Annual report 2018

CTIVD

Review Committee on the Intelligence and Security Services

Annual report

2018

Review Committee
on the Intelligence and
Security Services

Preface

Balancing national security and legal protection

The year 2018 was a special one for the AIVD and the MIVD, our intelligence and security services, and by extension for us as independent oversight body CTIVD. The year saw a marked interest in the services from society, politics and the media. That interest was not prompted by any incidents bringing to light shocking revelations, but by the new Intelligence and Security Services Act which came into force on 1 May 2018 and by the outcome of an advisory referendum in the run-up to that legislation. Opponents of the new legislation won the vote on the referendum by a very narrow margin, although it was not always clear exactly what they were opposed to. Based on the outcome of this non-binding referendum, the government made further commitments regarding the contents of the act and the legislation was subsequently introduced. The cabinet also committed to an independent evaluation of the legislation's effect, to be initiated within two years of its introduction.

Prior to the referendum, the CTIVD examined the act in detail, something it had also done a number of times in the design phase leading up to the parliamentary debate. Our final conclusion was that the act was balanced, which means that there was a balance between the importance of protecting national security in our country and the importance of the legal protection of its citizens. In our view, the act met the minimum standards demanded by the human rights treaties to which the Netherlands is bound and by the national and European case law based on them.

In the parliamentary debate on the act, both the House of Representatives and the Senate urged the CTIVD to speed up its oversight on how the AIVD and the MIVD implement and comply with the legislation, in anticipation of the evaluation. Their request found support from the Minister of Internal Affairs and Kingdom Relations and from the Minister of Defence and was honoured by the CTIVD. In December 2018, the CTIVD therefore issued the first of a series of progress reports on this matter. These reports will be published every six months until the evaluation of the legislation starts on 1 May 2020 at the latest and will be made available to parliament and the Ministers involved. The CTIVD's first progress report established that both services fundamentally lagged behind on key aspects in implementing the legislation, in particular in terms of incorporating the obligations for the legal protection of citizens in policy and work processes. That greatly increases the risk of unlawful conduct arising.

It was clear that both the AIVD and the MIVD had underestimated the impact of the new legislative provisions on their policies, their existing work processes and the set-up of their computerized data-processing systems. This is not to say that the services had been twiddling their thumbs in the run-up to the act's implementation. On the contrary, they had put in a lot of work; it was just that the volume of work had been underestimated. The report concluded that both services would have to pull out all the stops to ensure the CTIVD could present a more positive picture in its second progress report that is to be issued in June 2019.

Our first progress report set tongues wagging, and not just in parliament. There was a great deal of media attention with the services promising emphatically to mend their ways. Occasionally, however, a remarkable political view was put forward: the question whether the new legislation involved too many obligations which would adversely impact our secret services' operational strength. Particularly if it meant having to withdraw financial resources from operations in order to implement the obligations that ensure the legal protection of citizens and in order to monitor compliance internally. Apparently some people think that a choice can be made between "either" the importance of our national security "or" that of our citizens' legal protection. That is a false choice, except in circumstances beyond one's control where the law is broken because of an imminent threat - for which accountability will be rendered afterwards. In short, there is no stark choice for 'either/or'. It is a matter of 'both/and'.

It is important to recognize that compared with the former Act of 2002, the new Intelligence and Security Services Act 2017 consists chiefly and in a complementary way of the codification of that which our constitution, human rights treaties and the general principles of data protection already demand of the Netherlands. Our country is expressly bound to these insights and obligations, including by binding court rulings. Likewise, the new legislation codifies the recommendations adopted from the review reports issued through the years by the independent CTIVD.

If the increased administrative and organizational burden of the new legislation could only be borne by structural cuts to the services' operations, that would indeed be a worrying situation. There would only be one solution to that situation, which would be to grant both services an additional budget that would enable them to juggle both national security and legal protection. This means greater financial resources, such as when the services were given new investigatory powers. After all, it's a matter of both: national security and legal protection.

The year 2018, in which the new legislation was implemented, also meant a number of changes for us at the CTIVD. Two departments were set up ('Oversight' and 'Complaints Handling'), our IT expert unit was developed further and our investigatory powers were expanded. Apart from the effects that the new legislation has had, our regular work continued unabated, issuing review reports and handling complaints, as this annual report shows.

For Aad Meijboom and myself, this will be the last annual report drawn up under our responsibility. I will be stepping down on 1 November 2019 and Aad Meijboom on 1 January 2020. Our appointed terms will expire and in view of our age, a second term is not a matter for consideration.

On behalf of my fellow committee members, I hope you enjoy reading this report.

Harm Brouwer
CTIVD chairman


mirror object to mirror
mirror_mod.mirror_object
operation == "MIRROR_X":
irror_mod.use_x = True
irror_mod.use_y = False
irror_mod.use_z = False
operation == "MIRROR_Y":
irror_mod.use_x = False
irror_mod.use_y = True
irror_mod.use_z = False
operation == "MIRROR_Z":
irror_mod.use_x = False
irror_mod.use_y = False
irror_mod.use_z = True
election at the end
_ob.select= 1
er_ob.select=1
ntext.scene.objects.acti
("Selected" + str(modifie
irror_ob.select = 0
bpy.context.selected_ob
ata.objects[one.name].se
int("please select exact
OPERATOR CLASSES
Operos.Operator):
mirror mirror to the selected
ct mirror_mirror_x"
actit.active_object is not

Table of contents

1


0101 001011 10101
11011 001 1101 01
100 110101 000110
11 01110 01 11010
0110 11 01 10 100
- BUSINESS
- NETWORKING
- SOCIAL NETWORK
- TECHNOLOGY
- MEDIA
- CREATIVE
- FINANCE
- INVESTMENT
- CULTURE
- ECONOMY

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 gain an in-depth understanding of the lawfulness of the services' conduct across the full range of their tasks. The CTIVD considers it its duty to provide an insight into the right balance between the interests of national security and the legal protection of citizens. The CTIVD also handles complaints and reports on misconduct by the AIVD and the MIVD. Complaints may be filed by individual citizens and interests groups working on their behalf. At its discretion, it may issue binding decisions on 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 a fully public report translated into English and made available on the CTIVD's website, www.ctivd.nl. Before you is the 2018 annual report.

