Annual Report 2016

IT expert unit being set up

International Cooperation

Responses to the new ISS Act

Oversight & effectiveness

Five Review Reports

"While a lot is going well, improvements can and must be made"

Thirteen complaints

CT IVD

Review Committee on the Intelligence and Security Services

Annual Report

2016

Review Committee
on the Intelligence and
Security Services

Preface

2016 and beyond!

The CTIVD's primary focus in 2016 was on the exercise of its legal task: reviewing the activities of our secret services, the AIVD and the MIVD.

The Committee performed its task in its customary manner, by issuing Review Reports and submitting advisory opinions on complaints about the services lodged by citizens to the Ministers. These Review Reports in accordance with the law eventually made their way to our Parliament, where they, to varying degrees, became topics for debate and political decisions. This Annual Report briefly addresses the review and advisory reports published in 2016.

The overall picture of 2016 is consistent with that of previous years. A lot is going well, and the unlawful conduct identified is limited in scope and generally not of a structural nature. However, the identification of such shortcomings does imply that improvements can and must be made. Extra attention must still be provided to the services' use of their powers against special categories of citizens, like lawyers. The assessments made by the AIVD and MIVD as to whether a foreign service may be cooperated with and the related implementation of the applicable cooperation criteria, too, continue to require attention, especially given that a great many developments are taking place in the context of the cooperation with foreign services. Finally, there are concerns about the services' data management systems, especially with respect to the destruction of personal data that is not, or no longer, relevant for the performance of their tasks. In addition to this overall picture, the CTIVD, on the basis of its extensive experience in performing its oversight task, finds that both the AIVD and the MIVD demonstrate a high level of professionality in their operational performance as intelligence and security services and produce results accordingly.

As could be expected, the CTIVD in 2016 also devoted attention to the new Intelligence and Security Services Act, which has been adopted by the House of Representatives and is currently being debated by the Senate. The Committee already submitted an extensive response when the preliminary draft was subjected to an internet consultation in 2015. Following the introduction of the Bill to the House of Representatives, the CTIVD next submitted its View, supplementing this with its Detailed Position during the plenary hearing. The aforementioned documents received due attention during the debate on the Bill and resulted in it being amended in certain respects.

Key to the CTIVD's position was the question whether the Bill sufficiently addressed the performance of effective oversight in view of the expansion of the powers granted to the services. In November 2016, this question had to be answered mostly in the negative. A more affirmative answer could be provided following the adoption of the amended Bill by the House of Representatives, as some of the criticisms levelled had been addressed. However, the Bill is still insufficiently clear in a number of respects. In its March 2017 letter on the amended Bill to the Senate, the Committee once again explained its position.

I do want to single out one other issue, which relates to the recurring concerns expressed about the CTIVD's own functioning. I refer to the alleged lack of technical know-how possessed by the Committee. This criticism is a justifiable one, and we have taken a number of steps in 2016 to remedy the matter. The CTIVD established an IT expert unit that will, *inter alia*, delve into the operations of the services' increasingly automatised data processing systems, from the initial collection of data, through its analysis, selection and use, to its destruction. This unit is currently being set up. One IT adviser familiar with the services' systems has already been recruited. More staff will be attracted once the CTIVD is granted additional funding in connection with the implementation of the new Act. A long-term action plan, which consolidates technical knowledge and legal expertise relevant for our oversight task, has recently been completed and is currently being executed. Please refer to our website for this plan. But here I am, already discussing 2017 too much!

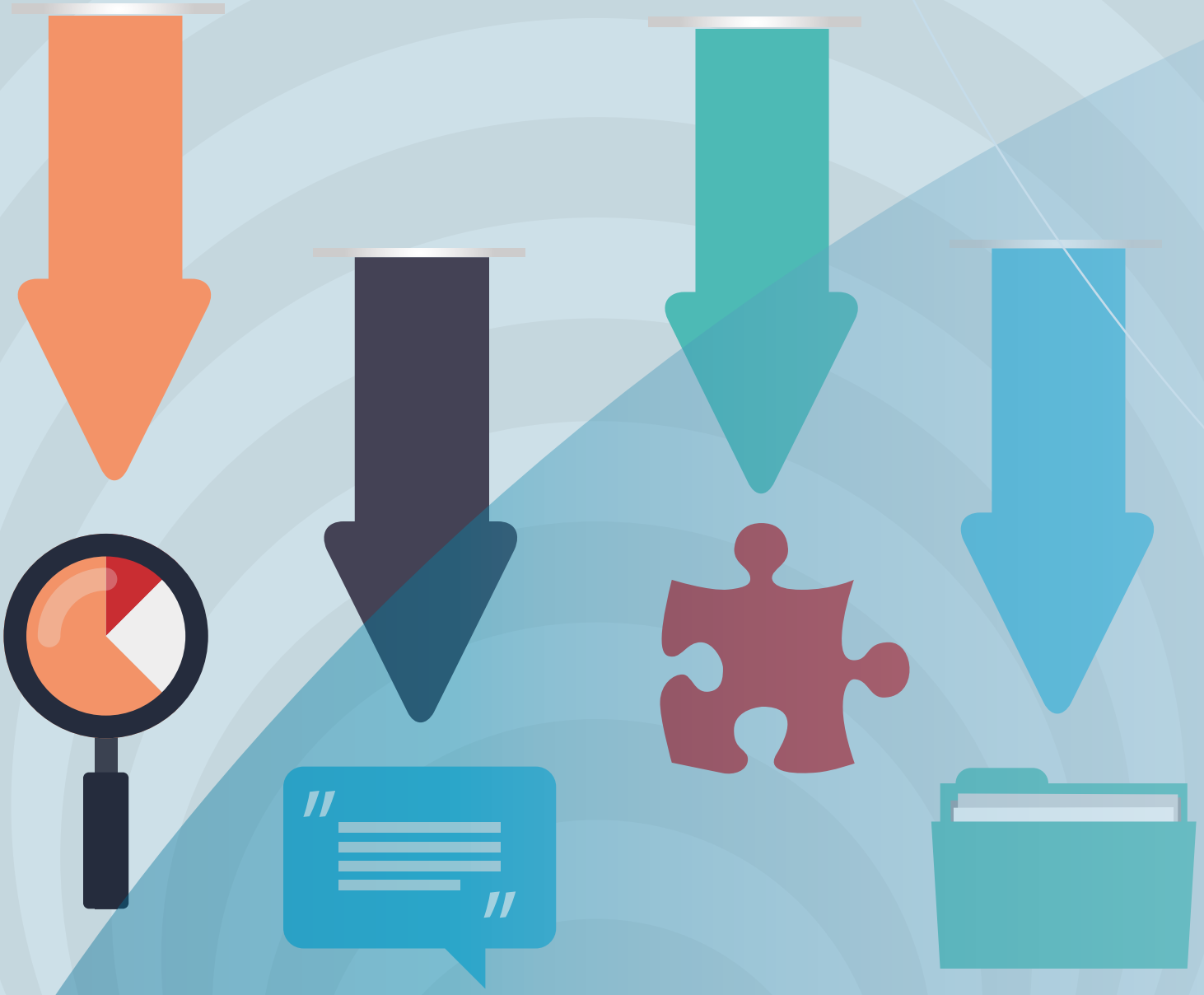
The year 2016, the subject of this report, is presented to you in the below. Should you wish to raise any questions or to submit a response, you are most cordially invited to do so.

On behalf of the Review Committee on the Intelligence and Security Services

Harm Brouwer
Chairman

Inhoud

1



Introduction

The Review Committee on the Intelligence and Security Services (hereinafter: the "CTIVD" or the "Committee") reviews the legality of the activities of the General Intelligence and Security Service (the "AIVD") and the Military Intelligence and Security Service (the "MIVD"). 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 serves as advisory complaints commission for the handling of complaints lodged about the AIVD and the MIVD (hereinafter also: the "services").

