Annual Report 2017

Review Committee on the Intelligence and Security Services

Annual Report

2017

Review Committee
on the Intelligence and
Security Services

Preface

2017!

The year 2017 was a special year. This is due, in part, to the topics and themes the CTIVD reviewed and investigated. Some of these topics, such as the use of the hacking power and the acquisition of bulk data sets on the internet by our secret services, were subject to public debate. However, the CTIVD also paid attention to topics that were playing in the background but were no less important, such as the way the AIVD and the MIVD fulfil their obligation to actively inform citizens that certain investigatory powers have been used against them (the obligation to notify) and the way they deal with the citizens' right to inspect the data the services keep on them. The reports made of these investigations, as well as the complaints handled in 2017, are summarised in this annual report.

The year 2017 was also special due to the parliamentary debate on the new Intelligence and Security Services Act, the ISS Act 2017, which most certainly did not pass unnoticed. A great many civil society organisations stepped forward, expressed their concerns and brought them to the attention of Parliament. This did not cease when the bill was adopted, resulting in an advisory referendum being held in March 2018. You should be familiar with the results. The majority of the people casting their vote voted against the Act. It is sometimes argued that citizens and politics have drifted far apart. Whatever the truth of that assertion may be, the public debate on the ISS Act 2017 turned out to be intensive indeed. A positive development, especially given that it concerned an Act on the regulation of the powers of a secret service.

The CTIVD has intensively followed the developments on the ISS Act 2017 from its earliest beginnings and has not failed to share its views with the world at large, including with Parliament - as is evidenced by our website. Summarily put, we, like many others, believed that, while the services should be provided with more powers, the Act lacked sufficient safeguards for the legal protection of the citizens. We also found that there were insufficient possibilities to perform effective oversight in a number of respects. Our concerns on many issues were met during the debate on the Act in both Houses of Parliament, by way of legislative amendments, motions, further explanation and promises made. A number of specific promises made to Parliament in December 2017 - i.e., after the Act had been adopted - by a new, differently composed government finally won us over. Our final conclusion was that the ISS Act 2017 is a viable act that strikes a balance between the interests of our national security and the safeguards in place for the legal protection of the citizens and that allows for effective oversight. We explained our conclusion to the public by way of our “Final Balance”.

Read the Final Balance **here**

One item addressed during the social debate I wish to expressly return to. It concerns the question whether the CTIVD when performing its task, i.e., the assessment of the lawfulness of the conduct of the services, is sufficiently able to understand the associated technical applications. The answer is: yes. We have not been idle in this regard over the past two years, both as concerns the preparation of policy and as concerns being properly staffed.

At its core, an investigation into the lawfulness of the conduct of the services is a legal question that will continue to require legal expertise. Due to the increasing role played

by technology in the work of the services, the CTIVD over the past two years primarily hired legal experts whose studies or work experience focused on the theme of IT and law and who have demonstrable affinity with technology. However, we did not find this to be enough. The CTIVD has also established an IT expert unit. This unit is staffed by experts knowledgeable about the working processes of the services and the technical resources (tools) they use, but also, on the more general level, about data analysis processes and cyber and internet technology. We have already hired an IT adviser and a data specialist and will shortly start recruiting an internet specialist. This enables the CTIVD to properly monitor the (automatised) data processing and analysis development processes within the AIVD and the MIVD and to ask the right questions about the composition of the tools.

But that's not all we did. It was on the urging of the CTIVD that a so-called duty of care was finally imposed on the services in the new Act. This duty entails that the management of the services must guarantee the organisational, personnel and technical quality of the data processing processes, including the protection of personal data and the use of algorithms and models. This duty relates, *inter alia*, to ensuring both the accuracy and completeness of the data to be processed and guaranteeing that the tools actually do what they are supposed to do. The CTIVD is responsible for the oversight of the compliance with this duty of care for the quality of data processing. In this way, a new form of oversight on the services' lawfulness is added to the package: system-based oversight, meaning the external monitoring of the internal quality.

The effectiveness of this form of oversight is also determined by the instruments used by the services in fulfilling their duty of care. The CTIVD for a long time urged the legislator to include a range of quality instruments in the Act for this purpose, in line with the regulations which apply to other government services and the market sector under the EU General Data Protection Regulation applicable from May 2018. This has not taken place. In addition to specific policy and procedures, this range of instruments could include audits and privacy impact assessments to be performed when introducing new computerised processing systems. After the Act had been adopted, the new cabinet by way of a letter to Parliament found reason, after all, to order the services to ensure that an adequate range of quality instruments is in place prior to the entry into force of the new Act. The CTIVD is currently awaiting the results of this order and will, from May 2018 onward, also carefully monitor this aspect of the implementation of the ISS Act 2017.

This way, a viable system of oversight on the computerised processing of data has been effected. Whether this system is truly viable will become clear from practice and the independent evaluation to take place within 2 years.

I hope you enjoy reading this report. Should you have any questions or comments, please do not hesitate to bring them to our attention via info@ctivd.nl.

Harm Brouwer
CTIVD chairman

Inhoud

1

Introduction

The Review Committee on the Intelligence and Security Services (hereinafter: the "CTIVD" or the "Committee") reviews the lawfulness of the activities of the General Intelligence and Security Service (the "AIVD") and the Military Intelligence and Security Service (the "MIVD") (hereinafter also referred to as: the "services"). It conducts investigations that result in public reports with, where necessary, classified appendices. In addition, it explores the core activities of and mainly technological developments within the services, in order to be able to carry out ongoing oversight. It also handles complaints about the AIVD and the MIVD.

Every year, the CTIVD publishes an Annual Report before 1 May, which is offered to Parliament and the Ministers concerned. The Annual Report is therefore made public in full. It is also translated into English. This is the 2017 Annual Report.

Read the 2016 Annual Report **here**

The Annual Report has the following structure. In Chapter 2, the CTIVD provides a short description of the Review Reports that have been published in this reporting year. In Chapter 3, we discuss which investigations were carried out and concluded in 2017 and which investigations were launched. Chapter 4 sets out complaints that have been handled by the CTIVD and the related themes. Chapter 5 addresses how the CTIVD has been preparing for the new Intelligence and Security Services Act (ISS Act 2017). In Chapter 6, we discuss how the CTIVD cooperates on an international level. Finally, Chapter 7 explains the composition of the CTIVD in 2017.