The annual report discusses the following topics in succession. Chapter 2 deals with the effects of the new legislation, the Intelligence and Security Services Act 2017 (ISS Act 2017), on the CTIVD's organization, its responsibilities and the focus of its oversight activities. Chapters 3 and 4 detail the activities carried out by the Oversight Department and the Complaints Handling Department in 2018 and lists the items on the agenda for 2019. Chapter 5 is concerned with the relationship between the CTIVD and the Review Board for the Use of Powers (TIB). Chapter 6 addresses the cooperation between the CTIVD and the oversight bodies of foreign intelligence and security services. Finally, Chapter 7 describes how the CTIVD's organization developed in 2018.

2

"The new legislation meant a change to the CTIVD's organization, a modification of its responsibilities and a new focus for its oversight activities."

What were the implications of the ISS Act 2017 for the CTIVD?

The Intelligence and Security Services Act 2017 (ISS Act 2017) entered into force on 1 May 2018. The new legislation meant a change to the CTIVD's organization, a modification of its responsibilities and a new focus for its oversight activities.

What changed in the CTIVD's organization?

From 1 May 2018, the CTIVD comprises four members and is divided into two departments: the Oversight Department and the Complaints Handling Department. This separation was effected to guarantee that both departments remain impartial towards each other when forming their decisions. It prevents members of the Oversight Department becoming involved in the decision-making of the Complaints Handling Department and vice versa. CTIVD staff support both departments.

The Oversight Department investigates the lawfulness of the AIVD and MIVD's conduct. Each investigation results in a report that is published in almost all cases. The Oversight Department may also issue an advisory opinion to the Ministers involved in the ISS Act 2017 on request or at its discretion. The Oversight Department comprises three members, of which the chair also acts as chair of the CTIVD.

The Complaints Handling Department handles complaints and reports of misconduct. The Complaints Handling Department consists of a chair, who is also a member of the CTIVD, and a further three members who may be involved in handling complaints and reports of misconduct on an ad-hoc basis.

The new organization structure further entailed an update of the website (www.ctivd.nl), an amendment to the Rules of Procedure published in the Government Gazette, a new consultation structure between the departments and a modification of the internal protocols for oversight and complaints handling.

What changed in the CTIVD's responsibilities?

With the ISS Act 2017 entering into force, CTIVD's complaints handling changed fundamentally. The CTIVD no longer has an advisory role when handling complaints by the Minister involved. From 1 May the Complaints Handling Department handles complaints that have already been handled by the Minister involved at an earlier stage. It may issue binding opinions on the Ministers involved and 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. In fact, handling reports of misconduct is an entirely new task for the Complaints Handling Department and indeed for the CTIVD as a whole.

How has the focus of the oversight activities changed?

Since the ISS Act 2017 entered into force on 1 May 2018, the Oversight Department has concentrated its oversight activities on the scope 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 made a number of specific requests to the CTIVD for accelerated or closer oversight. The cabinet 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 that took place early 2018. The CTIVD complied with these requests and in 2018 published its first progress report on the scope of the ISS Act 2017. The report focused on how both services implement the safeguards for the legal protection of citizens that have either been laid down in legislation or assured in terms of policy. The report further looks at the effectiveness of the oversight which is becoming increasingly dependent on sound internal control mechanisms within the services themselves. The technology-neutral wording of the statutory investigatory powers compel the services to monitor the operation of their data-processing systems themselves, before, during and after using it, including when using new technologies.

The CTIVD will issue a similar report every six months until May 2020 to provide parliament and society with an 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.

For some time now, the CTIVD has paid attention to the large amounts of bulk data processed by the AIVD and the MIVD as well as on the application of new computerized 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 informers 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. 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 umbrella theme in oversight by the CTIVD. 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, executing joint operations or providing support to a foreign service – must also be provided with sufficient safeguards. With respect to these two themes, the ISS Act 2017 offers an enhanced framework that aims to protect citizens' fundamental rights. One example is the requirement that the collected data should be assessed for relevance as quickly as possible and immediately destroyed when not relevant. Another is that unassessed data may only be issued to a foreign service after authorization of the Minister and that the CTIVD must be notified.

Apart from its focus on the operation of the new legislation in practice, the CTIVD also conducts regular thematic lawfulness investigations. In chapter 3 the CTIVD will discuss in more detail the oversight activities it conducted in 2018 and its plans for 2019.

“The technology-neutral phrasing of the services' legal investigatory powers means that the legislation must continuously be converted into practice and clearly set down in internal procedures.”

Which activities did/ does the Oversight Department conduct?

3.1 How does the Oversight Department oversee the implementation of the ISS Act 2017 by the AIVD and the MIVD?

The ISS Act 2017 entered into force on 1 May 2018. This new legislation grants the AIVD and the MIVD investigatory powers to collect data on a very large scale. These large amounts of data have become more complex in nature and both services increasingly use computers to process them. Technological developments and the closer cooperation with foreign intelligence and security services bring another dimension to the data processing by the services. The ISS Act 2017 therefore contains safeguards to reinforce the legal protection of citizens. Important statutory obligations relate to permanent data reduction and an ongoing internal monitoring by the services themselves to lawful data processing.

Oversight activities into the functioning of the ISS Act 2017

From 1 May 2018, the Oversight Department has targeted its oversight activities on the functioning of the new legislation and in particular on those topics that received a great deal of attention in the political and social debate on the act. Using so-called baseline measurements, the Department identifies whether the legal and promised policy-related safeguards have been implemented in the services' practice of data processing. The technology-neutral phrasing of the services' legal investigatory powers means that the legislation must continuously be converted into practice and clearly set down in internal procedures. Essentially, a baseline measurement relates to the availability of policy, work processes and the set-up of technical systems as well as marginally assessing these. In that respect it is comparable to a risk analysis, where the risks for unlawful conduct are identified. The Oversight Department further focuses on the application of parts of the law in practice by means of regular in-depth investigations. The oversight activities into the scope of the ISS Act 2017 will continue at least until May 2020, with a progress report to be published every six months.