Every year, the CTIVD publishes an Annual Report before 1 May, which is offered to Parliament and the Ministers concerned. The Annual Report is made public. It is also translated into English. This is the 2016 Annual Report.

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 2016 and which investigations were launched in 2016. Chapter 4 addresses the effectiveness of the oversight. Chapter 5 sets out complaints that have been handled by the CTIVD and the themes therein. Chapter 6 examines developments in relation to the new Intelligence and Security Services Act. In Chapter 7, we discuss how the CTIVD cooperates on an international level. Finally, Chapter 8 explains the composition of the CTIVD in 2016.

2

"When carrying out its oversight tasks, the CTIVD always strives to provide maximum transparency about its findings."

Which investigations did the CTIVD conclude in 2016?

The CTIVD published the following five Review Reports between 1 January and 31 December 2016.

- The use of interception powers and the power to select sigint by the AIVD (no. 46)
- The use of interception powers by the MIVD (no. 47)
- The implementation of cooperation criteria by the AIVD and the MIVD (no. 48)
- The exchange of unevaluated data with foreign services by the AIVD and the MIVD (no. 49)
- Contributions of the MIVD to targeting (no. 50)

The primary reason for conducting these investigations is the nature of these activities of the services, which infringe on fundamental rights and freedoms, and the related political and social debate on these activities. When carrying out its oversight tasks, the CTIVD strives to provide equal attention to the AIVD and the MIVD and to provide maximum transparency about its findings. It publishes its Review Reports on its website. It submitted a confidential appendix to reports 46 and 47 to the House of Representatives Committee on the Intelligence and Security Services containing an overview of the cases reviewed. A brief overview of the most important conclusions presented in the reports published in 2016 is provided in the below. The reports are available in full on our website, www.ctivd.nl.

No. 46 | The use of interception powers and the power to select sigint by the AIVD

Published on: 9 February 2016 (not available in English)

The AIVD's power to intercept communications and to select non cable-bound telecommunications obtained by untargeted interception are of substantial importance to its performance of its tasks. Yet, at the same time, the use of such powers involves extensive interference with the right to privacy. For this reason, the CTIVD, as in previous years, investigated the use of these powers. This latest investigation covered the period from March 2014 through February 2015.

The CTIVD's overall view of the use of these powers by the AIVD is positive. The AIVD in general uses its powers in a well-considered manner. In the vast majority of operations reviewed the AIVD had made lawful use of its powers and had acted with due care The Committee identified unlawful conduct in a limited number of operations, where the considerations of the AIVD should, in the opinion of the CTIVD, have resulted in a different decision. In these cases, the use of the interception powers or the writing out of communications was not necessary or proportional, for instance.

In this report, the Committee pays special attention to the use of the power to intercept the communications of lawyers. It did not identify any unlawful conduct or lack of due care with respect to the direct interception of the communications of lawyers. However, with respect to the indirect interception of the communications of lawyers – for instance, by way of the communications of their clients – the Committee found that the AIVD failed to meet the more stringent proportionality test in thirteen cases. It therefore found that the writing out of these conversations was unlawful. The Minister of the Interior and Kingdom Relations in his response to the report stated he will terminate the operations found to be unlawful or, as the case may be, destroy the results thereof.

No. 47 | The use of interception powers by the MIVD

Published on: 23 March 2016 (not available in English)

Compared to the AIVD, the MIVD makes only limited use of the power to intercept communications. Nevertheless, the CTIVD considers it important to also review the use of such powers by the MIVD.

The general conclusion resulting from the investigation of the operations conducted in the period from June 2013 through June 2015 is that the MIVD makes lawful and careful use of the interception powers in the majority of cases. Unlawful conduct was identified in one operation, the application for the use of the interception powers having been registered in the names of the wrong persons. Inadequate substantiation of grounds for the use of the interception powers resulted in the MIVD being found to have been lacking due care in a number of operations. The Minister of Defence undertook to improve such inadequate substantiation.

In this report, the Committee pays special attention to the use of this power with respect to persons entitled to professional privilege, such as doctors, clergymen, lawyers and journalists (as concerns the protection of their sources). The Committee did not identify any unlawful conduct or lack of due care with respect to the direct application of these powers. In a very limited number of cases, conversations with persons entitled to professional privilege have been intercepted indirectly, for instance by way of the client of a lawyer. The MIVD did not write out these conversations or use them for intelligence purposes.

No. 48 | The implementation of cooperation criteria by the AIVD and the MIVD

Published on: 30 June 2016 (available in English)

In April 2014, the House of Representatives held a debate on the interception activities of the NSA and the part played by the Netherlands in this connection. The motion (no. 89) by MPs Schouw (D66) and Segers (CU) was adopted during this debate. By this motion, the House requested that the government provide more information on the assessments made by the AIVD and MIVD in their cooperation with foreign services. The House requested that the CTIVD review the execution of the motion.

The CTIVD therefore in this report investigated the implementation of the criteria for the cooperation with foreign services by the AIVD and the MIVD. These criteria for cooperation must be met when, for instance, deciding to exchange data with those services.

It is, in the first place, up to the AIVD and MIVD themselves to determine whether to cooperate with a foreign intelligence and/or security service and, if cooperation does take place, to decide on the nature and intensity thereof. The considerations of the services on the basis of an assessment against the cooperation criteria are recorded in a so-called "weighting note". The weighting note must provide insight into the limits of the trust that can be placed in the foreign service, such by way of a risk analysis. The foreign services' respect for human rights and democratic anchorage are included in this assessment. In specific cooperation cases, for instance when exchanging data files, two questions must be answered in the affirmative for the exchange to be permitted:

(1) Does the exchange of data fit within the limits of cooperation, as defined in the weighting note?

(2) Does the actual exchange of data meet the requirements of necessity, proportionality and subsidiarity?

The weighting note thus forms an important safeguard for the protection of fundamental rights and freedoms.

The primary conclusion of the CTIVD's investigation is that the services still have a lot of work to do to produce weighting notes of a sufficiently high quality. The Committee therefore considers the report to only reflect the progress to date and announced that it will perform another investigation into the progress made in 2017. The Ministers concerned have, in their response to the report, confirmed the obligation of the services to make strenuous efforts to improve the state of affairs in this connection. However, at the same time, the proposed new Intelligence and Security Services Act Bill includes a transitional provision delaying the coming into force of the system of safeguards for the cooperation with foreign services, including the drafting of weighting notes, for two years from the date the Bill passes into law. The CTIVD expressed its astonishment with this provision in its view on the Bill. The transitional provision has, however, been retained thus far. The Committee has therefore decided not to perform a follow-up investigation into the weighting notes and their quality for the time being.

No. 49 | The exchange of unevaluated data with foreign services by the AIVD and the MIVD

Published on: 30 June 2016 (not available in English)

During the aforementioned April 2014 debate by the House of Representatives on the interception activities of the NSA, the House also adopted motion no. 96 by MP Schouw (D66). By this motion, the House demanded that the government instruct the AIVD and the MIVD to only exchange (meta) data with foreign services after having received authorisation thereto from the Minister concerned. The Ministers of the Interior and Defence in their response to the motion undertook to ensure that the exchange of (meta) data with foreign intelligence and security services would, in the future, require their prior authorisation. The House requested that the CTIVD review the execution of the motion.

The CTIVD categorises the concept of (meta) data, as used in the motion, as unevaluated data, i.e., data that has not, or not yet, been evaluated on its relevance to the performance of the AIVD's or the MIVD's tasks. This often refers to a larger volume of data (also known as "bulk"). The promised ministerial authorisation system intends to provide stricter data protection. When granting authorisation, the Minister must take account of (1) the level of justified trust in the foreign service and (2) the assessment of the specific exchange of data. The level of trust must be assessed, for each service, on the basis of the cooperation criteria. The Minister evaluates whether the assessment defined in the "weighting note" is correct.