2

“CTIVD reports lead to adjustments of procedures. Not just on paper, but also in practice.”

Which investigations did the CTIVD conclude in 2017 ?

The CTIVD published the following five Review Reports between 1 January and 31 December 2017:

- Performance of the obligation to notify by the AIVD and the MIVD (no. 51)
- Use of investigatory powers against lawyers and journalists by the AIVD and the MIVD (no. 52)
- Use of the investigatory power to hack by the AIVD and the MIVD in 2015 (no. 53)
- Handling of requests to inspect personal data by the AIVD and the MIVD (no. 54)
- Acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties (no. 55)

The Committee included a secret appendix providing additional explanation with reports 53 and 55 as submitted to the Parliamentary Committee on the Intelligence and Security Services (CIVD).

A brief overview of the most important conclusions presented in the reports published in 2017 is provided below. The reports are also digitally available on the Committee's website, www.ctivd.nl.[1]

No. 51 | Performance of the obligation to notify by the AIVD and the MIVD

Published on 1 February 2017

The investigation formed the first phase of the wider investigation on the theme of "transparency of the processing of personal data by the AIVD and the MIVD". This first phase concerned the performance of the so-called obligation tonotify. Five years after having used an investigatory power against a person, the services are required by law to investigate whether this person can be notified of this use. In many cases, the person cannot be informed of this in connection with the legal grounds for refusal the services may invoke, such as the protection of sources. The Committee investigated whether both the AIVD and the MIVD have lawfully performed their obligation to notify. In addition, the Committee investigated to which extent the recommendations of the 2013 Review Report no. 34, which solely concerned the AIVD's performance of the obligation to notify, were followed up on.

[1] Report no. 53 on the use of the investigatory power to hack by the AIVD and the MIVD is available in English on www.ctivd.nl.

The Committee found that the decisions regarding notification which were investigated, both those of the AIVD and those of the MIVD, were based on solid grounds. The unlawful conduct identified was mostly of a procedural nature. The MIVD, for instance, fails to take decisions regarding notification in time and exceeded the legal terms in all cases. In addition, central coordination, a general overview, service-wide policy, sufficient documentation and reporting are all lacking within the MIVD. As a consequence, the MIVD lags behind in processing notification decisions. The AIVD still needs to cross some t's as concerns its reporting. The CTIVD recommended that the procedures be changed and, with respect to the MIVD, that it quickly implements procedural safeguards. The Ministers adopted these recommendations.

No. 52 | Use of investigatory powers against lawyers and journalists by the AIVD and the MIVD

Published on 28 March 2017

Lawyers and journalists enjoy additional protection of their communications. The services may only depart from this in case of compelling operational interests, such as when specific indications of a direct threat to national security exist. In this investigation the Committee assessed whether the acquisition and further processing of confidential communications with lawyers and journalists by the AIVD and MIVD is lawful. This investigation was prompted, *inter alia*, by the entry into force in 2016 of the "Temporary regulation on the independent assessment of the use of investigatory powers under the ISS Act 2002 against lawyers and journalists".

On the basis of the investigation, the Committee found that, except for the AIVD in one special case, no investigatory powers had been used against lawyers and journalists. However, the communications between targets of the services and their lawyers and/or journalists have been intercepted at times. This concerned so-called indirect interception. Unlawful conduct was identified in this context. In addition, the Committee found that the policy adopted and procedures followed by the services are lacking with respect to, inter alia, the destruction of data, the requesting of authorisation from the Temporary Assessment Committee and the processing of and access to confidential communications within the AIVD. The latter is permissible only on a need-to-know basis.

The Committee made recommendations to prevent (further) unlawful conduct. It emphasised the importance of more internal control on the careful processing of communications subject to professional privilege. The Committee also made recommendations with respect to the storage and destruction regime in place. The Minister concerned adopted the majority of the recommendations made. The Ministers believed the recommendations with respect to retroactively and regularly checking data files on the unlawful presence of confidential communications to be too labour-intensive.

The Committee in addition called attention to the indirect use of an investigatory power against a journalist, specifically, to the direct use of a power against a suspected source and the communications of that source with a journalist. No additional safeguards exist for such indirect use, neither under the current law nor under the ISS Act 2017. The CTIVD argued for having a protection regime in place that is similar to that applicable to the direct use of the powers. The Ministers did not adopt this recommendation.

No. 53 | Use of the investigatory power to hack by the AIVD and the MIVD in 2015

Published on 25 April 2017

Due to technical developments and changes in society, more and more data is becoming digitally available. By way of this investigation the Committee assessed whether the services have lawfully used the hacking power.

During its investigation, the Committee found that the AIVD and the MIVD in general proceed carefully when using the hacking power and that they in general have made lawful use of this investigatory power. The Committee found that the procedures of the services mainly failed in the areas of the destruction of data, retention terms, reporting, and dealing with unknown vulnerabilities in computerised devices or systems (the so-called zero days).

Read the report **here**

As a rule, the requests for authorisation for the use of the hacking power are carefully substantiated and state which computer systems of which persons or organisations will be subjected to the hack, which purpose is served by the use of the investigatory power and which information is sought by doing so. In a limited number of cases, however, computerised devices or systems not covered under the original authorisation have been broken into. The Committee finds this to be unlawful. In addition, the Committee found that the authorisation procedure for extensions should be improved. Due to administrative processes, the AIVD does not include the latest state of affairs in its requests for extension, which is negligent. The MIVD wrongly did not submit a request for an extension to the Minister. This is advisable, as the nature of an operation may change over time. In one case, the changes in the course of the operation were so significant that they should have been brought to the attention of the Minister (when an extension was requested). This was found to be unlawful.

The most important recommendations of the Committee relate to (increasing) the authorisation level, reporting on the performance, reporting on the use of the so-called zero days, retention terms and the destruction of data. In their responses to the report, the Ministers stated that they would adopt all recommendations made in the report and have committed themselves to implementing measures to prevent the listed shortcomings.