No.59 | Progress report on the functioning of the ISS Act 2017

Adopted on 27 November 2018, published on 4 December 2018

The first progress report was published in December 2018. This report deals with the duty of care that the services have to process data lawfully, the continuous obligation to reduce data, the investigation-related interception, international cooperation and procedures for handling complaints and reports of misconduct. The essence of the first progress report is that the services lag behind and both the AIVD and the MIVD have fundamental steps to take in order to implement important parts of the new legislation. Both services are at risk of unlawful conduct. Vital safeguards for citizens' legal protection are still lacking in part or in their entirety, as are their implementation in internal policy, work processes and the set-up of technical systems. There are no instruments for the compulsory internal control and partly because of that the CTIVD is as yet unable to conduct effective external oversight. In the short-term, the AIVD and the MIVD must take concrete steps in their organizations to ensure that the requirements of the ISS Act 2017 are being met in practice. For instance, there is no policy in key parts of data protection (such as the implementation of data protection by design and by default) and there is no identifiable application of the criterion 'as targeted as possible' (e.g. the use of a filter that is as targeted as possible when intercepting data itself and the choice for selection criteria that are as targeted as possible). The data reduction required by law is still very much work in progress, in part because of a flawed supporting IT infrastructure at the MIVD and in part because too little heed is taken of legal safeguards for the computerized metadata analysis (such as prior authorization in all cases and limited access of staff to metadata). Furthermore, the CTIVD is as yet not sufficiently able to effectively oversee compliance with a number of obligations set by the legislation. For example, the instruments for the services' legal duty of care to lawfully process data have not been adequately specified and as a consequence, any ongoing internal checks on important work processes, for example compliance, are lacking. Oversight on compliance is therefore not sufficiently possible.

Development of oversight methods

The Oversight Department began working with baseline measurements: establishing the availability of and marginally testing policy, work instructions, manuals, tools and/or preconditions, offering a starting position for effective oversight. The 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 at that time. A baseline measurement can be compared to a risk analysis and is used by the Department when a new investigatory power or a new processing technology is applied for example. Based on the outcome of a baseline measurement, the Oversight Department determines the further structure of its oversight activities.

Setting up internal control mechanisms, such as assessments and audits, by the AIVD and the MIVD should enable the CTIVD to conduct system-based oversight. This is aimed at the workings of a system (or the whole of systems) for data processing by

the services. Where a regular in-depth investigation by the CTIVD is primarily aimed at the results of data processing, e.g. whether certain data should have been collected and analysed and whether it was rightly designated relevant, a system investigation examines how the data processing that led to the result concerned was 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 point is whether the services themselves have adequately established their internal control of compliance with legal obligations. 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 random checks in 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 may be applied depends on the development of internal control mechanisms by the AIVD and the MIVD.

The CTIVD is also working hard at being able to conduct technical investigations, in order to continue to scrutinize the computerized data processing 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 expert unit that is currently being expanded in the field of IT architecture and internet expertise. Chapter 7 discusses this in more detail.

Furthermore, the CTIVD explores the use of computerized data processing in oversight itself, e.g. by automatically comparing the 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. This will enable it to gain a broader understanding of any risks of unlawful data processing by the services

3.2 Which investigations did the CTIVD conclude in 2018?

The Oversight Department issued one progress report in 2018 (no. 59; see the preceding section) and concluded five review reports. Three review reports were fully public (nos. 57, 58 and 60), one review report was published in a public version and in a more detailed confidential version issued to the Committee on the Intelligence and Security Services (CIVD) of the House of Representatives (no. 56) and one review report issued to the CIVD was completely state secret (no. 61).

An overview is given below of the main findings of the investigations concluded in 2018, unless these are confidential. The public review reports may also be accessed through the website www.ctivd.nl.

No.56 | The multilateral exchange of data by the AIVD on (alleged) jihadists

Adopted on 7 February 2018, published on 28 March 2018

The AIVD is involved in new forms of cooperation with several foreign services. These cooperative partners are in closer physical proximity and they not only exchange data, but also jointly store and further process personal data. Although this contributes significantly to the effectiveness of the cooperation, it also raises new questions on safeguarding the protection of fundamental rights and the effectiveness of oversight. The infringement of citizens' privacy is greater due to the sheer volume of the data exchanged and intensity with which the joint data is processed ('multiplier effect') than is the case when data is simply shared. In its report 56, the CTIVD establishes that additional privacy safeguards are necessary in this respect.

Examples of new forms of cooperation are the operational platform of the Counter Terrorism Group (CTG) opened in 2017 and the CTG database set up in 2016 containing evaluated personal data. The services of 30 countries take part in the CTG. The CTIVD has put forward the recommendation to develop a joint framework for these new forms of cooperation that is based on general principles of data protection and that applies to all participating countries. That means that joint agreements must be made on a range of topics such as in which cases personal data is stored in the database, the reliability of that data, keeping it up to date, management of the database by the AIVD, destroying data that is no longer relevant, etc. There are currently insufficient agreements in place.

Oversight would also benefit from reinforcement in this respect. An adequate level of data protection for these specific forms of cooperation calls for oversight that goes beyond the mere sum of national oversight by each of the participating countries. The CTIVD recommends providing joint oversight. There are several ways in which this could be set up.

The results of the investigation paint a picture of the current situation in developing multilateral cooperation between the AIVD and foreign intelligence and security services. The existing implementation practice of the AIVD is mainly conducted within the framework of the law. All investigated personal data that was exchanged by the AIVD in the period early 2015 to mid-2017 complied with the statutory requirements of necessity, proportionality and due care. However, there are two structural irregularities: risk assessments were not made prior to the cooperation and the reliability of the personal data provided by the AIVD was not clarified.

In the period investigated, the AIVD made active efforts to exchange personal data in multilateral situations faster and more efficiently. New forms of cooperation have quickly developed under pressure from circumstances and the necessity to fight terrorism. It is important that the phase of development in which the cooperation currently finds itself is followed by a phase in which attention is given to adequate joint safeguards for legal protection and effective oversight. The CTIVD's recommendations are aimed at setting additional safeguards and thereby preventing unlawful conduct

by the AIVD and the MIVD (where it concerns sigint cooperation). The Minister of the Interior and Kingdom Relations and the Minister of Defence indicated in their response to the report that they would take action regarding the established unlawful conduct and would make an effort to bring the CTIVD's recommendations to the attention of the relevant cooperative partnerships.