The CTIVD's investigation has shown that neither the AIVD nor the MIVD has established a written policy concerning what must be understood by the term "unevaluated data" and under what circumstances, how and when authorisation must be obtained from the Minister. The Committee in its report recommends that written policy is drawn up, that each instance of data provision is recorded and that the ministerial authorisation for the provision of data to a foreign service is granted for a specific period, for instance one year. In their response to the report, the Ministers stated that they will no longer grant authorisation for an indeterminate period, but will instead only issue authorisations for a period of no more than one year.

No. 50 | Contributions of the MIVD to targeting

Published on: 26 September 2016 (available in English)

The potential use of Dutch intelligence for the unlawful use of force by other states has been discussed regularly in the Dutch Parliament in recent years. The debates revealed the existence of questions about the role and activities of the MIVD in this connection. This led the CTIVD to investigate the possible contributions of the MIVD to targeting and the lawfulness of such actions.

Targeting relates to the process that can result in the (lethal) use of force by armed forces in order to achieve a strategic objective within the context of a (military) operation. The MIVD itself is not authorised to use force. The report focuses on the MIVD's provision of data that may contribute to the decision on the use of force during a (military) operation. The Committee considers such provision of data to be unlawful if it involves an unacceptable risk of contributing to the unlawful use of force. It has become apparent from the investigation that the legal framework applied by the MIVD in this connection takes insufficient account of this risk. The Committee therefore recommends that the legal framework is further elaborated to reduce the risk of the unlawful use of force, such in addition to the advice rendered in reports 48 and 49, and provides specific suggestions for this. Finally, the MIVD must remain alert to indications that data provided has nevertheless contributed to targeting processes involving the unlawful use of force and actively enquire into the matter (*feedback loop*). If such is the case, the results thereof must be included in the reconsideration of the "weighting note" pertaining to the cooperation with the foreign service concerned.

On the basis of the investigated files and the interviews with the service's employees, the Committee found that no concrete indications exist that the MIVD has taken an unacceptable risk of a contribution to the unlawful use of force when providing data. The Minister of Defence stated that the existing legal framework will be updated in accordance with the recommendations of the CTIVD and will be implemented in the first half of 2017.

3

"The CTIVD conducted a wide range of investigations in 2016."

What investigations were ongoing in 2016 and what is planned for 2017?

Ongoing, not yet concluded investigations in 2016

The CTIVD conducted a wide range of investigations into the lawfulness of the activities of the AIVD and the MIVD in 2016. The Review Reports of these investigations are scheduled to be published in 2017. The CTIVD once again conducted an investigation into the use of investigatory powers by the AIVD and the MIVD against lawyers and journalists, for instance. It also investigated the use of hacking powers by both services. The investigation into the exchange of data on (alleged) jihadists by the AIVD in 2016 primarily focused on the international exchange of data. In addition, the Committee reviewed both services' performance of the obligation to notify and the response to applications for access to data submitted by citizens within the context of an investigation into the transparency of personal data processing. By conducting these investigations, the CTIVD strives to provide equal attention to the AIVD and the MIVD, and to the various activities deployed by these services. The ongoing investigations are set out in brief below.

Transparency of personal data (AIVD & MIVD)

It is necessary for the task performance of the AIVD and the MIVD to collect and process personal data. The services make use of, *inter alia*, their investigatory powers to effect this. However, can a person whose data has been collected ever find out that their data has been used by the AIVD or the MIVD? A number of options to obtain such information is available under the ISS Act 2002. The CTIVD investigated how both services allow for these options under the theme of "transparency of personal data processing". On 3 March 2016, it announced its intent to investigate the topics of notification and access to personal data at the AIVD and the MIVD. Both provisions serve to allow the individual citizen concerned to obtain insight into the generally classified activities of the AIVD and the MIVD, wherever possible, so as to be able, or better able, to exercise their fundamental rights.

The first part of the investigation relates to the performance of the obligation to notify as provided in Article 34 of the ISS Act 2002. This obligation to notify requires the AIVD and the MIVD to investigate, five years after the use of a certain (investigatory) power against specific persons was ceased, whether the persons concerned may be informed thereof. The law also provides for a number of grounds for exception to this obligation to notify, for instance if someone cannot be traced or because such is impossible in connection with protecting sources or methods. The CTIVD concluded its investigation in late 2016 and published its Review Report No. 51 in February 2017.

The second part of the investigation relates to the processing of applications for access to personal data within the meaning of Articles 47 and 50 of the ISS Act 2002. The CTIVD started this investigation in late 2016 and will conclude it with a Review Report, to be published in the summer of 2017.

Investigation into the use of investigatory powers against lawyers and journalists by the AIVD and the MIVD

The right to confidential communications with parties entitled to professional privilege, like lawyers and journalists, is an important right. For any person must, in principle, be able to freely approach such parties. The right to professional privilege as granted to journalists primarily relates to protection of their journalistic sources. In previous investigations, complaints and Annual Reports, the CTIVD devoted attention to the way the AIVD and the MIVD observe this right when using investigatory powers. In 2015, the court, too, issued judgments on this subject. This led to the establishment by the cabinet – by way of a temporary arrangement – of an independent assessment committee that issues a binding opinion on the intended use of investigatory powers against lawyers and journalists. This arrangement is intended to be temporary and to apply only until the new Intelligence and Security Service Acts enters into force. In view of these developments, the CTIVD announced on 4 May 2016 that it would investigate the – direct and indirect – use of investigatory powers against lawyers and the use of investigatory powers against journalists if this use relates to tracing journalistic sources. The investigation, which covers the period from October 2015 through March 2016, was found to be more complex than expected and was only concluded in early 2017. Review Report No. 52 was published in March 2017.

Investigation into the use of hacking powers by the AIVD and MIVD

The AIVD and the MIVD have the power to gain access to computerised devices or systems, such as computers. This is also referred to as the hacking power. In a world where personal digital information is increasingly available and can be hacked into by various methods, the CTIVD believes it important to review whether the services strike the right balance between national security and safeguarding private life. On 17 March 2016, the CTIVD announced that it would institute an investigation in this connection. Its investigation related to both physical hacking (such as of a laptop seized by the services) and remote hacking (for instance, via the Internet). The investigation was concluded in late 2016. The Review Report is set to be published in April 2017.

Exchange of data on (alleged) jihadists (AIVD)

The investigation into the exchange of data on (alleged) jihadists by the AIVD is divided into a national and an international component. In March 2016, the CTIVD started with the international part of the investigation. It soon found that the exchange takes place in a dynamic arena, where developments occur in rapid succession, especially in multilateral settings. For this reason, the CTIVD decided to focus first on the multilateral cooperative partnerships in which the AIVD takes part. The investigation charts which exchanges of data on (alleged) jihadists take place within which cooperative partnerships, as well as the legal basis for such exchange. 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 of necessity, propriety and due care, amongst others. The CTIVD also assesses how these safeguards are implemented in practice. This part of the investigation will be concluded in the spring of 2017, while the Review Report is set to be published in the second half of 2017.

The second phase of the investigation concerns the exchange of data within the national context. This concerns, *inter alia*, official messages submitted by the AIVD to, for instance, the Public Prosecution Service, the Immigration and Naturalisation Service (IND) and mayors. This second phase started in December 2016 in practice, when an initial exploration was started up. The CTIVD expects to conclude this part of the investigation in late 2017 with the publication of a Review Report.

Annual planning 2017

In 2017, the CTIVD will conclude the aforementioned ongoing investigations with the publication of Review Reports.

With a view to the scope of the ongoing activities and the forthcoming legislative amendment and related parliamentary debate, the CTIVD has decided to only sparingly launch new investigations.

The new Act will require an update of the working processes and IT systems of both services. Though the services are working on implementing this update, this requires time. While the CTIVD keeps a finger on the pulse, it believes it to be too early to already issue an opinion on the observance of the new legal provisions. Moreover, the new Act will have far-reaching consequences for the performance of the oversight task. The Committee deems it of importance at this stage that its oversight will be adjusted to the new developments. To be able to do so, it will, in 2017, focus on consulting with both services on the technical and legal consequences of the new Act. It will, in particular, address the implementation of the interception, data processing and data destruction procedures prescribed by the new Act.

