIVD and the MIVD.
Handled informally means that a solution was found to the complainant's satisfaction without a formal complaints procedure being initiated.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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 primarily by the minister involved or the complainant failed to respond after the CTIVD asked for additional information.

In total the CTIVD handled 13 complaints in 2019. In 7 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 2019.

*Partly well-founded complaints*
Three of the handled complaints – one about the AIVD and two about the MIVD – were declared to be partly well founded. The complaint about the AIVD concerned the alleged use of investigatory powers against the complainant and partly about the way the complaint was handled by the Minister of the Interior and Kingdom Relations. The CTIVD ruled that the complaint was unfounded where it concerned the use of investigatory powers but founded where it concerned the complaints handling by the minister. The complainant had repeatedly tried to submit a complaint with the minister, but each time his complaint was not recognized as such. The Complaints Handling Department found this to be improper conduct.

One of the complaints about the MIVD concerned repeated requests for information from another government body about the complainant. That emerged from a letter that the complainant had received from the other government body. The complainant stated that the MIVD had wrongly made repeated requests for information. The complainant then inquired with the MIVD. According to the complainant the explanations he received from the MIVD were not convincing and not clear. The CTIVD ruled that the complaint was unfounded where it concerned the repeated requests for information, because its investigation showed that due to a computer error (at the other government body) the complainant had been informed that the MIVD had requested information about him multiple times, whereas in fact this had only occurred twice. The part of the complaint that concerned the explanations that the MIVD had given about the complainant, the CTIVD ruled to be founded. The MIVD had failed to give a clear explanation to the complainant and moreover had failed to check if requests for information about the complainant had in fact been made wrongly. The department therefore ruled the complaint to be partly founded..

The second complaint about the MIVD was about the duration of the security screening, the information provided on the duration of the security screening and how the MIVD subsequently informed the complainant when the MIVD processed the complaint. The CTIVD ruled the complaint to be well-founded on the first point and unfounded on the last two points. In addition, the CTIVD saw cause to assess how the MIVD handled the complaint. The CTIVD found that the MIVD had wrongly handled the complaint by addressing it formally without first attempting to handle the complaint informally. The CTIVD therefore ruled the complaint to be well-founded on this aspect. In the context of the investigation into this complaint, staff from the department responsible for conducting security screenings were interviewed about their procedure for security screenings. These interviews revealed that the statutory period for handling security screenings (eight weeks) was not properly safeguarded. Furthermore, it was unclear who was responsible and when for monitoring the statutory periods and for taking action when there was a risk that the deadline would not be met. Partly based on those interviews, the MIVD informed the CTIVD that a number of changes have now been made to the work process of security screenings to be able to better monitor the progress of security screenings.

*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 three of those complaints to be 'apparently unfounded'. That means that the content of the written complaint itself already showed that the complaint was unfounded. In the case of those three complaints, the CTIVD did not conduct any investigation into the complaints. However the CTIVD did on its own initiative assess the complaints handling procedure at the AIVD for two of the three complaints. The CTIVD ruled that the Minister of the Interior and Kingdom Relations wrongly classified one of the complaints as a repeated complaint, while that was only partly the fact. In the other complaint the CTIVD ruled that the Minister of the Interior and Kingdom Relations had wrongly classified the complaint as a report by a concerned citizen. The fourth complaint was ruled by the CTIVD to be unfounded. That means that the CTIVD conducted an investigation into the complaint and assessed it on its contents. In that complaint, the AIVD's conduct was not found to be improper.

*Informally handled complaints*

Lastly, the CTIVD was able to handle three complaints about the AIVD informally. Two of those concerned the duration of the security screening and the failure to provide the security clearance. The third complaint concerned the failure by the AIVD to respond to an application for access to data. All three complaints were settled by an intervention. Those interventions meant that the AIVD was able to inform the party involved of the state of affairs and, where necessary, apologize for the delay.

### Accessibility of the complaints process

Special investigatory powers are used covertly by both services. That means a citizen will generally be unaware 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. 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 online (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. This was not the case in the complaints handled by the department in 2019.

### 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 Screenings 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 convincing 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 2019 no alleged misconduct has been reported to either service or to the CTIVD.


4

# 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 to 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 2019 focused primarily on the application by the AIVD and the MIVD of the frameworks set by the TIB and the CTIVD. Those mainly involved the application of Section 50 of the ISS Act 2017, the special investigatory power to conduct automated data analysis on metadata obtained through investigation-related interception. In 2019 the TIB and the CTIVD did not publish any legal uniformity letters.

# 5

# International cooperation

In 2019 the CTIVD welcomed oversight bodies from Australia and Germany. In turn it visited the oversight bodies of Belgium, Germany, France, Norway and the United Kingdom. The CTIVD also participated in various international conferences in the field of privacy, intelligence and security and oversight.