No. 54 | Handling of requests to inspect personal data by the AIVD and the MIVD

Published on 5 September 2017

The investigation into the handling of requests to inspect personal data by the AIVD and the MIVD formed the second and last phase of the investigation on the theme of "transparency of the processing of personal data by the AIVD and the MIVD" (see also the discussion of Report 51, above). The right to inspect means that everyone is entitled to inspection of their personal data as processed by the services. The services may refuse to allow inspection on the grounds of refusal listed by law, such as the current level of knowledge or the protection of sources. In this report the Committee investigated whether the services lawfully handled requests to inspect personal data.

It became apparent that, in general, the services do disclose the data that must be disclosed. Barring some exceptions, the services lawfully apply the legal grounds for refusal when certain data cannot be disclosed. Both services possess a well-maintained register of requests for inspection and the handling of such requests is centrally coordinated.

However, the Committee did find that the AIVD has in some cases wrongly decided not to disclose certain data, invoking grounds for refusal. It was found in this connection that the AIVD in certain respects fails to properly process the decisions within the legal term, to take decisions at the required level of authorisation, to properly record the decision-making process, and as regards the procedure followed by the complaints committee of its Legal Affairs department. The MIVD wrongly decided not to disclose certain data in one decision. In addition, the CTIVD found that the MIVD in certain respects fails to properly process decisions within the legal term, to inform the requesting party accordingly, to properly record the check performed and to inform the CTIVD in case of negative decisions on requests for inspection. The Committee recommends that the services re-assess the data not disclosed and that they pay additional attention to those aspects where their conduct falls short. The Ministers have adopted these recommendations.

On the basis of the previous investigation into the obligation to notify and of this investigation, the Committee concluded that the obligation to notify and the possibility to inspect personal data do not significantly contribute to transparency. The legal grounds for refusal the services may invoke in the interest of national security form a justifiable obstacle to such transparency.

No. 55 | Acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties

Adopted on 28 December 2017, published on 13 February 2018

For the purpose of performing their task the AIVD and the MIVD collect bulk data sets offered on the internet. These data sets may contain large quantities of (bulk) personal data, but also technical information. In some cases, the data set was comprised of data on over 100 million persons. These bulk data sets are offered on the internet by third parties. The legal basis for the collection of such sets is formed by the general power, specifically, the power to receive data from informants when the data set is acquired from third parties and the power to receive data from an open source if the data set is publicly accessible.

In this investigation the Committee assessed the acquisition and further processing of four bulk data sets. It became apparent that the acquisition and processing of the data from these four bulk data sets was necessary for the services' performance of their tasks. Two of the bulk data sets did not contain personal data, but mainly data of a technical nature. The Committee finds the acquisition and processing of these two bulk data sets to be lawful.

The other two bulk data sets did contain personal data, such as names, e-mail addresses and passwords, and their acquisition therefore formed a more serious interference with the right to privacy. The Committee found that authorisation was granted at the proper level (Minister of the Interior) for the acquisition of the first of these two bulk data sets. However, this was not the case for the second of these two bulk data sets (management of the service). The Committee finds the acquisition of the first data set to be lawful and the acquisition of the second data set to be unlawful.

In addition, the Committee investigated the so-called “outer box, inner box procedure”. This procedure forms an important safeguard for the protection of the data of persons included in the bulk data sets. Under this procedure, the entire data set is placed in a so-called “outer box”, to which only a very limited members of staff have access, after its acquisition. If an operational team wishes to access the data in this outer box, it must first request permission. If permission is granted, the selected data is moved to the so-called “inner box” and becomes accessible to more members of staff. The Committee finds this procedure to be lawful.

Based on this investigation, the Committee recommends that clarity is provided on the legal basis for the acquisition and further processing of data in the bulk data sets that the services' staff is informed of this basis. The Committee therefore recommends that a general policy framework on the collection and processing of personal data in bulk is drawn up and published. Finally, the Committee recommends that only the necessary minimum of personal data is processed. The Ministers adopted all recommendations.

Effectiveness in 2017

As becomes clear from the above description, the Ministers involved concurred with the Committee in all cases where it identified unlawful conduct in its reports. With respect to recommendations for the future, such as those related to preventing unlawful conduct, in four out of the five reports (nos 51, 53, 54 and 55) the Ministers adopted those in full. With respect to the use of investigatory powers against lawyers and journalists (report no. 52) the Ministers stated that some of the recommendations would not be adopted, The reason for this was firstly, because they had a different opinion on the legal framework for the use of investigatory powers against journalists and, secondly, because they believed the specific implementation of the careful processing of communications subject to professional privilege which the Committee had proposed to be too labour-intensive. Debate on this issue in the House of Representatives did not produce a different result.

Following reports published in 2017 the Committee consulted with the work floor staff to become aware of how the findings and recommendations are received by the services' workforce. It led to good, constructive talks that showed that the Committee's reports lead to adjustments of procedures, not just on paper, but also in practice. Some time after publishing a report, the Committee requests the Minister to demonstrate the extent to which the recommendations adopted have been followed up on. Where this leads to further questions, the Committee consults with the Minister. If the Committee is of the opinion that the recommendations adopted have not been properly implemented, it informs the Minister accordingly or announces a follow-up investigation. There was no cause for this in 2017.

3

"The 2018 investigation schedule will focus on the functioning of the ISS Act 2017."

Which investigations were ongoing in 2017 and what is planned for 2018?

When selecting various types of investigations, the CTIVD strives to divide its attention equally over the AIVD and the MIVD and over the various activities of both services. The investigations concluded, as detailed in the previous Chapter, mainly related to the use of powers by the services and the rendering of account for this use. In 2017 the theme of transparency was also reflected in the investigation into the handling of requests to inspect so-called administrative affairs data. In addition, in 2017 the CTIVD paid a great deal of attention to the exchange of data with other bodies. The ongoing investigations are set out in brief below.