4

"The CTIVD is sometimes considered to be the 'eyes and ears' of Parliament."

How effective is the oversight?

External purpose of oversight: informing Parliament and the public

The classified nature of the activities of the AIVD and the MIVD hampers political control over and social debate on these services. The establishment of the CTIVD allowed for a form of indirect transparency: the CTIVD's Review Reports grant the outside world insight into the lawfulness of the operations of the AIVD and the MIVD. The CTIVD is independent in selecting the subjects of its investigations and in conducting them. In its reports, it explains the legal framework and describes the practical state of affairs as identified by it. It draws conclusions and makes recommendations so as to ensure a proper balance between national security and the protection of private life. In his response to a Review Report, the Minister concerned states the extent to which he will respond to the unlawful conduct identified and recommendations issued. The Review Report is next offered to both Houses of Parliament, together with the Minister's response. Parliament may use it to enter into a debate with the responsible Minister. By publishing its reports, the CTIVD contributes to a more informed parliamentary debate and, in this way, benefits democratic accountability. For this reason, it is sometimes considered to be the "eyes and ears" of Parliament. As all Review Reports are published on the CTIVD's website, the public, too, may obtain insight into the way both services perform their tasks and into the extent they observe the law while doing so.

Internal purpose of oversight: informing the party subjected to oversight

Oversight does not serve an external purpose only. It also contributes to the AIVD and the MIVD obtaining more insight into how to apply the law and, in this way, to increasingly lawful conduct by these services. The CTIVD clarifies the interpretation of applicable legislation. The proper transition of legislation into practice is of importance in this connection: Is practice in line with the law and, if not, how can this be rectified? In this connection the Committee focuses on both the work floor and the services' management, for it is at that level that the tension between protecting national security and protecting fundamental rights is at its most tangible and concrete. It is up to the services' management to adjust their policies and procedures wherever necessary, in order to have a professional (operational) practice which stays within the limits of the legal framework.

Effectiveness in 2016

The CTIVD regularly assesses whether it sufficiently meets these objectives and, in other words, if it carries out effective oversight. There were a number of noteworthy developments in 2016.

1. Sounding board contributes to the quality of investigations and reports

In 2014, the CTIVD established a Knowledge Network comprised of external experts. This Knowledge Network plays two roles. First, it explores the current and future themes prevalent in the academic world and society together with the CTIVD and comments on the development of the Committee (such as with respect to setting up an IT expert unit). Second, the Knowledge Network serves as a sounding board. It presents the CTIVD with a critical and different (academic) view in specific investigations. Both roles played by the Knowledge Network and its members are considered to be highly valuable, for they contribute to increasing the relevance and quality of the products submitted by the CTIVD, rendering them both more profound and practical. In this way, they contribute to the effectiveness of the oversight.

2. Ministers generally adopt recommendations

In 2016, the Ministers concerned concurred with the conclusions drawn by the CTIVD in its reports in the large majority of cases. They generally undertook to adopt the recommendations. Whenever a Minister did not do so, he substantiated his position, providing Parliament with an overview of the grounds for opting not to do so.

The CTIVD finds that the AIVD and the MIVD sometimes start adjusting their policies and procedures while an investigation is still ongoing. In 2016, this occurred in the context of Report 50 on the contributions of the MIVD to targeting and of Report 51 on the performance of the obligation to notify, for instance.

The CTIVD considers both developments to be positive contributions to the effectiveness of its oversight.

3. The House of Representatives considers the CTIVD's Reports in its parliamentary controls

Whenever the CTIVD publishes a report, the Parliamentary Standing Committee concerned (the Committee on the Interior or the Committee on Defence, or the Committee on the Intelligence and Security Services, respectively) usually requests that it provide a verbal explanation on the Report by way of a technical briefing. This briefing is sometimes held behind closed doors. This allows the CTIVD to directly respond to the questions raised within Parliament by the Report. The technical briefings also provide it with a clear picture of the issues prevalent in Parliament.

The substance of the parliamentary debate between the House and the Ministers concerned held in the context of the publication of a Report was different for each Report in 2016. Some Reports led to extensive rounds of questions and answers (Report 50), while the debate was relatively limited in other cases (Reports 48 and 49).

The CTIVD concludes, on the basis of the responses by the members of Parliament, that the contents of the Review Reports together with the verbal explanation meet the expectations of Parliament.

4. The importance of conducting a dialogue with the work floor staff

During its investigations, the CTIVD holds extensive dialogue with the work floor staff of the service concerned, both to obtain a view of the specific occurrences and procedures and to get a sense of the interests and challenges at play. The CTIVD believes it to be important to have an eye for operational realities and be aware of what is going on within the AIVD and the MIVD when conducting its investigations. In this way it strives to find a proper balance between its juridical observations on the one hand and the practicability of its recommendations on the other.

In the past little feedback was received once a Report was published, while it is important, from the perspective of the internal effectiveness of the oversight, to be aware of what the actual response of the organisation is to the Report. The CTIVD therefore started so-called “work floor meetings” in late 2016. Two months after a Review Report is published, the CTIVD meets with the relevant staff of the services. The staff concerned is asked how the Review Report was received and whether the recommendations made are clear and practicable. One meeting held in 2016 resulted in the CTIVD being informed that the framework it proposed was useful and easily applicable in operational practice, for instance, while it became apparent during a meeting on another Report that the specific interpretation of a certain recommendation was still unclear. In cases like the latter, the Committee will provide a further explanation. The CTIVD believes this dialogue with the work floor to be a positive development in improving the effectiveness of its oversight.

5. Implementation of the recommendations

Whenever the CTIVD concludes an investigation, it is up to the management of the services concerned and the Minister to implement the recommendations they adopt.

Should there be cause to do so, the CTIVD will conduct a follow-up investigation. Such cause may be provided by the importance of the theme in question or of the recommendations, for instance. In this connection, the CTIVD investigated the performance by the AIVD of its obligation to notify for the third time in 2016 (Report No. 51), while it also reviewed the use of interception powers by the AIVD for a second time (Report No. 46).

The Committee as yet does not systematically monitor compliance with all its past recommendations. It is considering doing so more structurally, so as to promote the effectiveness of its oversight task.

5

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

What complaints were handled by the CTIVD in 2016?

If somebody has a complaint about the conduct of the AIVD or MIVD, it can, pursuant to the ISS Act 2002 and in accordance with the General Administrative Law Act (Awb), be submitted to the Minister of the Interior and Kingdom Relations or the Minister of Defence. The Minister decides about the admissibility of the complaint. If the Minister decides to handle the substance of the complaint, he will, in coordination with the complainant, draw up the formal wording of complaint. He will then engage the CTIVD as an independent advisory complaints commission to assess the substance of the complaint. The CTIVD will hear the complainants and examine the relevant files and/or will hear staff from the service concerned. The CTIVD will assess whether the relevant activities of the AIVD or MIVD were proper, testing them against the standards for proper conduct by government services also used by the National Ombudsman. It will next, on the basis of its investigation, advise the Minister about 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 complaints handled by the CTIVD in 2016 are listed in the below. This is followed by a description of the various complaints, grouped by theme.

Number of complaints handled

In the year 2016, the CTIVD handled thirteen complaints: eleven concerned the AIVD and two concerned the MIVD. It issued advisory opinions to the Minister concerned. The Minister concerned adopted the CTIVD's advisory opinions for all complaints.

In addition, at the end of the reporting year, the CTIVD was still processing one complaint about the AIVD and one complaint about the AIVD and MIVD jointly. It finds that the number of complaints has remained roughly the same over the past few years. The complaints have, however, become more legally complex.