No.57 | The exchange of data within the Netherlands by the AIVD on (alleged)jihadists

Adopted on 13 March 2018, published on 24 April 2018

The AIVD provides oral and written personal data on (alleged)jihadists to other government bodies within the Netherlands, such as the Public Prosecution Service, the Immigration and Naturalisation Service and local authorities. The aim is to notify these bodies promptly of any information they need to carry out their tasks, for instance to take repressive measures against an individual involved. This is done within the context of the Integral Approach to Jihadism action programme adopted by the government in 2014.

The CTIVD's investigation shows that in the investigated period from January 2016 to March 2017 the data provision by the AIVD was necessary in the interest of national security. There was no undue proliferation of data sharing. However, it also emerged that in a number of cases the AIVD did not act with due care. This was particularly the case when sharing data orally in meetings, such as in bilateral meetings with a number of municipalities and in the Coordination Meeting Terrorism (AOT) with the Public Prosecution Service and the police. The staff who participated in these meetings were not given clear guidelines as to what information they were permitted to share in the meetings. No written agreements were made with the chain partners in the action programme about the use of the data shared by the AIVD. This procedure presents the risk of unlawful data provision.

One of the written products discussed in the investigation was the AIVD's publication on individuals who travelled to ISIS territory from the Netherlands: 'Living with ISIS, unravelling the myth' (January 2016). The CTIVD established that this publication, besides its general aim to inform the public on this topic, also had the specific aim of offering concrete information to other government bodies to contribute torepressive measures against individuals. In the light of that specific aim, the CTIVD found that the publication had not been drawn up with the necessary care and that the contents also contained some flaws. In light of the role that this publication may play in criminal proceedings and immigration law proceedings, the CTIVD sent a letter bringing the flaws it established in July 2018 to the attention of the Council for the Judiciary, the Netherlands Bar Association, the Dutch Association of Defence Counsel and the Dutch Association of Asylum Lawyers.

The Minister of the Interior and Kingdom Relations adopted all the recommendations made by the CTIVD.

No.58 | The handling by the AIVD and the MIVD of requests to inspect administrative affairs data

Adopted on 2 May 2018, published on 12 June 2018

The CTIVD investigated whether the requests to inspect administrative affairs data were handled lawfully. These include requests to inspect data related to internal policy (decision making), activities (communication interception statistics), events (international conference held in the Netherlands) or an organization (a former political party or interest group). It concluded that the AIVD and the MIVD generally apply the legal grounds for refusal correctly and disclose the information they ought to disclose, except for some decisions on requests to inspect data in which a limited amount of data was wrongfully not disclosed. In addition, there were some flaws in the inspection process of both services. For example, the processing time was structurally exceeded and the decisions on requests to inspect data lacked the explanation specifying as much as possible the actual grounds used for the refusal. The CTIVD subsequently issued three advisory opinions aimed at better communication with requesting parties, help in effectively wording requests to inspect data and improving the active disclosure of data. In the report and on the basis of interviews with experts by experience, the CTIVD paid heed to societal experiences with the implementation of the right to inspect. This approach was prompted by the bottlenecks and recommendations of the Dessens Committee who evaluated the ISS Act 2002 in 2013, in part on the inspection regime. Both Ministers endorsed the conclusions, recommendations and advisory opinions and implemented them.

This investigation follows on from the investigation into the handling of requests to inspect personal data (review report no. 54). Taken together, these review reports provide a comprehensive picture of how both services implement the right to inspection of the ISS Act 2002. Together with the review report on classifying/declassifying confidential information (no. 33) and the review reports on the implementation of the obligation to notify (nos. 24, 34, 51), the review reports on the right to inspect offer an insight into how the services implement the statutory provisions for the benefit of openness and protection of fundamental rights.

No.60 | Weighting notes of the AIVD and the MIVD for international cooperation with the Counter Terrorism Group and sigint partners

Adopted on 21 December 2018, published on 6 February 2019

The AIVD and the MIVD must lay down the considerations underlying a cooperative relationship with foreign intelligence and security services in a weighting note. This weighting note includes the identification of the risks of cooperation based on the assessment of certain cooperation criteria, such as respect for human rights, legal powers and the abilities of the relevant foreign service and the offered level of data protection.

At the end of 2017, the Minister of the Interior and Kingdom Relations and the Minster of Defence assured parliament that the weighting notes for the lead group of cooperative relationships would be ready when the ISS Act 2017 came into effect. The lead group consists of European security services participating in the cooperative partnership Counter Terrorism Group (CTG) and foreign intelligence and sigint services participating in certain cooperative relationships in the area of sigint. The CTIVD established that this undertaking was met and subsequently assessed the weighting notes on lawfulness.

The investigation shows that the weighting notes of the AIVD and the MIVD are not up to standard in terms of content. Both services fall short on a structural basis when establishing the foreign service's level of data protection. Furthermore, the AIVD failed to identify the legal powers and technical capabilities of its partners and in most cases failed to assess substantively whether the cooperation entailed a risk of contributing to illegal targeting. Some of the investigated weighting notes therefore are unlawful in part because the content reveals little or nothing about why the risks of the cooperative relationship are assessed as limited. However, that does not mean that the cooperative activities conducted with those services are unlawful by definition. The law purposely allows room for cooperation in situations in which action must be taken even with an incomplete understanding of the risks, because the operational importance to protect national security is great.

All the weighting notes investigated by the CTIVD require improvement to some degree if they are to provide a clear understanding of the risks of the cooperation in question. The Minister of the Interior and Kingdom Relations and the Minister of Defence adopted all the recommendations from the report and indicated that the revision of the investigated weighting notes would be completed by 1 July 2019.

No. 61| Investigation at the request of the CIVD

Adopted on 13 June 2018, sent to the CIVD on 26 June 2018

At the request of the Committee for the Intelligence and Security Services (CIVD), the CTIVD conducted an investigation into the facts of an investigation by the AIVD. This concerned a specific case, known as the 'Balie case'. The investigation of the facts conducted by the CTIVD was not aimed at assessing the lawfulness of the AIVD-investigation. It resulted in a review report that was entirely classified as state secret. In issuing this annual report, the number 61 was assigned to the report and the investigation was referenced on the CTIVD's website.

3.3 Which investigations were initiated in 2018 and what is on the agenda for 2019?

Investigation into the provision of unevaluated data to foreign services

This investigation was announced on 26 October 2018 and forms part of the CTIVD's review activities into the scope of the ISS Act 2017. The review report is expected to be published mid-2019.