3.1 Ongoing, not yet concluded investigations in 2017

Investigation into the multilateral exchange of data on (alleged) jihadists by the AIVD
(adopted on 7 February 2018, published on 28 March 2018)

The threat emanating from violent jihadism is a complex and diffuse one. Terrorist attacks like those committed in Brussels, Paris and Londen are prepared and performed within terrorist organisations, cross-border networks, small cells and, sometimes, by lone wolves. The timely recognition, and subsequent removal, of the threat they pose is not a simple task. The Netherlands has elected to adopt a comprehensive approach to fighting jihadism. The General Intelligence and Security Service (AIVD) plays an important part in this connection. On the international level, a very broad range of cooperation initiatives exists, both within and outside of Europe. The multilateral cooperation with foreign services is essential to obtaining insight into the threat posed by violent jihadism to national and international security. The AIVD often plays a leading role in such cooperation and maintains intensive and far-reaching cooperative relations with the intelligence and security services of other countries in this connection.

In 2016 the Committee launched an investigation into the cooperation of the AIVD in international, multilateral partnerships. The investigation examines the exchange of personal data within these forums from the beginning of 2015 to mid-2017. The investigation is focused on whether sufficient safeguards are in place to ensure that the exchange of data by the AIVD meets the legal requirements. The CTIVD assesses how these safeguards are implemented in practice. This report was published on 28 March 2018.

Read the report **here**

Investigation into the exchange of data on (alleged jihadists) within the Netherlands by the AIVD

(adopted on 14 March 2018, publication expected in May 2018)

By way of its "Integral Approach to Jihadism" action programme of 29 August 2014[2] (hereinafter: the action programme)[1] the Netherlands chose a broad approach to tackling violent jihadism. The organisations that subscribe to it work on both the local and the national level, bringing together various disciplines. Persons linked to violent jihadism are subjected to repressive measures to reduce the risks posed by them. The AIVD contributes to these measures by providing data on (alleged) jihadists to government bodies authorised to take measures, such as the Public Prosecution Service or municipal executives, for instance by way of official messages. Due to the attacks in and outside of Europe, this approach has seen a significant increase in social and political attention over the past few years. The urgency of the need to reduce the threat posed by violent jihadism results in mounting pressure to take measures. This requires all parties involved to take quick and decisive action. Especially given this dynamic, it is important to review whether the AIVD has remained within legal boundaries when providing data on (alleged) jihadists.

This was cause for the CTIVD to investigate whether the AIVD acted lawfully when providing data on (alleged) jihadists to Dutch government bodies in the period from January 2016 to March 2017. In this connection the Committee both investigates written documents (official messages, intelligence reports and publications) and the oral exchange of data during meetings. This report is expected to be published in May 2018.

Investigation into the handling of requests to inspect administrative affairs data by the AIVD and the MIVD

(drawn up in February 2018, publication in the summer of 2018)

The right to learn of data processed by the AIVD and the MIVD (right to inspect) provides content to the importance of transparency about the services' activities within the framework provided in the Intelligence and Security Services Act (ISS Act 2002). The underlying notion is that the intelligence and security services grant full disclosure of their activities once keeping them secret is no longer justified in the interest of national security. When this is the case, the general public must be able to perform a check of these activities, the AIVD and the MIVD must render account to society, while journalistic, scientific and historical investigations must become possible.

In view of this function and the importance of the right to inspect, the Committee deemed it important to investigate how the AIVD and the MIVD perform this task. The investigation focuses on requests to inspect administrative affairs data, i.e., data on topics, themes and events. In its investigation, the CTIVD on the one hand considers the lawfulness of the implementation of the right to inspect and on the other explores options to pursue more openness within the limits of the law. By way of this investigation the Committee progresses from its report on inspection of personal data (no. 54, published in September 2017, see Chapter 2). With respect to the AIVD, the investigation relates to decisions on requests to inspect data over the period from June 2016 to June 2017. In the case of the MIVD the Committee's investigation covers

2 *Parliamentary Documents II* 2013/14, 29 754, no. 253 (appendix)

the period from January 2016 to June 2017 due to a more limited number of decisions on requests to inspect data. This report is expected to be published in the summer of 2018.