### Intelligence Oversight Working Group

In 2015 the CTIVD initiated a joint project in which the oversight bodies of five countries (Belgium, Denmark, the Netherlands, Norway and Switzerland) conducted a similar investigation, each within the framework of their own mandate, and compared their results and experiences. The project ran until November 2018 and resulted in the publication of a **joint statement** in which national legislators were called on to review the existing legal obligation on secrecy between the oversight bodies. Secrecy between oversight bodies proved a significant obstacle to the effectiveness of the oversight of international exchange of data between intelligence and security services. There is a risk of an accountability deficit. The oversight bodies will continue to work closely together in the coming years to fill this accountability deficit.

In 2019 the British oversight body on the intelligence and security services joined the cooperative partnership. Within that cooperative partnership, four meetings were held in 2019. Those meetings focused on the current legal and technological issues that affect each of the oversight bodies and on sharing best practices in oversight. The key objective in that respect is to improve the own oversight methods. In December 2019, the six oversight bodies signed a Charter, in which their cooperation is consolidated, and their cooperative partnership was given the title **Intelligence Oversight Working Group**. The CTIVD is tasked with the secretariat of the cooperative partnership until 2020.

### European Intelligence Oversight Conference

The CTIVD further aims to strengthen a wider European cooperation between oversight bodies. In December 2018 it participated in the first conference of European oversight bodies for the intelligence and security services in Paris. The CTIVD organized a follow-up conference in The Hague in December 2019.

The European Intelligence Oversight Conference 2019 brought together 18 oversight bodies from 16 European countries in the Ridderzaal (Knights' Hall), to discuss the opportunities of reinforcing the oversight on international cooperation between intelligence and security services. The conference was officially opened by the Minister of Defence and of the AIVD. As a result of the contributions to the conference and the discussions that these initiated, the similarities and the differences between the oversight bodies became more transparent. A general conclusion that can be drawn is that the oversight bodies present endorse the urgency to strengthen oversight in an international context.

They expressed their intention to put arrangements in place at least within their own means.

A good result of the conference was the intention to start several smaller cooperation projects on topics that a small number of oversight bodies have in common and to

share the outcome of those projects at a next conference. Oversight bodies are thus progressively working on improving cooperation. In 2020 the conference will be organized by the Italian oversight body after which the British oversight body will take up the baton in 2021.

The CTIVD's website will be updated in the course of 2020 with information on the European Intelligence Oversight Conference 2019.


6

# Organizational developments

## Composition of the CTIVD

For the majority of 2019, the CTIVD consisted of Harm Brouwer (chair), Aad Meijboom (member), Marylène Koelewijn (member) and Addie Stehouwer (member). On 1 November 2019, Nico van Eijk took over the chairmanship from Harm Brouwer. On 1 January 2020, Harm Trip joined the CTIVD as a member.

The CTIVD is divided into two departments:

## Oversight Department

***Harm Brouwer***
*Chair until*
*1 November 2019*

***Aad Meijboom***
*Member until*
*1 January 2020*

***Marylène Koelewijn***
*Member*

**Nico van Eijk**
*Chair from*
*1 November 2019*

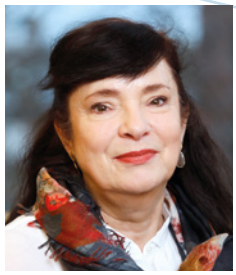
**Harm Trip**
*Member from*
*1 January 2020*

## Afdeling klachtbehandeling

**Addie Stehouwer**
*Chair*

**Hermine Wiersinga**
*Member*

**Jan-Louis Burggraaf**
*Member until*
*1 April 2019*



**Anne Mieke Zwaneveld**
*Member since*
*1 March 2019*

## Composition of staff

The CTIVD's general secretary is Jantine Kervel-de Goei.

At the end of 2019 recruitment efforts were initiated for a new general secretary, as Jantine Kervel will be employed elsewhere from March 2020.

The staff further comprises nine review officers, an IT unit with four specialists and two part-time secretaries.

## Staff development

In 2019, the CTIVD concentrated on further developing its IT unit. The unit was further expanded in July 2019 with the recruitment of an IT architect and a cyber security specialist. The ICT unit advises the CTIVD on the changes that are necessary for it to continue exercising effective oversight of the services' activities, which are becoming increasingly digitized. The unit also advises and supports the review officers, conducts technical investigations and advises the CTIVD in the area of complex technical issues. In 2019 the CTIVD also appointed review officers with operational experience in the field of intelligence and security.

## 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 2019 was 2.5 million euros.

## In conclusion

The second half of 2019 was marked by the departure of Harm Brouwer as chair and Aad Meijboom as member. The CTIVD thanks them for their leadership and commitment over the past years. The CTIVD would also like to express its appreciation for the efforts, expertise and flexibility shown by staff in their work over the past year.

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

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