In its investigation, the CTIVD identifies the nature and volume of the unevaluated data (in particular bulk data) provided by the AIVD and the MIVD and assesses whether it was provided in compliance with the provisions of the ISS Act 2017, such as ministerial authorization. The investigation focuses on assessing the policy, the procedure and the practice of the AIVD and the MIVD from 1 May 2018, when the ISS Act 2017 entered into force, until December 2018.

The investigation also includes the obligation to notify the CTIVD. This obligation to notify was incorporated in the ISS Act 2017 where it concerns the provision of unevaluated data obtained through investigation-related interception. On 25 April 2018, the Minister of Internal Affairs and Kingdom Relations and the Minister of Defence gave the assurance that each authorization granted to provide unevaluated data to a foreign service must be reported to the CTIVD, regardless of the source of the data.

Investigation into the application of filters

During the parliamentary debate on the ISS Act 2017 and in the run-up to the subsequent advisory referendum, a great deal of attention was given to the new investigatory power to intercept bulk data on the cable. The application of 'as targeted as possible' filters is a significant safeguard in the interception process. These filters determine which data may be stored by the services to be processed further and which may not.

In the Progress report of 4 December 2018, the CTIVD concluded that the criterion 'as targeted as possible' was not applied in any recognizable form when filtering interception of satellite and radio communications. The report shows that the criterion had not been implemented in the services' policy or work processes and that the decision-making

processes were not reported. The CTIVD indicated that among other things these observations lead to the conclusion that the risk of unlawful conduct by the AIVD and the MIVD is high. The negative results of the baseline measurement conducted have led the CTIVD to prioritize the topic of filtering. An in-depth investigation will assess whether the detected risks actually manifested. This investigation was announced on 5 December 2018.

The ongoing investigation into the application of filters covers the period from 1 May 2018, when the ISS Act 2017 entered into force, to 1 February 2019. The investigation focuses on filtering interception of satellite and radio communications but is also significant for the investigation-related interception on the cable. This new investigatory power to intercept bulk data on the cable has in particular led to much political and social debate in the run-up to the ISS Act 2017 entering into force. The review report is expected to be published mid-2019.

Investigation into the use of the power of selection

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. In the run-up to the advisory referendum of 21 March 2018 on the ISS Act 2017, public debate centred mainly on the expansion of the existing 'bulk interception powers' of satellite communication and radio traffic to cable (such as internet traffic through cables in the ground). One concern in society is for example the risk of the communication between random citizens being intercepted in the process.

The first progress report into the scope of the ISS Act 2017 prompted this in-depth investigation. In its progress report the CTIVD concluded that the execution of the power of selection carried with it a high risk of irregularities where it concerns compliance with the target requirement and obligation to reduce data. Selection of intercepted communication is based on selection criteria such as telephone numbers, IP addresses and email addresses as well as key words belonging to certain individuals, organizations or topics in which the services are interested. One of the things the CTIVD examines in its investigation is whether the selection criteria are as targeted as possible. It also assesses how both services decide if the selected data is relevant and if irrelevant data is destroyed promptly. This investigation was announced on 5 December 2018. The report is expected to be published in the summer of 2019.

The second progress report

In May 2019 the CTIVD will adopt its second progress report on the scope of the ISS Act 2017. The report is expected to be published mid-June 2019. The report will deal with the specific steps the AIVD and the MIVD have taken to tackle the risks established in the first progress report. Key objectives in this respect are the instruments to be set up and implemented for the services' duty of care to process data lawfully, how the AIVD and the MIVD implement the reduction of data required by law, and how they collect and process data in an as targeted way as possible in the context of the system of investigation-related interception. The CTIVD will also examine the investigatory power of automated data analysis. There are two types of this investigatory power: 1) a specific regulation for the analysis of metadata obtained from investigation-related interception and 2) a general regulation for the automated analysis of all other data collected by both services. Automated data analysis is a core activity of both the AIVD and the MIVD.

Proposed in-depth investigation into bulk hacks

Within the CTIVD and at meetings it has with the TIB, the question is often raised whether there are sufficient safeguards for the use and application of hacks with which large amounts of bulk data may be obtained. The TIB has expressly addressed this issue in its response to the draft amendment of the ISS Act 2017. With a view to a possible interim amendment of the ISS Act 2017 or the evaluation to be conducted two years after the legislation entered into force, further investigation into the use and application of bulk hacks is important. The use of the hacking power is an important aspect in the broader theme of bulk processing by the AIVD and the MIVD. The CTIVD is acutely aware of this theme. The investigation will be initiated before the summer of 2019 and is expected to result in a review report at the end of 2019.

Proposed in-depth investigation into the processing of travel data

A second topic within the theme of bulk processing by the AIVD and the MIVD concerns the use of the services' general investigatory power which also allows for the processing of large amounts of data. The investigation will focus on how the AIVD and the MIVD handle travel data. The investigation will also be initiated before the summer of 2019 and is expected to result in a review report at the end of 2019.

Proposed in-depth investigation into the weighting notes of the AIVD and the MIVD

The Minister of the Interior and Kingdom Relations and the Minister of Defence have said that the weighting notes would be available from 1 January 2019 for all other foreign services with which there is a cooperative relationship and who are not part of the lead group of foreign services on which the CTIVD reported in its review report no. 60. The recommendations from report no. 60 were adopted by the Ministers involved. They indicated that the revision of the investigated weighting notes would be completed by 1 July 2019 at the latest. From July 2019 the CTIVD will investigate whether these two undertakings have been met and whether the substance of the weighting notes is up to standard. The review report on the weighting notes for the other partner services is expected at the beginning of 2020.

Proposed 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. The CTIVD will initiate an investigation into the implementation of weighting notes in practice in the summer of 2019. A key question of the investigation will be whether the AIVD and the MIVD remain within the boundaries of the weighting notes in the specific cooperative activities, such as the exchange of data and joint execution of operations, and whether these cooperative activities also comply with the requirements of the ISS Act 2017. The investigation will also result in a review report at the beginning of 2020.

3.4 How does the Oversight Department safeguard the quality and effectiveness of its oversight?

Expertise

Technological developments are enabling 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 has therefore reinforced the technological expertise of its staff by appointing a data specialist in 2018 for its IT expert unit and by recruiting review officers with knowledge and experience at the interface of IT and law. Chapter 7 deals with the development of the CTIVD's organization.