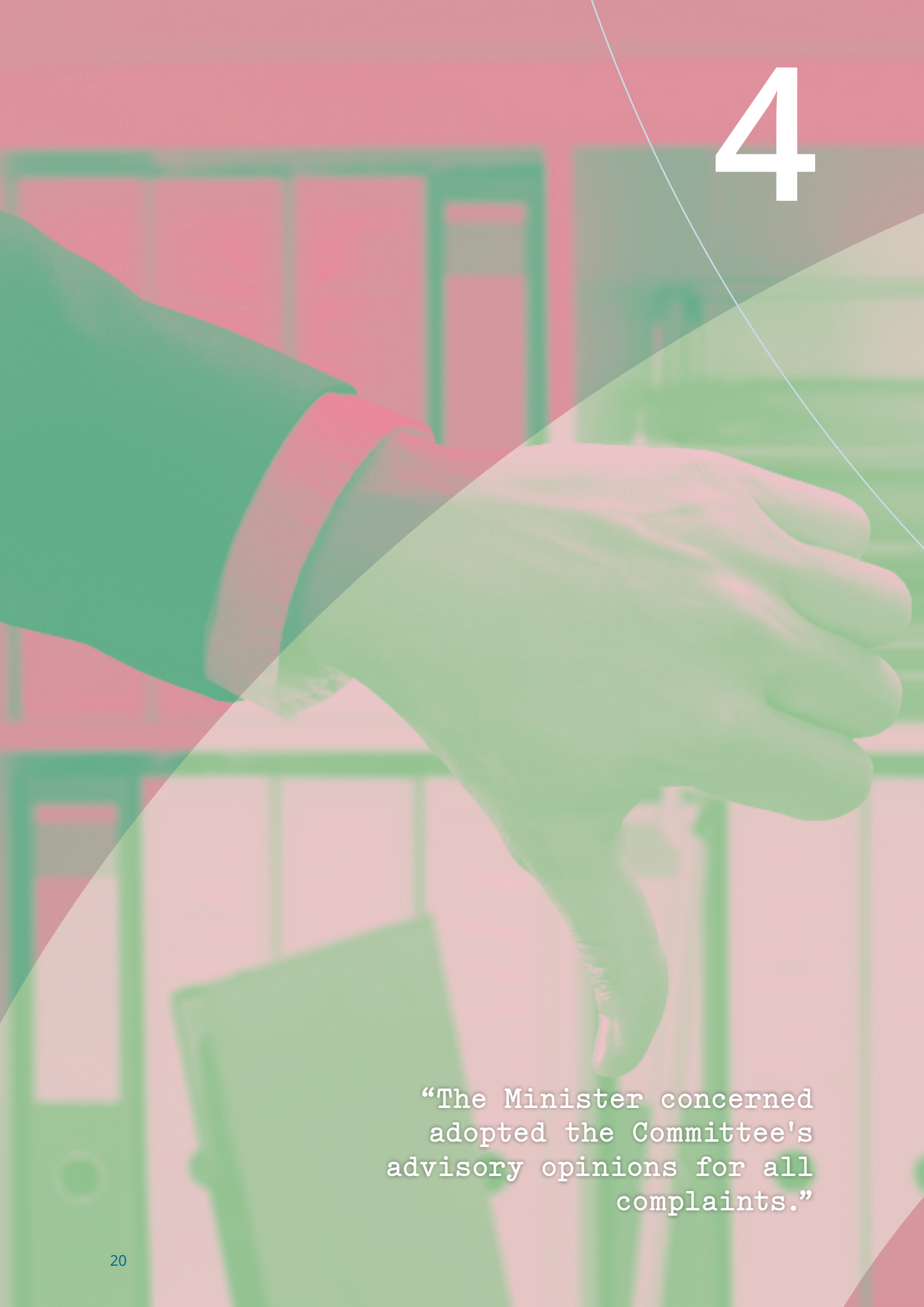
3.2 Annual planning 2018

In 2018, the CTIVD will conclude the aforementioned ongoing investigations with the publication of Review Reports.

From the moment the ISS Act 2017 enters into force, the CTIVD will expeditiously and intensively perform oversight of the activities of the AIVD and MIVD, in particular as concerns the use of new powers. It will do so on the basis of baseline measurements, monitoring and investigation activities. The 2018 investigation schedule will therefore focus on the oversight on the functioning of the ISS Act 2017. This is addressed in further detail in section 5.3 of this Annual Report.

In addition, the CTIVD also leaves time in its annual schedule for requests made of it by Parliament or the Ministers involved and for investigations to be launched in the short term, as prompted by current affairs.

4



"The Minister concerned adopted the Committee's advisory opinions for all complaints."

What complaints were handled by the CTIVD in 2017?

The ISS Act 2017, which will enter into force in May 2018, will affect how the Committee handles complaints. This is detailed further in Chapter 5. Obviously, the complaints about the AIVD or MIVD in 2017 were still handled in accordance with the provisions of the ISS Act 2002. Succinctly put, the applicable procedure is the following. If someone has a complaint about the conduct of the AIVD or the MIVD, they can, pursuant to the ISS Act 2002 and in line with the provisions of the General Administrative Law Act, submit this complaint to the Minister of the Interior or of Defence, respectively. If the Minister decides to handle the complaint, he must engage the Committee as an independent advisory complaints' commission. The Committee will then handle the complaint. It will hear the complainant and examine the relevant files and/or will hear employees from the service concerned. On the basis of its investigation, the Committee will assess whether the conduct of the AIVD and the MIVD the complaint concerns is proper. It will then issue an advisory opinion to the Minister on the merits of the complaint. The Minister is ultimately responsible for deciding whether the complaint is well-founded or not. The ISS Act 2002 allows the complainant to next lodge a complaint with the National Ombudsman.

The number of complaints handled by the Committee in 2017 is presented in section 4.1. The various complaints are then set out in more detail by theme in section 4.2.

4.1 Number of complaints handled

In 2017, the CTIVD handled eleven complaints: nine about the AIVD, one about the MIVD and one about both the AIVD and the MIVD. It issued advisory opinions to the Ministers concerned. At the time the reporting year was concluded, the Committee was still handling one of the complaints about the AIVD. The Committee has seen the number of complaints stay roughly the same over the past few years, with fluctuations in the extent of content-related and judicial complexity.

Number of complaints about the AIVD	Number of complaints about the MIVD	Number of complaints about the AIVD and the MIVD	Advisory opinions
-	-		Manifestly unfounded
6	–	1	Unfounded
1	–	–	Partly unfounded, partly manifestly unfounded
1	–	–	Partly unfounded, partly well-founded
1	1	–	Well-founded

The Minister concerned adopted the Committee's advisory opinions for all complaints.

4.2 Description of the complaints handled

So as to provide a better view of the nature of the complaints, the CTIVD has categorised the complaints by theme. The description is anonymised, so as to protect the privacy of the complainants. The description of the complaints is based on the information released to the complainants by the Ministers concerned.[3]

Use of investigatory powers

The law provides that the AIVD and the MIVD may use investigatory powers in the performance of their task. These powers include surveillance, monitoring and intercepting telephone communications. Any party may submit a complaint about the (alleged) use of investigatory powers by the AIVD or the MIVD to the Minister concerned.

The CTIVD then investigates whether the AIVD or the MIVD has used investigatory powers and, if so, whether that use was lawful. It informs the Minister concerned of the results of its investigation by way of its advisory opinion. The Minister then decides on the merits of the complaint. As a rule, the Minister will not confirm or deny the actual use of investigatory powers in his decision. This information is a state secret, as it may provide insight into a specific procedure or the current level of knowledge of the services.

In 2017 the CTIVD handled six complaints about the AIVD that dealt with the lawfulness of the use of investigatory powers, including surveillance, hacking and interception. With respect to all these complaints, the CTIVD found that no unlawful or other improper action was taken against the complainant, neither by nor on behalf of the AIVD.

Provision of data to a foreign body

The AIVD/MIVD cooperates with foreign services in the context of the performance of the task of the AIVD or the MIVD or in the interest of that foreign service. This cooperation may consist of providing support, for instance by using investigatory powers, or it may consist of the provision of (personal) data.