Number of complaints about the AIVD	Number of complaints about the MIVD	Advisory opinions
1	1	Manifestly unfounded
7	-	Unfounded
3	1	Partly unfounded, partly well-founded
-	-	Well-founded

Description of the complaints handled

A short description of the complaints handled by the CTIVD this reporting year is provided in the below. The description is anonymised, as the CTIVD is not free

to publicise individual complaints due to privacy considerations with respect to complainants. The decision to freely publish the complaint can be made by the complainant or the Minister in consultation with the complainant. The description of the complaints is based on the information released to the complainants by the Ministers concerned.[1]

Use of investigatory powers

Pursuant to the ISS Act 2002, the AIVD and the MIVD may use investigatory powers in the performance of their tasks. Such powers include surveillance, monitoring, intercepting telephone communications and hacking computers. Legal safeguards are in place with respect to the use of these powers. Complaints about the use of investigatory powers can be handled by the CTIVD. Upon receipt of a complaint, the Committee will investigate whether investigatory powers have been used against the complainant and whether such use was lawful. It will communicate the results of its investigation in an advisory opinion submitted to the Minister. As a rule, the use of investigatory powers against a complainant will neither be confirmed nor denied in the complaints procedure. Occasionally, the Minister will inform the complainant whether he has been subjected to an investigation by the service when settling the complaint.

In 2016, the CTIVD handled six complaints against the AIVD concerning the lawfulness of the use of investigatory powers.

For two of these complaints, the complainants stated that investigatory powers were used against them without there having been a legal basis to do so. This concerned the interception of telephone or internet communications and/or the monitoring and surveillance of the complainants. The CTIVD found that both complainants had been subjected to investigation by the service.
In its investigation into one of the two complaints, the CTIVD did not identify unlawful conduct, but it did find that there had been a lack of due care. However, this lack was not so serious as to comprise improper conduct towards the complainant. It advised that the complaint be dismissed as unfounded.
With respect to the other complaint, the CTIVD found that part of the operational investigation had been incorrectly performed. Insufficiently significant reasons for performing this part of the investigation existed, meaning that the requirement of proportionality had not been met. The CTIVD found that the AIVD had, in this respect, acted improperly towards the complainant. In addition, it identified a lack of due care of such a nature that it did not constitute improper conduct. The CTIVD advised that the complaint be declared well-founded in part and unfounded for the remainder.[2]

The third complaint put forward that the AIVD, or at any rate police officers performing work on behalf of the AIVD, had acted unlawfully with respect to the complainant.[3] These actions at any rate consisted of the monitoring and surveillance of the complainant. In its investigation, the CTIVD did not find any evidence that the AIVD, or

---

1 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.

2 This complaint is included in the "unfounded" section in the above table.

3 Article 60 of the ISS Act 2002 provides that police officers may perform work on behalf of the AIVD. This work is performed under the responsibility of the Minister of the Interior. Complaints may be lodged with the Minister of the Interior with respect to such work, to the extent it is performed in accordance with the provisions of Article 60 of the ISS Act 2002.

at any rate police officers performing work on behalf of the AIVD, had acted improperly towards the complainant. It advised that the complaint be dismissed as unfounded.

In addition, the CTIVD advised that the complaint be forwarded to the chiefs of the relevant police units to the extent it related to police actions other than work performed on behalf of the AIVD.

The fourth complaint concerned the interception of the communications of the complainant in his house and improper treatment of the complainant. On the basis of its investigation, the CTIVD found no evidence that the AIVD had acted improperly towards the complainant. It advised that the complaint be dismissed as unfounded.

In the fifth complaint, the complainant put forward, *inter alia*, that the AIVD had opened and read or intercepted the mail, correspondence, telephone conversations and e-mails between him and his lawyer. On the basis of its investigation, the CTIVD found no evidence that the AIVD had acted improperly towards the complainant. It advised that the complaint be dismissed as unfounded in this respect. The other components of the complaint concerned actions that could not, within reason, be attributed to the service, such as influencing the supply of hot water to the complainant's house and using devices to monitor when the complainant was sleeping or taking a shower. The CTIVD found these components to be manifestly unfounded.

The sixth complaint was a complaint lodged by two lawyers. They put forward that the AIVD had indirectly intercepted or recorded telephone conversations or electronic communications between them and one of their clients and/or had subsequently written out communications covered by professional privilege. The CTIVD applies the following definition of indirect interception: intercepting a client's communication with their lawyer via a tap.[4] On the basis of its investigation, the CTIVD found no evidence that the service had acted improperly towards the complainants. It advised that the complaint be dismissed as unfounded.

Collecting information

In one complaint, the complainant put forward that the AIVD had collected information about them using unlawful methods. The CTIVD established that the AIVD had conducted an investigation in the context of the performance of its legal tasks. The CTIVD found that the investigation should not have been carried out during a certain period of the time concerned, ruling that this part of the investigation was improper. It advised that the complaint be declared well-founded in this respect and unfounded for the remainder.

Provision of information on persons

Essentially, the investigations conducted by the AIVD and MIVD serve the purpose of providing information to external organisations in the interest of national security. This primarily concerns Dutch bodies which are authorised to take measures on the basis of the information provided, such as the responsible (local) administrators or the office

[4] Refer to the CTIVD's 2015 Annual Report, Section 4.4.

of the Public Prosecutor. The ISS Act 2002 sets forth requirements for the provision of information, particularly with respect to personal data. The provision of information about individuals to external organisations as a rule takes place by official message.

In 2016 the CTIVD handled two complaints about the AIVD's issue of official messages to national bodies.

The first complaint related to an official message the AIVD had issued to the Child Care and Protection Board (hereinafter: the "Board"). The complaint concerned both the issue of the official message and the phrasing of its contents. The CTIVD found that, pursuant to Article 36 of the ISS Act 2002, the AIVD is entitled to issue official messages to the Board and that the provision of information had in this case been necessary in the interest of national security. The CTIVD also found that the service, when issuing its official message, had weighed the interests at stake, attaching sufficient importance to the possible consequences of the official message to the parties concerned, and that the service had acted with sufficient care when weighing these interests. The CTIVD established that there was no evidence that the service had wilfully tried to circumvent the legal safeguards by issuing the official message. As concerns the contents of the official message, the CTIVD established that they were supported by the underlying information and that this information was rightfully considered to be reliable by the AIVD. The CTIVD found that the provision of information had not imputably been suggestive or selective. Finally, the CTIVD established that while the official message indeed infringed on the complainant's family life, there was sufficient justification to do so. It advised that all components of the complaint be dismissed as unfounded.

The second complaint related to an official message the AIVD had issued to municipal authorities. The complaint disputed, *inter alia*, the issue of the official message. The CTIVD found that Article 36 of the ISS Act 2002 provided a legal basis for the issue of the official message to the municipal authorities, that the official message was supported by the underlying information and that the requirements of proportionality and necessity had been met. The complaint also concerned the fact that the AIVD had provided information to the municipal authorities verbally, in addition to the official message. The CTIVD established that the AIVD had, indeed, verbally provided information to those municipal authorities. In the view of the CTIVD, this was not improper, as the verbally provided information did not contain any new facts, did not provide a different interpretation of the contents of the official message and had not been of decisive importance to the municipal authorities in their decision to take action. The complainant also brought forward that the AIVD had a duty to ensure that the information would not be shared with third parties or to only provide the information on the condition that it not be issued to third parties. The CTIVD established that the AIVD had not issued the official message under the condition as referred to by the complainant. However, in the opinion of the CTIVD, this was not required, as official messages are issued for the purpose of using the information contained therein. For each of the components of the complaint, the CTIVD found that they were unfounded. The complaint also related to the AIVD's use of investigatory powers against the complainant without prior judicial review. The CTIVD established that it was not competent to address this issue, as it did not concern a specific action taken by the AIVD but a general question of whether the ISS Act 2002 accords to the provisions of the ECRM. The CTIVD advised the Minister to declare the complaint to be inadmissible as regards this component.[5]

[5] This complaint is included in the "unfounded" section in the above table.