The CTIVD may also attract expertise from outside the organization. Under Section 108 of the ISS Act 2017, in the CTIVD may make use of an experts' report in the context of an investigation. An experts' report is a theoretical analysis or in-depth study on a particular issue, requested for example if the Oversight Department runs into legal or technical issues on which its expertise is too limited or non-existent or if it wishes to explore a certain element of an investigation in greater depth. It may seek an advisory opinion from an expert and have the specific issue worked out in more detail in an expert's report. For example, an expert's report was drawn up in the context of report no. 56 on the legal grounds for multilateral data exchange (appendix IV of the report). The CTIVD will make investments in the near future to further build up a pool of experts in a broad range of legal areas and technological fields of expertise.

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 expert 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 being involved in the investigations. The members of the knowledge network not only reflect on the CTIVD's schedule and choice of new investigations but also on its action plans, assessment frameworks, findings from 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 current participants in the knowledge network are listed on the website of the CTIVD.

Reflection from society

The CTIVD has a broad network of contacts in interest groups, oversight bodies and scientific institutions in the Netherlands. This helps it to keep in touch with social and scientific debate on balancing the interests of national security and protecting the citizens' fundamental rights involved. The CTIVD expressly recognizes the social debate on the expansion of the AIVD and MIVD's investigatory powers when the ISS Act 2017 entered into force and keeps this in mind when selecting investigation topics. The CTIVD also sees it as its duty, given its impartiality and expertise, to provide insight into how the services implement their investigatory powers in practice and apply safeguards in doing so.

Reception of reports within both services

Following each report, the Oversight Department consults with the work floor staff to find out how the findings and recommendations 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. 2018 saw a focus on this as well. The CTIVD finds these consultations constructive and helpful in improving its oversight duty 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

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.

In 2018, the CTIVD expressly addressed the backlog at the MIVD in implementing their obligation to notify as the follow-up to its recommendation in review report no. 51 (Feb. 2017). Towards the end of 2017, the CTIVD assessed whether the backlog had been cleared in accordance with the Minister of Defence's undertaking. That proved not to be the case. The CTIVD did establish that the MIVD management was taking the backlog seriously and that the organization was working hard to clear it. That led the CTIVD to decide to continue monitoring the process. It subsequently took 1 May 2018 as the benchmark for the MIVD to clear the backlog - the date on which the ISS Act 2017 entered into force. That meant that 1 May 2018 was the completion date for the notification of the use of special investigatory powers based on the ISS Act 2002, which use had finished before or in 2013 and which was thus eligible for a notification investigation five years later, i.e. before or in 2018. Based on its investigation, the CTIVD came to the conclusion that the MIVD had cleared the backlog. It also established that the MIVD had followed the CTIVD's recommendations to prevent any future backlog in the obligation to notify. A contributing factor is that the volume of notification investigations is set to decrease because the power of selection no longer leads to an obligation to notify under the ISS Act 2017. The CTIVD has confidence that the MIVD is now in control when implementing the obligation to notify and has therefore decided that the results of its monitoring do not give rise to any subsequent steps.

4

“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.”

Which activities did/does the Complaints Handling Department conduct?

4.1 How does the Complaints Handling Department monitor the handling of complaints and reports on misconduct by the AIVD and the MIVD?

In the run-up to the new legislation entering into force, the CTIVD held various meetings with the services' legal affairs departments and the ministries about the operation of the complaints regulation in the ISS Act 2017. Shortly after the ISS Act 2017 entered into force, the CTIVD conducted a baseline measurement into the set-up and procedures for handling complaints and reporting misconduct at the AIVD and the MIVD as set down in policy and work processes. The operation of the procedures in practice is assessed, officially or otherwise, when handling complaints filed with the Complaints Handling Department.

On 1 May 2018, the policy regulations of both services for handling complaints and reporting misconduct were not yet ready. By December 2018, when the CTIVD published its first progress report into the scope of the ISS Act 2017, the CTIVD concluded that this was now the case. The regulations are clear, up to date, complete and in line with the applicable legal framework. The policy regulations are sufficiently specific and provide staff with adequate guidelines to properly handle complaints and reports of misconduct. Sufficient information is provided both within the services and outside (on their websites) about how complaints and reports of misconduct are handled by the services. The AIVD and MIVD websites also refer correctly to the CTIVD.

The Complaints Handling Department will formally assess the internal procedures of the service in question when handling a complaint. In addition, there are regular meetings with the services' staff tasked with handling complaints and reports of misconduct. On a periodic basis, both services also submit lists of the complaints they handled or decided not to handle. In this way the Complaints Handling Department is able to monitor developments in internal procedures at both services.

4.2 Which complaints were handled in 2018 and which reports of misconduct were investigated?

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. From 1 May 2018, 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 2018 after the ISS Act 2017 entered into force on 1 May 2018.

Service	Complaints received	Declared unfoun-ded	Declared partly well-founded	Handled informal-ly [1]	Not handled[2]	Repealed	Refer-red[3]	Pending on 31 December 2018
AIVD	18	6	-	8	3	1	-	4
MIVD	5	-	-	2	1	-	2	-

Complaints handled by the Complaints Handling Department of the CTIVD

Below is an overview of the number of complaints processed by the CTIVD in 2018 before and after the ISS Act 2017 entered into force on 1 May 2018.

CTIVD	Complaints received	Declared unfoun-ded	Declared partly well-founded	Not handled	Forwarded to the Minister	Repea-led	Pending on 31 December 2018
Before 1 May 2018 re AIVD	4	4		-	-	-	
Before 1 May 2018 re MIVD	-	-	-	-	-	-	-
After 1 May 2018 re AIVD	17	1	-	10	4	1	1
After 1 May 2018 re MIVD	1	-	-	-	-	1	-
After 1 May 2018, other [4]	8	-	-	8	-	-	-

1 Handled informally means that a solution was found to the complainant's satisfaction without a formal complaints procedure being initiated.
2 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.
3 Complaints filed with the wrong body are referred. The complaints is forwarded to the correct body in consultation with the complainant.
4 In other complaints it was unclear if the complaint related to the AIVD and/or the MIVD.

In total the CTIVD handled five complaints in 2018, including four based on the ISS Act 2002 and one based on the ISS Act 2017. The decision on this last complaint was published on the website of the CTIVD. Of the complaints handled, one complaint was apparently considered unfounded, two complaints were considered unfounded and in two cases the CTIVD decided it partly lacked competence and the complaints were otherwise unfounded.

Those complaints assessed on their content and ruled unfounded by the CTIVD related in each case to the alleged unlawful use of special investigatory powers by the AIVD against the complainants. The CTIVD investigated these complaints and assessed them substantively. The CTIVD is unable to indicate in its advisory opinion before 1 May 2018 or in its decision on the complaint after 1 May 2018 whether or not the AIVD used special investigatory powers. It does indicate whether in its decision the AIVD's conduct against the complainant was improper, but does not specify whether special investigatory powers were used or not. In the current complaints the AIVD's conduct was not found to be improper. Given the nature of the decisions of the Complaints Handling Department, no measures were imposed as referred to in Section 124 (4) of the ISS Act 2017.

Special investigatory powers are used covertly by both services. That means citizens generally are 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 special 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 Complaints Handling Department may only refuse a complaint on a limited number of grounds. A complaint may be lodged 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.

In 2018 the CTIVD checked whether the accessibility of complaints handling was reflected in an awareness in the public domain. It checked if the options for filing a complaint about the AIVD and the MIVD had been correctly and recognizably included on the website of the central government and on the websites of interest groups, other oversight bodies and complaints authorities such as the National Ombudsman. Where necessary the CTIVD alerted the bodies to the option of including a reference to the complaints handling pages on the website of the CTIVD.

Reporting misconduct

The ISS Act 2017 contains a procedure on reporting of alleged misconduct by one of the services or the Coordinator of the Intelligence and Security Services. Such reports may be submitted to the CTIVD. 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 plausible 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 anonymised report on the report on its website.

Since the ISS Act 2017 entered into force in 2018, no alleged misconduct has been reported to either service.

The Complaints Handling Department of the CTIVD received one possible report of misconduct. The Department had insufficient information to interpret the report and to subsequently decide whether or not to handle it. The report was repealed.

5

“The legal uniformity consultations prevent the same legal provision being interpreted in different ways. That not only serves the legal certainty of citizens, but also clarifies to both services the legal framework that applies to the implementation of their tasks.”

How do the CTIVD and the Review Board for the Use of Powers (TIB) relate to each other?

The Review Board for the Use of Powers (TIB) assesses in advance whether the authorization granted by the Minister involved for the use of a special investigatory powers by the AIVD and the MIVD is lawful. Only after the TIB has found the granted authorization to be lawful may the special investigatory powers be used. Broadly speaking, the CTIVD assesses whether the AIVD and the MIVD abide by the law. Its assessment is conducted both during operations and in retrospect and can be more in-depth because, contrary to the TIB, the CTIVD has independent access to the systems and staff of the AIVD and the MIVD. The CTIVD is therefore able to assess the use and application of special investigatory powers within the context of the entire operation and thereby scrutinize the underlying information and decision-making processes of both services. The assessment by the TIB of the lawfulness of the use of special investigatory powers and any restrictions set in that respect by the TIB may help the CTIVD to assess the application of that use.

The TIB and CTIVD regularly meet to ensure the same interpretation of the ISS Act 2017 in what is known as legal uniformity consultations. Both bodies have the duty pursuant to legislative history to consult where necessary and to preserve legal uniformity. Particular interest is given to coordinating the interpretation of legal provisions about special investigatory powers in the ISS Act 2017. The legal uniformity consultations prevent the same legal provision being interpreted in different ways. That not only serves the legal certainty of citizens who gain a greater understanding of the scope and application of the use of special investigatory powers by the AIVD and the MIVD, but also clarifies to both services the legal framework that applies to the implementation of their tasks.

When both review bodies have taken a joint position, they inform the Minister involved and parliament through a 'legal uniformity letter' which is subsequently published on the CTIVD website and the website of the TIB. The legal uniformity letters of the TIB and the CTIVD serve as a framework for the services where the implementation of that legislation is concerned.

In 2018 the TIB and the CTIVD published three legal uniformity letters on the following topics:

1. The legal protection of lawyers and journalists abroad.
Lawyers and journalists abroad should be subject to the same protection regime as lawyers and journalists in the Netherlands. That means that regardless of where a lawyer or journalist is and regardless of their nationality, the same legal protection

should apply. In specific terms this legal protection means that advance authorization for use of special investigatory powers must be granted by the court in The Hague and that there has to be a greater proportionality consideration which must be reflected in the requests for authorization. This is the case when special investigatory powers are used against a journalist when that use could lead to information about their sources being obtained. It also applies to the use of special investigatory powers against a lawyer (direct use) and to processing data relating to confidential communication between an individual against whom special investigatory powers are used and his lawyer (indirect use).

2. The scope of the lawfulness assessment by de TIB.

The AIVD and the MIVD work together with the intelligence and security services of other countries in the interest of national security. This cooperation must be included in the substantiation for the use of special investigatory powers when relevant to the lawfulness assessment. This may be the case for example when data, before it is obtained, is expected to be shared with foreign services or when the use of special investigatory powers takes place with the help of a foreign service. A legal uniformity letter explains more fully in which circumstances the cooperation with foreign services is significant for the lawfulness assessment by the TIB.

3. Automated data analysis pursuant to Section 50 of the ISS Act 2017.

In the political and social debate on the ISS Act 2017, there was a lot of interest in metadata analysis and the extent to which this is an infringement of citizens' privacy. The law states that the AIVD and the MIVD must request authorization from the Minister if they wish to identify individuals or organizations through the automated analysis of metadata obtained by investigation-related interception. That authorization is subsequently assessed by the TIB. Only then may the investigatory power be used. The CTIVD oversees the implementation. The CTIVD also handles any complaints about the use of this investigatory power. This section of the law may seem relatively simple but in practice its implementation proves complex. The legal uniformity letter explains which framework the TIB and the CTIVD attach to the exercise of this investigatory power and how the AIVD and the MIVD should use it.

6

“Secrecy between oversight bodies proved a significant obstacle to the effectiveness of the oversight on the international exchange of data between the intelligence and security services. There is a risk of an accountability deficit.”

How does the CTIVD cooperate internationally?

While the cooperation between intelligence and security services has entered a period of intensification and innovation, the cooperation between oversight bodies is still in its infancy. One of the CTIVD's priorities is therefore to enhance cooperation with its foreign counterparts. The CTIVD has already built a valuable network of bilateral contacts. Oversight bodies from Germany, Sweden and Switzerland were welcomed to the CTIVD in 2018. In turn it visited the oversight bodies of Belgium, Denmark and Germany.

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. In 2018 the CTIVD participated in two meetings with this group of oversight bodies. The project ran until November 2018 and resulted in the publication of a joint statement in which national legislators were called 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 on the international exchange of data between the 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. They discuss current legal and technological issues that affect each of them and share best practices in oversight. The aim is to expand the group of five countries. 2018 also saw the creation of an informal international secretariat that was assigned to the CTIVD until 2020.

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. A subsequent conference will be held in The Hague in 2019 and will be organized by the CTIVD and the Review Board for the Use of Powers (TIB).

In 2018 CTIVD further contributed to various meetings in the field of privacy, intelligence and security, and oversight, for example by holding presentations at the following international events:

- *Intelligence and Oversight* conference, organized by the *Conseil d'Etat and the Commission nationale de contrôle des techniques de renseignement* in Paris;
- *European Intelligence Oversight Network* workshop, organized by *Stiftung Neue Verantwortung* in Berlin;
- *International intelligence collaboration* conference, organized by the *Belgian Intelligence Studies* Center in Brussels;
- *Human Rights*, *Big Data and Technology* workshop, organized by the *University of Essex* together with the *Investigatory Powers Commissioner's Office (IPCO)* in Colchester;
- *Expert meeting 'Networked oversight'*, organized by the *German Institute for Human Rights*, the *Friedrich Naumann Stiftung* and the *Stiftung Neue Verantwortung* in Berlin;
- *International Intelligence Oversight Forum 2018*, organized by the UN Commissioner for Privacy in Malta.

7

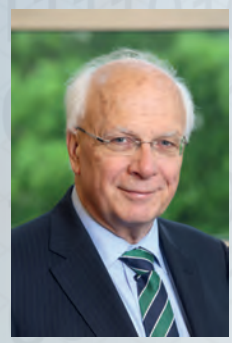
“The CTIVD sets great store by reinforcing its technical and operational expertise. It is also developing new, efficient and more effective oversight methods, preferring to remain compact and incisive in its oversight.”

How did the organization of the CTIVD develop in 2018?

Composition of the CTIVD

Before 1 May 2018, the Committee comprised Harm Brouwer (chair), Aad Meijboom (member) and Marylène Koelewijn (member). From 1 May 2018, there are two departments:

Oversight Department



Harm Brouwer
chair
(also chair CTIVD)

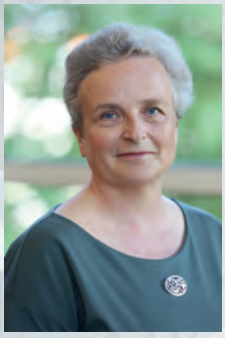
Aad Meijboom
member
(also member CTIVD)

Marylène Koelewijn
member
(also member CTIVD)

Secretary

Jantine Kervel-de Goei
general secretary

Complaints Handling Department



Addie Stehouwer
chair
(also member CTIVD)

Hermine Wiersinga
member

Jan-Louis Burggraaf
member

Wilbert Tomesen
member
(to 1 November 2018)

Composition of staff

The CTIVD's general secretary is Jantine Kervel-de Goei. She took over from Hilde Bos-Ollermann on 1 April 2018. The staff further comprises of (legal) review officers, an IT expert unit, and administrative support.

In 2018, the CTIVD also concentrated on further developing its IT expert unit. On 1 September 2016, an IT adviser who has extensive operational knowledge of signals intelligence (sigint) joined the CTIVD.That was the first step towards the formation of an IT unit. The IT expert unit is to provide expertise in the fields of IT infrastructure, data processing and cyber security. On 1 May 2018, a data specialist joined the IT expert unit. The unit will be further expanded in early 2019 with the recruitment of an IT architect and a cyber security specialist. The IT expert unit advises the CTIVD on the changes that are necessary for it to continue exercising effective oversight on the services' activities that 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 consultation with the AIVD and the MIVD, the CTIVD examines how the services can introduce safeguards into their systems for the purpose of internal control, thereby enabling effective external oversight by the CTIVD.

The CTIVD opted not to expand its number of review officers further in 2018. Although the workforce of the AIVD and the MIVD is growing substantially, any corresponding growth at CTIVD is not necessary. The CTIVD sets great store by reinforcing its technical and operational expertise by attracting review officers with operational experience in the field of intelligence and security and review officers with expertise at the interface of law and IT. It is also developing new, efficient and more effective oversight methods, preferring to remain compact and incisive in its oversight.

Facilities developments

Administratively, the CTIVD falls under the Minister of General Affairs. This means that the CTIVD can call on the Ministry's financial management, IT and HR services. Furthermore, the Ministry of General Affairs, together with the Central Government Real Estate Agency and the States General, realized new and permanent accommodation for the CTIVD. From the end of December 2018, the CTIVD is located at Oranjestraat 15 in the centre of The Hague.

The CTIVD makes its own decisions about spending its financial resources. In connection with the ISS Act 2017 entering into force, the CTIVD's budget was increased from EUR 2 million in 2017 to EUR 2.5 million in 2018.

In conclusion

The new legislation that entered into force entails a lot of work, not only for the AIVD and the MIVD but also for the CTIVD. It has not been easy to scrutinize the data processing by both services in the light of new legal provisions and commitments by the cabinet in the run-up to the entry into force of the ISS Act 2017. Oversight under the ISS Act 2017 requires a great deal of legal consideration, operational know-how, technical expertise and social engagement. The CTIVD is grateful to its staff for their huge efforts and for the skill and innovation they have shown in their work during the past year. Never before have so many meetings been held with the AIVD and the MIVD, the ministries concerned, the TIB, interest groups and knowledge institutions in the Netherlands and oversight bodies abroad as in the past year. We would like to thank our staff for the quality of their hard work and the flexibility they have shown throughout 2018.

P.O. Box 85556
2508 CG The Hague, the Netherlands

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