In 2017 the Committee handled one complaint about the AIVD that dealt with the service having provided personal data of the complainant to various countries, including Turkey and Morocco, causing him to be unable to enter those countries, or to be allowed to do so with great difficulty only. In addition, the Committee handled one complaint that concerned both the AIVD and the MIVD. This complaint concerned the AIVD or the MIVD having cooperated with the Moroccan security service. With respect to both complaints, the Committee found on the basis of its investigation that the AIVD nor the AIVD and the MIVD, respectively, had conducted themselves unreasonably against the complainant.

3 The anonymous nature of the data means that references are simply made to the complainant and "he"; however, this could also be a reference to a female complainant.

Security screenings

Two complaints concerned the length of a security screening. Both complaints were about the AIVD. The Security Screening Act provides that the AIVD or the MIVD must perform a security screening prior to issuing a security clearance to a person in connection with a position involving confidentiality. A position involving confidentiality is a role whereby national security could be damaged, e.g. by leaking state secrets or providing access to targets for an attack. The Security Screening Act provides that a security screening must be completed within a term of eight weeks. This term may be suspended. Persons involved may submit a complaint about the length of a security screening to the Minister concerned.

The first complaint related to the fact that it took so long for the results of a security screening by the AIVD to be provided that the complainant's employer was no longer able to offer him a position, causing him to be dismissed. The Committee established that the security screening took eighteen months. This constituted a very severe exceeding of the legal term. The CTIVD established that the interest of national security did not justify the term being exceeded in this case and therefore was of the opinion that the AIVD had not performed the security screening with the required level of expedience. The Committee also deemed it to be improper conduct that the AIVD had at no point contacted the complainant about the length of the security screening. It advised that the complaint be declared well-founded.

The second complaint also concerned the length of a security screening. In addition it complained about the provision of information by the AIVD and about the fact that the AIVD had not tried to obtain the required data on the complaint via alternative ways. The security screening of the complainant was characterised by the fact that data from foreign bodies was required for the assessment, as the complainant had been abroad for longer than three months in the period under assessment. In such a case the AIVD submits a request for information to the foreign body or bodies. The person concerned also had to request certain data from a foreign body himself, while the AIVD requested data from another foreign body. The Committee found that the AIVD had acted negligently and unreasonably when providing information to the complainant on how to request data from the foreign body concerned. The information provided by the AIVD was incomplete, the service had failed to respond to a request by the complainant to provide more information and the AIVD had only provided the required information to the complainant at a late point in time. With respect to the length of the security screening, the Committee found that the AIVD had not acted sufficiently expeditiously: the security screening had been halted multiple times while the AIVD had caused delays by submitting an incomplete request for information to a foreign body and had only submitted a reminder to that foreign body after eleven weeks had lapsed. It advised that both parts of the complaints be declared well-founded. In addition, the Committee advised that the complaints that the AIVD had failed to obtain the required data on the complainant in an alternative fashion be declared unfounded. The Committee established that the foreign body had failed to respond to the request because it had not received it in proper order and the AIVD had not been informed of this. In the opinion of the Committee, these are not circumstances which require the AIVD to try and obtain information about the complainant via different channels. On the basis of this complaint the Committee issued a number of recommendations with respect to the procedure of performing security screenings to the Minister of the Interior. The Minister has adopted these recommendations, except for one aspect.

Exceeding the legal term for requests to inspect data

Any party may request the AIVD or the MIVD to be allowed to inspect the data processed by the service concerned. The law differentiates between a request to inspect personal data and a request to inspect data other than personal data, also referred to as administrative affairs. Administrative affairs may also concern data on an association or political party. A decision on a request to inspect data must be made within three months. This term may be extended by four weeks once.

In 2017 the Committee handled a complaint about the MIVD which concerned the service having exceeded the legal terms for a number of requests to inspect data. In addition, the complaint related to the fact that the MIVD had not honoured its commitments with respect to its handling of a request to inspect data, as well as to the fact that the decisions on the requests to inspect data did not contain the complainant's reference. The Committee found that the MIVD had exceeded the legal term with respect to fourteen requests to inspect data. It found this to be unlawful as well as improper conduct. With respect to the commitments, the Committee established that the MIVD had indeed made commitments on the handling of the request to inspect data and that these had not been honoured. The Committee found this to be improper conduct, as well. In addition, the Committee did not deem the complainant's request to have his reference number be stated on the decision unreasonable. The Committee found the MIVD's conduct in failing to meet the complainant's request in this connection to be improper.

5

"The CTIVD is able to follow the AIVD and MIVD's development processes in the area of data processing and analysis and to assess the related organisation and applications once the Act enters into force."

How is the CTIVD preparing for the entry into force of the ISS Act 2017

5.1 What was the CTIVD's input in the debate on the bill?

The year 2017 witnessed a great many happenings in the context of the drafting of the new Intelligence and Security Services Act. This new Act *inter alia* serves to grant the AIVD and the MIVD more powers to collect (personal) data on a very large scale. The related bill was passed by the House of Representatives on 14 February 2017 and by the Senate on 11 July 2017. The CTIVD provided input for the parliamentary and public debate, including by the publication, in January 2017, of its "Position", which progressed from its November 2016 "View" on the bill and its letter to the Senate of March 2017.[4] It was critical of the degree to which the bill contained safeguards against the unauthorised use of powers and provided for effective oversight of the conduct of the intelligence and security services. On 25 August 2017, the Intelligence and Security Services Act 2017 (the ISS Act 2017) was published in the Bulletin of Acts and Decrees.

The Act is currently scheduled to come into effect in May 2018. The coalition agreement presented on 10 October 2017, too, referred to the ISS Act 2017, stating, *inter alia*: "No arbitrary and large-scale collection of data of citizens in the Netherlands and abroad ('dragnet') can, may and will take place. The government will therefore rigorously enforce the additional safeguards provided by this Act in practice." On 15 December 2017, the Minister of the Interior submitted a letter to the House of Representatives on behalf of the government that listed additional safeguards for the ISS Act 2017. Early 2018 saw a resurgence of the public debate on the ISS Act 2017. This debate entered a new dimension when an advisory referendum on the ISS Act 2017 was applied for. This referendum was held on 21 March 2018, resulting in a majority vote against the Act.