Security screenings

Both within the government and the business sector, so-called positions involving confidentiality have been created. A position involving confidentiality is a position allowing for the misuse of knowledge or power to damage national security, e.g., by leaking state secrets or providing access to possible targets for an attack. In order to fulfil a position involving confidentiality, a VGB (security clearance) must be issued. Prior to the issuance of a VGB, the AIVD or the MIVD conduct a security screening of the person concerned. If the VGB is refused, the person concerned can appeal against the decision via the Minister, and then appeal to a court of law.

In 2016, the CTIVD handled one complaint about the MIVD, which related to the security screening procedure, and one complaint about the AIVD, which related to the conduct of the service in the context of an appeal procedure.

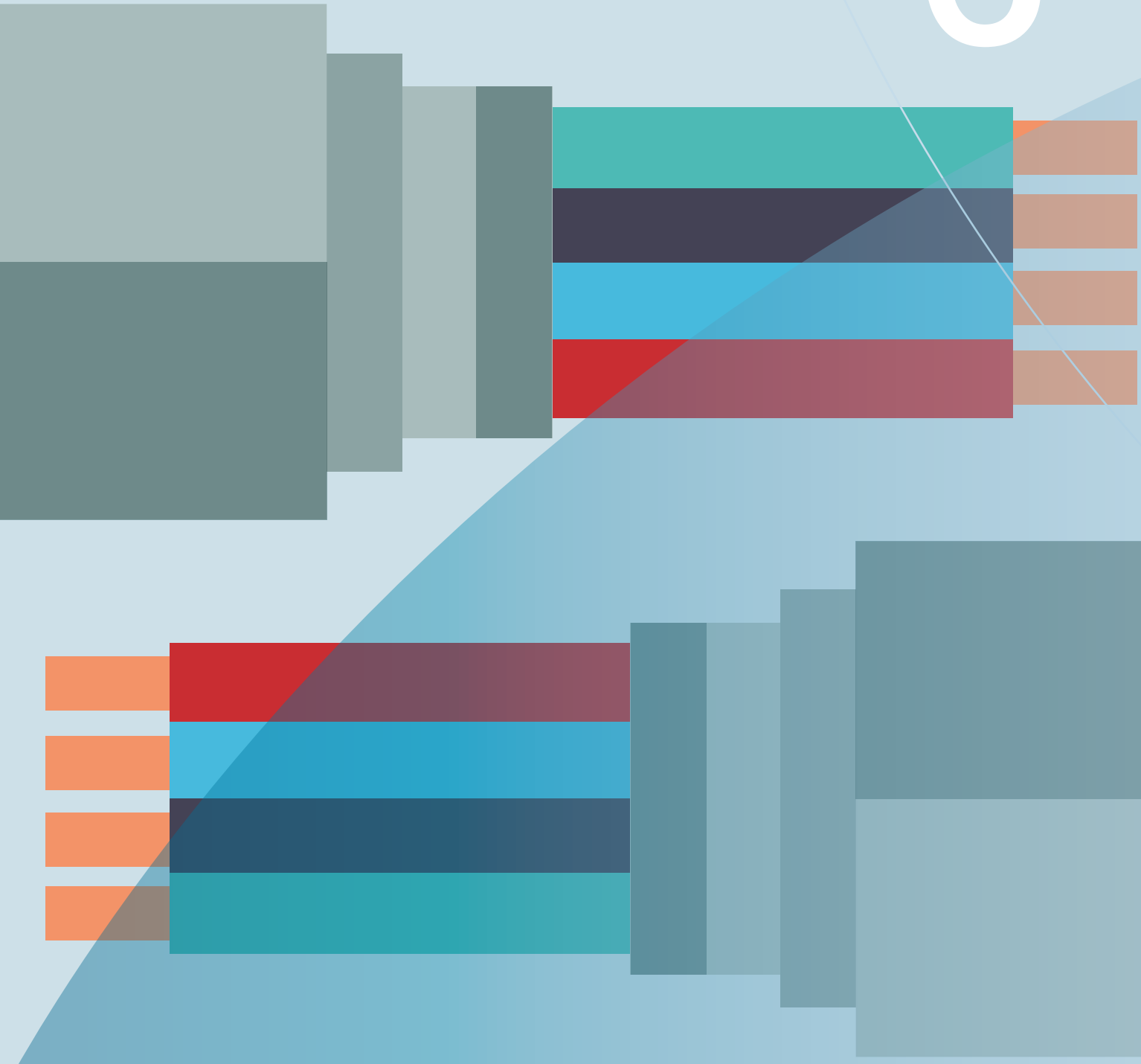
The complaint about the MIVD concerned, first, the way the security screening had been conducted and, second, the failure to issue a decision on two VGBs. The Committee found that the MIVD, when conducting the security screening, should have performed a more extensive investigation into the actual actions taken by the complainant. By failing to do so, the MIVD had acted improperly against the complainant. The Committee found that the Ministry had not acted improperly towards the complainant by not taking a decision with respect to the two VGBs involved, as the complainant had by that time made use of an arrangement to cease his employment. The CTIVD advised that the first component of the complaint be declared well-founded and the second component be dismissed as unfounded.

The complaint about the AIVD concerned a situation where the AIVD had labelled two VGBs previously issued to the complainant as being official errors and revoked the third VGB. The complainant put forward that the AIVD had, in the subsequent appeal procedures via the Minister and before the court of law, wilfully provided different reasons for its qualifications and decisions than the real ones, thereby concealing those real reasons. The CTIVD found that the AIVD should not have qualified one of the VGBs as having been issued erroneously before the bodies that handled the appeal, as the VGB had been granted in accordance with the AIVD's policy at the time of issue. The Committee considered the AIVD's actions as constituting unprofessional conduct. As concerns the other VGBs, the CTIVD found that the AIVD had not acted improperly towards the complainant. It advised that the complaint be partly declared well-founded, and partly be dismissed as unfounded.

Manifestly unfounded

Regarding one complaint about the MIVD and one about the AIVD, the CTIVD advised the Ministers concerned to dismiss it as manifestly unfounded in its entirety. It comes to this opinion when it becomes immediately evident from the written complaint that there can be no reasonable doubt about the complaint being unfounded.

6

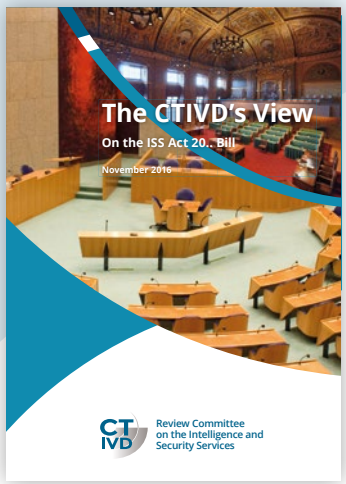


"The CTIVD believed it important to respond to the Bill in its capacity as independent oversight body, such in view of its knowledge of the procedures of the services and its experience with the practical application of the current ISS Act."

What are the developments in relation to the new ISS Act?

A significant number of responses to the draft Bill for the new Intelligence and Security Services Act were submitted during the summer 2015 internet consultation round. In the months thereafter, the cabinet worked on drawing up an amended Bill, which was submitted to the Council of State for advice in April 2016. So as to strengthen its guarantee function, the amended Bill introduced a new assessment committee charged with providing a binding assessment on the use of investigatory powers prior to their actual use. The use of untargeted powers of interception of cable-bound and non cable-bound communications (new) was given the new name of "investigation task-related investigation of communications". While the Council of State in its September 2016 critical advisory opinion stated to be in favour of the expansion of the powers of the services, it argued against the establishment of a new assessment committee. The cabinet retained the assessment committee in the Bill, however, and only amended a limited number of its provisions. The cabinet submitted the Bill to the House of Representatives in late October 2016.

The CTIVD, too, responded to the draft Bill in September 2015. The Ministers concerned had asked the CTIVD to do so. The CTIVD believed it important to give a response in its capacity as independent oversight body, such in view of its knowledge of the procedures of the services and its experience with the practical application of the current ISS Act. In November 2016, when the House of Representatives was debating the Bill, it believed the time to be ripe for submitting a new response. The Committee had, in the meantime, closely monitored the developments. In this connection, it had frequently been in contact with other public bodies involved, as well as with civil-society organisations. Its understanding of the new powers detailed in the Bill had increased by that time, also in view of the increased knowledge it possessed about, *inter alia*, the application of information technology within the services (refer to Chapter 8).



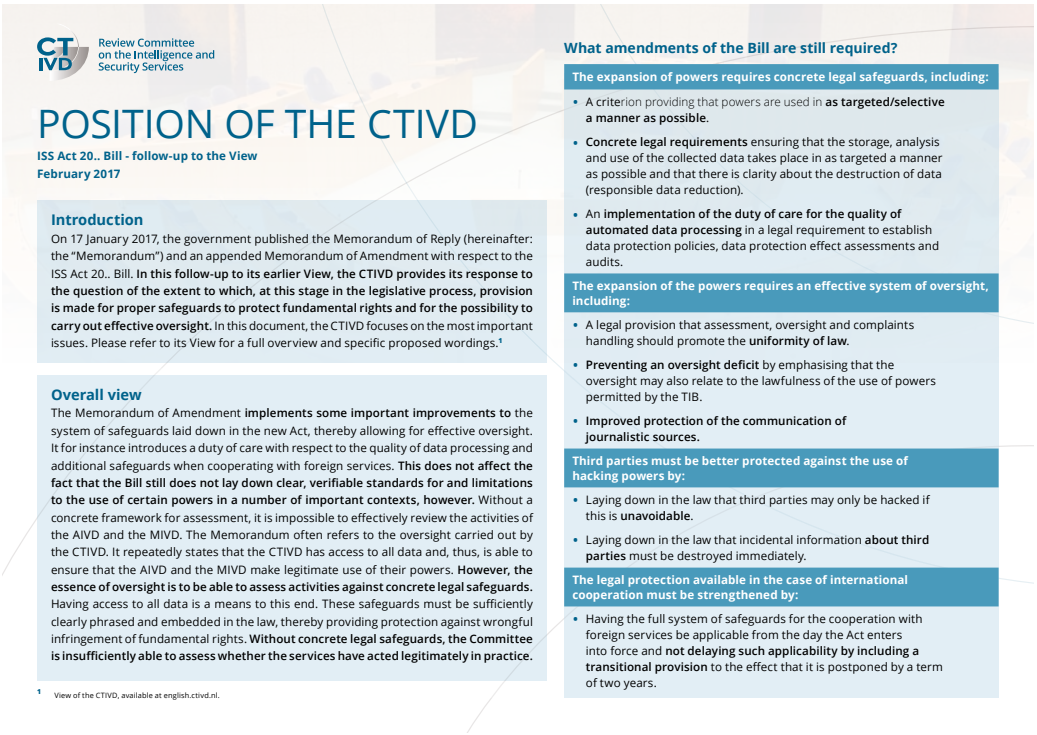
In its View (November 2016, available in English), the CTIVD stated that its picture of the operational practice confirmed the necessity of expanding and modernising the powers of the AIVD and the MIVD. However, though the Bill provides powers befitting the 21st century, it retains 20th-century safeguards. The Committee finds that the Bill lacks a proper balance between protecting national security and providing essential legal safeguards for the protection of fundamental rights.

Why did the CTIVD believe the ISS Act 20.. Bill as debated in the House of Representatives to be unbalanced in late 2016?

- The Bill emphasises the classic safeguards of authorisation and assessment prior to the use of powers, while the technological developments primarily require a strengthening of the safeguards in the data processing process where the infringement actually takes place.
- A clear legal framework is required so as to carry out effective oversight on this data processing process in the future – e.g., with respect to the automated analysis, selection and destruction of collected data. In this connection, the CTIVD emphasised the importance of as targeted a use of powers as possible and an obligation to continuously and responsibly limit the amount of data used during processing.
- The Bill creates a complex and layered system of independent prior assessment by the new investigatory powers assessment committee ("TIB") and subsequent oversight and complaints handling by the CTIVD. So as to limit the risk of differences in interpretation with respect to the application of the new Act, the CTIVD argued that a provision promoting uniformity of law and, thus, legal certainty be included.
- In addition, the Bill excludes the option of an a posteriori review of the use of powers if the TIB has granted its prior permission. The CTIVD warned that this in practice could result in an oversight deficit.
- The Bill also grants the services too much leeway to use hacking powers against third parties. The CTIVD argued in favour of increased protection of these third parties.
- The application of the system of safeguards when cooperating with foreign services will be delayed by two years from the entry into force of the Act. The CTIVD pointed out that this system is of major importance for the provision of legal protection. Moreover, the safeguards concerned by and large already exist in the current Act. It found there was no justification for this transitional provision and argued for the immediate implementation of these safeguards.

The CTIVD was able to provide an extensive explanation of its View during a technical briefing before the House of Representatives.

The parliamentary parties to the House posed a significant number of questions in the Report, leading to the cabinet submitting a Memorandum of Reply and a Memorandum of Amendment further clarifying and amending the Bill in January 2017. A duty of care for the quality of data processing, as was advocated by the CTIVD, was inserted into the Bill, while the safeguards in place when cooperating with foreign services were strengthened. For the benefit of the parliamentary hearing of the Bill in the House of Representatives, The CTIVD updated its View by issuing a Detailed Position in February 2017.



Review Committee on the Intelligence and Security Services

POSITION OF THE CTIVD

ISS Act 20.. Bill - follow-up to the View
February 2017

Introduction

On 17 January 2017, the government published the Memorandum of Reply (hereinafter: the "Memorandum") and an appended Memorandum of Amendment with respect to the ISS Act 20.. Bill. **In this follow-up to its earlier View, the CTIVD provides its response to the question of the extent to which, at this stage in the legislative process, provision is made for proper safeguards to protect fundamental rights and for the possibility to carry out effective oversight.** In this document, the CTIVD focuses on the most important issues. Please refer to its View for a full overview and specific proposed wordings.[1]

Overall view

The Memorandum of Amendment **implements some important improvements to** the system of safeguards laid down in the new Act, thereby allowing for effective oversight. It for instance introduces a duty of care with respect to the quality of data processing and additional safeguards when cooperating with foreign services. **This does not affect the fact that the Bill still does not lay down clear, verifiable standards for and limitations to the use of certain powers in a number of important contexts, however.** Without a concrete framework for assessment, it is impossible to effectively review the activities of the AIVD and the MIVD. The Memorandum often refers to the oversight carried out by the CTIVD. It repeatedly states that the CTIVD has access to all data and, thus, is able to ensure that the AIVD and the MIVD make legitimate use of their powers. **However, the essence of oversight is to be able to assess activities against concrete legal safeguards.** Having access to all data is a means to this end. These safeguards must be sufficiently clearly phrased and embedded in the law, thereby providing protection against wrongful infringement of fundamental rights. **Without concrete legal safeguards, the Committee is insufficiently able to assess whether the services have acted legitimately in practice.**

[1] View of the CTIVD, available at english.ctivd.nl.

What amendments of the Bill are still required?

The expansion of powers requires concrete legal safeguards, including:

- A criterion providing that powers are used in **as targeted/selective a manner as possible**.
- **Concrete legal requirements** ensuring that the storage, analysis and use of the collected data takes place in as targeted a manner as possible and that there is clarity about the destruction of data (responsible data reduction).
- An **implementation of the duty of care for the quality of automated data processing** in a legal requirement to establish data protection policies, data protection effect assessments and audits.

The expansion of the powers requires an effective system of oversight, including:

- A legal provision that assessment, oversight and complaints handling should promote the **uniformity of law**.
- **Preventing an oversight deficit** by emphasising that the oversight may also relate to the lawfulness of the use of powers permitted by the TIB.
- **Improved protection of the communication of journalistic sources.**

Third parties must be better protected against the use of hacking powers by:

- Laying down in the law that third parties may only be hacked if this is **unavoidable**.
- Laying down in the law that incidental information **about third parties** must be destroyed immediately.

The legal protection available in the case of international cooperation must be strengthened by:

- Having the full system of safeguards for the cooperation with foreign services be applicable from the day the Act enters into force and **not delaying such applicability by including a transitional provision** to the effect that it is postponed by a term of two years.

The views of the CTIVD were discussed extensively during the parliamentary hearing. A number of further adjustments were made to the Bill following the vote on the amendments and motions. On 14 February 2017, the House of Representatives adopted the Bill, which was then submitted to the Senate by the cabinet.

At the time this Annual Report was completed, the Bill was being debated by the Senate. In late March 2017, the CTIVD discussed the importance of the Bill, the legal strengthening of safeguards and the provision of guidelines for effective oversight with the Senate.

In the meantime, the CTIVD is also making preparations for the oversight it will have to carry out once the new Act has been adopted and enters into force. This concerns reviewing the application of the new powers of the services and the way the services implement the duty of care for the quality of the data processing. Also in connection with this, the CTIVD started setting up an IT expert unit in 2016. This unit will take the lead in developing new forms of oversight. It will do so in consultation with the AIVD and the MIVD, all with due observance of the role played by each party and their associated responsibilities.

The CTIVD is also preparing for the changes introduced by the new Act as concerns the complaints handling procedure. Under the Bill, the CTIVD will become an independent and external complaints body. It will rule on the admissibility of the complaint, investigate the merits of the complaint and issue an opinion on the lawfulness and propriety of the actions by the AIVD or the MIVD that will be binding to the Ministers concerned. In addition, the CTIVD will be charged with handling reports from whistleblowers on (alleged) abuses. The CTIVD will be divided into an Oversight Department and a Complaints Handling Department. It will be ready to get to work once the new Act enters into force.

7

“The joint project has granted the CTIVD valuable insights it can use during its own national investigation”

How does the CTIVD cooperate internationally?

From its oversight activities, the CTIVD has become aware that there is a strong increase in international cooperation between intelligence and security services and in the exchange of data taking place within this context. It is therefore important that the oversight bodies, too, consult more with each other in an international context. In its previous two Annual Reports, the CTIVD already highlighted this issue, stating that it would explore possible avenues for cooperation.

In 2016 the CTIVD also made efforts to increase cooperation between oversight bodies. The joint project started up in 2015, involving, in addition to the CTIVD, the Belgian, Danish, Norwegian and Swiss oversight bodies, was developed further in the past year. All of the participating oversight bodies are conducting an investigation into the exchange of data on (alleged) jihadists, each from their own national context and within the framework of its own mandate.

The aim of the project is to compare investigation methods, interpret legal problems and collate non-classified findings. Three meetings – two in The Hague and one in Brussels – took place in this context in 2016. The CTIVD actively participated in all three meetings.

The joint project has, thus far, granted the CTIVD valuable insights it can use during its own national investigation. On the one hand, it finds that there are common (legal) problems the various oversight bodies are running into. Discussing these problems results in a more in-depth understanding, knowledge building and mutual understanding. On the other hand, each oversight body works within its own legal framework and within the own national context. Comparing the various approaches taken and investigation methods employed results in new insights being obtained and in critical reflection on a body's own oversight practice.

The joint project was started up with the aim to take the first, tentative steps to overcome the limits of national oversight, also referred to as the accountability deficit. Moreover, comparing findings and conclusions results in a more complete overview of the international cooperation between intelligence and security services. At the same time, it becomes clearer that the sum total of each country's national oversight has its limitations. The project participants strive to publish a joint public report in 2017.

In 2016, the CTIVD participated in multiple international conferences, including a conference of the *International Association of Intelligence Education* (IAFIE) in Breda and the *International Intelligence Oversight Forum* in Bucharest set up by the UN Special Rapporteur on Privacy. In addition, the CTIVD hosted multiple delegations from France in 2016.

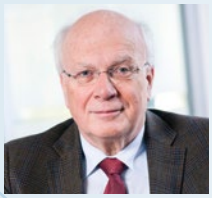
8

"The central theme in the advisory opinion of the ABDTOPConsult team was the importance of increasing IT expertise."

What were the developments in the CTIVD organisation in 2016?

Composition of the CTIVD and staff

At the start of 2016, the Committee was composed of Harm Brouwer (Chairman) and Aad Meijboom (Member). Marylène Koelewijn acceded as a Member in March 2016. Hilde Bos-Ollermann is the Committee's General Secretary. The CTIVD's bureau was composed of seven legal investigators and two (part-time) secretaries at the start of 2016. The investigative staff (both legal and IT, refer to the below) was expanded to comprise nine members in late 2016.



Harm Brouwer
Chairman

Marylène Koelewijn
Member

Aad Meijboom
Member

Hilde Bos-Ollermann
General Secretary

In October 2016, the CTIVD seconded one of its members of staff as an adviser to the House of Representatives Committee for the Intelligence and Security Services for a fixed period. This is a new position created to provide the party chairpersons involved with independent expert support. For the entire period of the secondment, the member of staff concerned will operate fully under the authority and responsibility of the Registry of the House of Representatives.

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 averaged some EUR 1 million per year since its foundation in 2002. In 2014, this was deemed to be insufficient. The cabinet therefore in 2016 increased the budget by EUR 0.5 million. As a result, the CTIVD's 2016 budget sufficed. The cabinet intends to increase the budget further once the new Act has entered into force. This increase of the budget must suffice to allow the CTIVD to properly perform its new and additional tasks arising from the ISS Act 20...

During 2016, the CTIVD's organisation was also engaged with finding suitable accommodation, as the contract for the current offices at Anna van Saksenlaan 50 in The Hague

will expire. However, it became evident in early 2017 that structural and security reasons prevented the move to the intended new accommodation. At the time this Annual Report was completed, the search for definitive new accommodation was still ongoing. Temporary accommodation will be available by May 2017.

Advisory opinion of the ABDTOPConsult team

In view of the upcoming changes of its tasks under the Bill, the CTIVD in mid 2016 requested the ABDTOPConsult team to issue an advisory opinion on the capacity and financial resources required in this connection. A central theme in this advisory opinion, which was submitted in September 2016, was the importance of increasing the CTIVD's IT expertise. The ABDTOPConsult team found that the developments within the AIVD and the MIVD and the proposed expansion of the (interception) powers require the CTIVD to closely monitor these services not only legally, but also technically. The CTIVD should start working on increasing this expertise as soon as possible and develop it further once the new Act enters into force. Additional expertise is advisable in other contexts as well, including the handling of complaints and of reports on abuse of power.

Establishment of an IT expert unit

On the basis of this advisory opinion, the CTIVD appointed an IT adviser charged with setting up this IT expert unit in September 2016. This expert unit, which comes under the responsibility of Committee Member Meijboom, started work in late 2016 and is focusing on the implementation of what is now referred to as "Project Oversight 3.0". The objectives of this project include mapping out how the organisation and procedures of the CTIVD must be structured to ensure that effective oversight is possible in the future as well. The main focus in this connection is on the possibilities to carry out oversight on and system reviews of the automated collection, analysis, selection and destruction of large amounts of data. In this way, the CTIVD strives to significantly increase its expertise and effectiveness on, *inter alia*, information technology in 2017 and will for this reason also increase the IT expert unit's staff size.

Finally

The CTIVD believes it to be important that its oversight covers a multiplicity of subjects and responds to social developments. Its investigations have to be sound. At the same time, it aims to be very productive. Given this drive, the outside world is often surprised about the small size of its office.

The CTIVD is very happy to have a small team of exceptionally dedicated and expert staff, who are able to fathom the complex regulations and practice of the intelligence and security services like no other while exerting all possible efforts to make the proper balancing of interests between national security and privacy transparent to the public. The Committee therefore wishes to express its heartfelt gratitude for their commitment in 2016.

---

[6] ABDTOPConsult is an independent, small team of experienced senior civil servants engaged in consultancy assignments within the (national) government; refer to www.algemenebestuursdienst.nl.

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