On 27 February 2018, the CTIVD published its so-called "Final Balance of the New Intelligence and Security Services Act (ISS Act 2017)". Its conclusion was that the ISS Act does sufficient justice to both the interests of national security and the legal protection of the citizen. Moreover, in its capacity as oversight body, it believes the Act to be viable. The Committee found that, over the course of the parliamentary proceedings, the safeguards for the legal protection of citizens have been strengthened. The actual acquisition and storage of personal data, for instance, must be as targeted as possible. In addition, the data stored must be assessed on its relevance, while the use of the data may not be arbitrary. The services have a duty of care for the promotion of the quality

4 All documents are available on www.ctivd.nl. The CTIVD's view on the ISS Act 20xx Bill November 2016) is available in English.

of the processing of data. The new Act and the explanation to this Act therefore provide testable and viable frameworks, also allowing the CTIVD to perform effective oversight.

In its Final Balance, the CTIVD also looked ahead to the implementation of the ISS Act 2017 in practice. Whether a balance between national security and legal protection of citizens has actually been achieved and will be maintained in practice will become apparent from the oversight performed by the CTIVD from 1 May 2018 onward (see below).

5.2 What are the implications of the ISS Act 2017 for the organisation of the CTIVD?

The ISS Act 2017 provides that the CTIVD, from the Act's entry into force on 1 May 2018, will come to be comprised of two departments: (i) the oversight department and (ii) the complaints handling department. This separation of tasks was effected to guarantee that both departments are unbiased when forming an opinion on each other's work. The Members of one department may not be involved in the decision-making process of the other department, for instance.

Succinctly put, the oversight department is charged with the oversight of the lawfulness of the AIVD and the MIVD's conduct. It is composed of the three existing CTIVD Members.

The complaints handling department handles complaints about the conduct of the AIVD and the MIVD and reports of alleged misconduct by the AIVD and the MIVD. It is composed of a Chair and three Members. Ms Addie Stehouwer will be appointed Chair in May 2018. She currently serves as a justice of the Central Appeals Tribunal. Jan-Louis Burggraaf (lawyer practising in Amsterdam), Wilbert Tomesen (vice chair of the Data Protection Authority) and Hermine Wiersinga (justice of the The Hague Court of Appeal) will be appointed Members of the complaints handling department.

Starting 1 May 2018, the CTIVD will be comprised of the three Members of the oversight department and the Chair of the complaints handling department. The Chair of the oversight department will also act as Chair of the CTIVD. The complaints handling department Members are not Members of the CTIVD.

5.3 What are the implications of the ISS Act 2017 for the performance of oversight?

From the moment the ISS Act 2017 enters into force, the CTIVD will expeditiously and intensively perform oversight of the activities of the AIVD and MIVD, in particular as concerns the use of new powers. During the debate on the bill, both the House of Representatives and the Senate have made a number of specific requests on oversight and evaluation to the CTIVD. The government, too, requested the Committee to rigorously supervise proper compliance with the Act in actual practice. In keeping with these requests, the CTIVD will, when performing its oversight, pay particular attention to, *inter alia*, the use of new powers (and whether they are applied in as focused a manner as possible), such as the interception of cable-bound communications in bulk, the process of responsible data reduction when processing data and the application of new technology, specifically in the field of the processing of large amounts of personal

data. It will in this connection assess the actual practice during and after operations, including the investigation plan, the scope and operation of systems and the processes.

The legal tasks of the CTIVD have, so far, always pertained to performing lawfulness investigations. Under the ISS Act 2017, these have been expanded with the oversight on the duty of care for the (automated) processing of data (Article 24 of the ISS Act 2017). This duty of care entails the heads of the services implementing the necessary measures to promote the accuracy and completeness of the data processed and to promote the quality of the processing of data, including the algorithms and models used in this connection. To be able to perform their duty of care, the AIVD and the MIVD must implement adequate tools, such as providing education and training to staff, the drafting of policy, the performance of privacy impact assessments and internal audits. The Committee will monitor this development and subsequently perform oversight.

In May 2018, the CTIVD will perform baseline measurements so as to obtain an overview of the base situation at both services. Next, it will monitor the relevant processes and report its findings on the various aspects of the functioning of the ISS Act 2017 by way of public review reports. By doing so, it will, in 2018 and 2019, provide Parliament and society with an overview of the implementation of the law in practice by the services. These reports may also contribute to the independent evaluation of the ISS Act 2017 to be launched within two years of the Act having entered into force, as promised by the government.

So as to prepare for this evaluation, the CTIVD has increased its capacity and expertise in these areas in 2017. It has closely followed the modifications of the working processes and IT systems of both services and has obtained a solid overview of the current state of the data management and the data processing processes of the services. It has also become further acquainted with new types of oversight. The CTIVD at present deems itself able to follow the AIVD and MIVD's development processes in the area of data processing and analysis and to assess the related organisation and applications once the Act enters into force.

5.4 What are the implications of the ISS Act 2017 for the handling of complaints and for reports on misconduct?

The ISS Act 2017 outlines a new procedure for the handling of complaints. It also introduces a separate procedure for the handling of reports on misconduct.

Complaints handling

Everyone has the right to submit a complaint on the (alleged) conduct of the AIVD or the MIVD to the complaints handling department of the CTIVD. Before a complaint may be submitted to the CTIVD, the Minister concerned - the Minister of the Interior for the AIVD and the Minister of Defence for the MIVD - must first be granted the opportunity to internally process the complaint. If the complainant is unsatisfied with the results of the internal complaints handling, they may submit their complaint to the CTIVD.

An important difference compared to the current procedure, which allocates an advisory role to the Committee, is that under the new procedure the Committee has

the authority to issue binding rulings. In addition, the CTIVD's complaints handling department may, when it finds that certain conduct has been negligent or improper, order that (i) an ongoing investigation be halted, (ii) the use of a power be ceased, or (iii) data processed by the services be removed or destroyed. The Minister must carry out the CTIVD's ruling. He must inform the Committee in writing on how and within what term the ruling will be enforced within two weeks of having received it. The CTIVD will publish an anonymised report on the complaint on its website. Incidentally, the CTIVD is not granted the authority to award damages; this remains the sole province of the civil courts.

Handling of reports on alleged misconduct

The ISS Act 2017 contains a procedure on the 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 complaints handling department of the CTIVD. Every person who is or has been involved with the performance of 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 plausible for misconduct to have occurred. The reporter and the Minister concerned are both granted the opportunity to explain their positions. The CTIVD's complaints handling department will draw up a report on the basis of its investigation. It informs the reporter and the Minister of its opinion and may include recommendations to the Minister. Next, the Minister informs the CTIVD on how and within which term it will follow up on this opinion. The opinion of the CTIVD's complaints handling department and the Minister's response are submitted to one or both Houses of the States General by the latter. The CTIVD will publish an anonymised report on the report on its website.

Preparing for the new practice

In 2017 the CTIVD spent a great deal of time and effort on making preparations for the tasks its complaints handling department will come to perform once the ISS Act 2017 enters into force. The rules for the handling of complaints and of reports on misconduct provided in the ISS Act 2017 have been translated into internal policy and procedures. In this connection the CTIVD has had regular contact with parties active in the field and with peer advisers. The chair and the members of the complaints handling department are responsible for adopting the policy and the procedures. They are expected to be able to fulfil their positions as from 1 April 2018.

The procedures for the handling of complaints and of reports of alleged misconduct will become available on the CTIVD's website once the ISS Act 2017 enters into force.

6

"The CTIVD believes it important for new initiatives to be started up once this first international cooperative partnership is completed."

How does the CTIVD cooperate internationally?

The arena of the intelligence and security services is developing at a rapid pace. This is particularly notable in terms of technology, but also in the field of the international cooperation between the intelligence and security services. And it's not just the CTIVD that is confronted with these developments: the same applies to its fellow oversight bodies. There is, therefore, great value in exchanging experiences and insights. For this reason, the contact with the oversight bodies of other countries is of great importance to the CTIVD.

While the cooperation between the intelligence and security services has entered a period of intensification and innovation, the cooperation between the oversight bodies is still in its infancy. In 2015, in connection with a joint project, the oversight bodies of five countries for the first time all conducted a similar investigation, each from their own national context and within the framework of its own mandate, and compared their results and experiences. The exchange of data on (alleged) jihadists was chosen to be the topic of this investigation. In 2016 and 2017, the oversight bodies of Belgium, Denmark, Norway, Switzerland and the Netherlands exchanged experiences obtained from their own ongoing investigations into this subject, which resulted in a more in-depth understanding and a more complete overview of the international cooperation between intelligence and security services. A start was made with drafting a joint report in late 2017. As the various oversight bodies each use a different approach and have to observe their own regulatory frameworks on the disclosure of information, this turns out to be no easy affair. Publication of a joint report is currently scheduled for 2018.

The CTIVD believes it important for new initiatives to be started up once this project is completed. It has in this connection joined with the four aforementioned oversight bodies, and a number of others, to explore what possible steps can be taken to expand and boost the cooperation. The oversight on technical processes, such as the acquisition and (automatised) processing of large quantities of data, would be a good example of a topic suitable for such cooperation.

In 2017, the CTIVD also participated in multiple international meetings, including workshops organised by the European Union's Fundamental Rights Agency and the International Intelligence Oversight Forum set up by the UN Special Rapporteur on Privacy. In addition, the CTIVD hosted delegations from Indonesia, Switzerland and Germany in 2017. -

7

What were the developments in the CTIVD organisation in 2017?

Composition of the CTIVD and support

In 2017, the Committee was composed of Harm Brouwer (Chairman) Aad Meijboom (Member) and Marylène Koelewijn (Member). Hilde Bos-Ollermann served as the General Secretary of the CTIVD in 2017. The bureau in 2017 expanded to comprise nine investigators, one IT adviser and two (part-time) secretaries.

Harm Brouwer
Chairman

Aad Meijboom
Member

Marylène Koelewijn
Member

Hilde Bos-Ollermann
General Secretary

Facilities developments

The Ministry of General Affairs is the managing ministry that provides services to the CTIVD with respect to financial management, IT and personnel issues. The CTIVD receives the cooperation that it requires from the managing Ministry. It makes its own decisions about spending its financial resources. The CTIVD's budget has increased from EUR 1 million in 2014 to EUR 1.4 million in 2016, to EUR 2 million in 2017 and to EUR 2.5 million in 2018. This allowed the CTIVD to properly prepare for the additional tasks it must perform under the ISS Act 2017.

As of May 2017, the CTIVD is housed in a temporary accommodation at Frederikkazerne in The Hague. The preparations for a new accommodation in the centre of The Hague are in full swing.

Staffing activities in preparation of the ISS Act 2017

Due to the aforementioned increase in its financial resources, the CTIVD had room to attract new staff in 2017. In preparation of the entry into force of the new ISS Act, it mainly focused on attracting new investigative staff who possess a technical as well as a legal background or specific knowledge about privacy law and the protection of

data on the Internet and in the cyber domain. Moreover, the CTIVD recruited a data specialist in early 2018 and will recruit an IT expert specialised in the cyber domain and Internet technology over the course of 2018. In addition, the CTIVD in 2017 explored the possibilities of engaging ad hoc technical expertise jointly with other oversight bodies.

Finally

The CTIVD's performance of its oversight task is developing rapidly. While, naturally, the aforementioned increase in staffing is a contributing factor, even more important was the involvement, substantive quality and inventiveness of the members of staff themselves in 2017. It is thanks to its staff that the CTIVD is able to focus its oversight activities on a multiplicity of topics, is in the possession of high-quality legal expertise, is able to consider the activities of the services from a variety of angles and is making good headway with the preparations for the many challenges arising from the implementation of the ISS Act 2017. It therefore wishes to express its heartfelt gratitude for their commitment in 2017.

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl