Annual Report 2014-2015

CT IVD

Review Committee on the Intelligence and Security Services

Annual Report

2014-2015

Review Committee
on the Intelligence and
Security Services

Preface

On 1 January 2014 I took up my duties as chairman of the Review Committee for the Intelligence and Security Services (further referred to as "CTIVD" in headings and as "Committee" in the text). This was the time when Edward Snowden's revelations about the large-scale interception practices of the American intelligence service NSA dominated the debate. In the course of 2014 the Committee published two reports on the methods used by the Dutch intelligence and security services for the interception and processing of communications. The message was: improvements are necessary, but there is no systematic circumvention of the law.

Now, more than a year after I took up office, the debate centres around completely different issues. The threat of international jihadism has increased and the January 2015 attacks in Paris have brought it very close. All this seems to have relegated political interest in Snowden's revelations to second place. Furthermore, there is by now broad political support for a considerable increase of both the resources and the special powers of the General Intelligence and Security Service (GISS) and the Military Intelligence and Security Service (GISS).

This turn which the debate has taken is typical of the tension that is inherent to the existence of intelligence and security services. On the one hand they are the protectors of our national security while on the other hand they can, with their broad powers, seriously infringe our privacy. Political focus on either the one or the other aspect sometimes appears to be determined by incidents, whether or not in combination with media attention and public opinion. This underlines the importance of an oversight body that strikes an independent and impartial balance, no matter how the winds of the political or public debate blow. For the time being, the picture I have gained after one year of chairmanship is that in the Netherlands the services usually operate within the limits of the law. I write 'usually' and not 'always', because in the course of its investigations the Committee does occasionally come across unlawful acts; also in the past year.

As a rule the ministers concerned follow the conclusions and recommendations presented by the Committee in its review reports. Nevertheless, there are also some recurring points of discussion. One of them is the tension between openness and secrecy. It is clear that for the most part intelligence and security services can only effectively perform their actual activities in secrecy. Sometimes, however, this leads to a culture of secrecy that is excessive and gives rise to unnecessary myths and misunderstandings. The basic principle is that the secrecy of data relating to sources must be sacred to the services. Nevertheless, the services' working methods need not be kept secret at all times. The question whether this is necessary will have to be assessed in each individual case on the basis of the relevant facts and circumstances. Too rigid secrecy will in the long run reflect negatively on both the intelligence and security services and their oversight bodies. In this context the 'blackening out' of some passages in a CTIVD review report in late 2014 by the minister of the Interior and Kingdom Relations was certainly not a highlight.

Now, in early 2015, the Netherlands is about to make major amendments to the Intelligence and Security Services Act 2002. In addition to critical thought being given to the necessity and specifics of new and broader powers of interception, the organisation and implementation of full-fledged and effective oversight are also up for discussion. In this context the Committee's guiding principle is that any increase of powers must be accompanied by stricter safeguards for the protection of privacy. Furthermore, independent oversight must also be reinforced. At this stage the latter point is not made sufficiently clear in the government proposals as published so far.

Over the past ten years the Committee has acquired considerable expertise. Its employees are expert and professional, its investigation methods are thorough and its review reports describe and assess a range of the services' activities transparently and publicly. But more is needed in this age of big data and digitalisation of the intelligence task. In the past year the Committee has therefore established a knowledge network made up of scientific experts who can advise the Committee on these matters. In the coming period the Committee will invest in the further professionalisation of its methods and procedures, including those in the field of ICT technology, so that it can continue to exercise its oversight effectively.

This annual report 2014-2015 deals with a multitude of subjects: the review reports that were issued, the complaints that were dealt with, the international contacts, more about the amendment of the law and about the tension between openness and secrecy. It was a more than busy year.

Harm Brouwer
Chair of the Review Committee for the Intelligence and Security Services

Table of Contents

1

Introduction

The Review Committee for the Intelligence and Security Services monitors whether GISS and DISS perform their tasks in accordance with the law. It conducts investigations that result in public reports, which have secret appendices where necessary. It also acts as complaints advisory committee in cases of complaints about GISS or DISS. In addition to these tasks the Committee explores the core activities of the services as well as developments within their organisations.

Every year before 1 May the Committee brings out an annual report, which it presents to parliament and the ministers concerned. The annual report is a public document, which is also made available in English. The year reviewed in the present report covers the period 1 April 2014 – 1 April 2015. The annual report describes the work of the Committee in the review year, with references to review reports and other publications that have been issued. In its annual report the Committee also provides insight into the issues which currently play a role in the field of overseeing the intelligence and security services.

Guide to the report

First, in chapter 2, you will find an outline of the developments which the Committee has encountered in performing its oversight task. Next, in chapter 3, you will read about the investigations completed by the Committee in 2014 and what were its principal findings. Chapter 4 deals with the complaints handled by the Committee and the issues playing a role therein. In chapter 5 the Committee addresses the tension between openness and secrecy which it faces in its oversight work. In chapter 6 the Committee offers a number of considerations regarding the proposed amendment of the Intelligence and Security Services Act. Chapter 7 tells you how the Committee is working on international cooperation. Chapter 8, finally, describes the organisation of the Committee.

"The Committee sees it as its task to provide an understanding of a proper balance between national security and privacy protection".

How did the CTIVD's oversight develop in 2014-2015?

In 2014 the Committee adopted its strategy and core values for its future investigation activities. The oversight perspective must be that of an outsider looking in and thus be linked (to a greater extent) to current issues and the public debate. In addition to this reactive focus, oversight must also have a focus that is proactive and sets an assessment framework. This chapter describes how such oversight works in actual practice.

Monitoring the balance between security and privacy protection

The Committee aims at carrying out independent and impartial investigations of the lawfulness of the activities of GISS and DISS. The Committee sees it as its task to provide both the public and politicians with an understanding of a proper balance between national security and privacy protection. To achieve this, it adopts its own investigation programme which addresses among other things the various activities of the services that are relevant to privacy protection. In addition to the Committee's own investigations the ministers concerned increasingly ask the Committee, at the request of parliament or otherwise, to investigate incidents and current issues. Furthermore, the Committee has been handling an ever increasing number of complicated complaints of citizens about conduct of GISS and DISS.

Objective: informing ministers, parliament and the public

Public interest in the work of the Committee is growing. When publishing its reports the Committee sets itself the objective of informing the ministers concerned, parliament and the public about its findings as best it can. The Committee regularly holds technical briefings for the Parliamentary Standing Committee on the Interior and Kingdom Relations for the purpose of further clarifying its reports and answering questions. The ministers and the Parliamentary Standing Committee know where to find the Committee and make good use of its experience and expertise. Thanks to the frequent contacts between parliament and the Committee about the content of the Committee's public reports, the scrutiny of the services by parliament can gain strength.

Parliamentary debates on the secret appendices to the CTIVD review reports are lagging behind. In the review year the parliamentary Committee on the Intelligence and Security Services (the ISS Committee) saw no reason to consult with the Committee about the secret appendices that were issued. Contact with the Parliamentary Standing Committee on Defence was limited, due to the fact that no review reports on DISS were issued in the review year. The Committee is confident that contact with this committee will intensify as it publishes more findings regarding DISS, which it firmly intends to do in 2015.

In the review year the Committee invested in developing a new house style and website in an effort to make its activities accessible to a wide public. The new website will be launched in the course of 2015.

Ministries and services easily approachable

As in preceding years, the Committee received the full cooperation of GISS and DISS. The Committee has direct and unlimited access to all ICT systems, documents and employees. Likewise, at the ministry of the Interior and Kingdom Relations and the ministry of Defence, whose ministers are responsible for the services, the official staffs and the ministers themselves are unreservedly accessible to the Committee.

Establishment of knowledge network

click **here** for more information

In order to achieve robust and future-proof oversight it is important to closely follow relevant technological, legislative and social developments. In December 2014 the Committee therefore formed a knowledge network which is made up of a number of scientific experts. The knowledge network advises and informs the Committee about these developments. The experts participate in the network in a personal capacity. The network meets at least three times a year, for example at the time of the annual planning and evaluation processes or in response to relevant events. In this way the Committee can use the input from the knowledge network when determining the selection and focus of its investigations. In addition, the Committee has requested some experts from the knowledge network to be also available to give the Committee early-stage advice on the content, coherence and relevance of the drafts of its investigation plans, reports and advisory opinions.

Technological dimension of oversight

Furthermore, oversight is faced with continuously advancing automation of the work done by GISS and DISS. The services exercise special powers which infringe the privacy of citizens by increasingly sophisticated technological means. They also work with larger volumes of data and increasingly use automatic systems for processing them. The review officers of the Committee have legal skills and thorough knowledge of the work done by GISS and DISS. They have proved to be quite capable of reviewing the operational activities of the services. But because of advancing automation, effective oversight nowadays also requires expertise in the field of ICT technology. The Committee therefore wants to invest without delay in such know how and expertise. This must ensure that the Committee will be better able to understand the digital processing systems of the services and to assess whether the systems contain sufficient privacy safeguards. At the same time the Committee wants to work at further automating its oversight. This can be done, for instance, by building safeguards into the systems for controlling access to data and the destruction of irrelevant data in such a way that they are automatically applied and registered.

3

“The Committee itself decides which issues it will investigate. The ministers concerned and parliament can, however, ask the Committee to investigate a specific issue.”

What did the CTIVD investigate in 2014-2015?

In 2014-2015 the Committee's attention focused on completing ongoing investigations and conducting investigations requested by the ministers concerned. In the coming period the Committee will focus on a new investigation programme. This chapter tells you about the reports published by the Committee in 2014 (§3.1) and about the investigations that are still ongoing or will be started in 2015 (§3.2).

3.1 Published reports

In 2014 the Committee published the following five review reports, all relating to GISS:

- Long-term agent operations GISS (no. 37)
- Social media GISS (no. 39)
- Power to intercept and Sigint 2012-2013 GISS (no. 40)
- Van Duijn GISS (no. 41)
- forensic investigation methods involving biological materials GISS (no. 42)

The conclusions from these reports are set out briefly below.

No. 37 | Long-term agent operations GISS

Publication date: 5 June 2014

GISS has the power to deploy human sources for gathering intelligence. If these sources come from outside GISS and if GISS instructs and controls them, they are called external agents. The Committee investigated five operations which each involved an external agent whom GISS deployed for years in the field of terrorism and extremism. Usually, the guidance provided by GISS to these agents went well. In the opinion of the Committee, however, GISS should invest more in the operational planning and evaluation of long-term agent operations. GISS had given all five agents permission to commit criminal offences. The Committee found that this was in fact necessary either for the proper performance of the task of the service or for the safety of the agent. In the conduct of its investigations the Committee did not come across any unlawful acts. In its report the Committee recommended, however, that GISS should improve its procedures for giving permission for, reporting on and evaluating the commitment of criminal offences by agents.

In his reaction to the report the minister endorsed the Committee's conclusions and adopted the recommendations.

No. 39 | Social media GISS

Publication date: 4 September 2014

Click **here** for the full report

Over the past few years GISS has invested a great deal in investigations on the internet. Such investigations have become an integral and effective part of the mix of instruments available to the service, and has led to a large number of intelligence operations on social media. The Committee investigated these intelligence operations. It has established that since these operations began to take place more frequently, the implementation of the privacy protection rules has lagged behind on some points. The Committee established that the service acted unlawfully in some of the investigated operations. For example: the exercise of certain powers (deployment of agents and hacking) was not always sufficiently substantiated by reasons and reporting on operations was sometimes incomplete. The Committee further established that the secret acquisition of data from a number of large general web forums was disproportional and therefore unlawful.

In his reaction to the report the minister endorsed the Committee's conclusions and adopted the recommendations.

No. 40 | Power to intercept and Sigint 2012-2013 AIVD

Publication date: 7 October 2014

Just as it did for preceding years, the Committee investigated how GISS exercised its power to intercept in the year 2012-2013. It arrived at the conclusion that in terms of volume the use made of this power was limited. The Committee further concluded that as a rule GISS exercised the power in accordance with the safeguards included in the law to ensure the privacy of citizens. A small number of interception operations were unlawful. For instance, GISS incorrectly characterised a group of persons as an organisation, and thus exercised the power to intercept with respect to all these persons at once under what is called an organisation approval. GISS should have submitted a separate application for the minister's approval to intercept with respect to each of these persons individually. The Committee also established unlawful procedures in the interception of non-targets (persons whose communications are intercepted in order to acquire data relating to a target) and in working out conversations of legally privileged persons (confidential professionals, e.g. doctors or lawyers).

The Committee also investigated the untargeted interception of satellite and radio communications followed by searching (sigint) by GISS. With respect to a number of operations GISS stated insufficient reasons for searching such communications. This made the operations unlawful.

In his reaction to the report the minister endorsed the conclusions of the Committee and adopted the recommendations.

The Committee wanted to mention in the report against how many persons and organisations GISS had exercised the power to intercept in 2012-2013 and how many sigint operations took place in this year. The minister removed these figures from the public report invoking the obligation of secrecy. The Committee regrets this. More information on the subject is presented in chapter 4 of this annual report.

No. 41 | Van Duijn GISS

Publication date: 14 January 2015

At the request of the minister of the Interior and Kingdom Relations the Committee investigated whether in the sixties, seventies and eighties of the last century the predecessor of GISS , the Dutch Internal Security Service ("BVD"), had used special intelligence means against Roel van Duijn. For example telephone tapping, surveillance or agent operations. This was not found to be the case; the attention given by the BVD to Van Duijn and his movements mainly took the form of administrative checks. The BVD e.g. gathered information from open sources such as media reports and publications. The Committee held that by the standards of the 1960s the attention given by the BVD to Van Duijn was appropriate. From the early seventies until 1989, however, the BVD continued storing data relating to Van Duijn in his personal file. The Committee judged this to be unlawful. The Committee did not think it likely, though, that Van Duijn – as he alleged - had been included in the definitive internment list 1966/67 (also known as the 'freezer' list) which the then minister of the Interior and Kingdom Relations had approved on a proposal from the BVD.

In his reaction to the report the minister said that he had meanwhile given Mr Van Duijn the archive material that the Committee's investigation had brought into the open for the first time.

No. 42 | forensic investigation methods involving biological materials GISS

Publication date: 25 March 2015

The law authorises GISS to use forensic investigation methods involving biological materials, e.g. DNA analysis or fingerprint detection. The Committee examined which preconditions apply to the use of such methods and how these are handled by GISS in actual practice. According to the law GISS may only use forensic investigation methods involving biological materials (a) by taking samples from objects and (b) for the purpose of establishing identity. After the identification there is no legal basis for keeping the investigation results. GISS may therefore not set up a DNA database of its own. At the time of the Committee's investigation GISS did have such a DNA database, of limited size. The Committee regarded this as unlawful.

The Committee investigated all operations in which the service used forensic investigation methods involving biological materials from 2002 until today. The number of operations was not large, but the use of the methods is growing. There were only a few operations in which unlawful procedures occurred. In these operations either one or the other of the following two situations occurred:

1 GISS conducted a forensic investigation involving biological materials while the identities of the persons concerned were already known;
2 GISS did DNA analysis for the purpose of making health analysis possible.

In his reaction to the report the minister indicated that he endorsed the conclusions and recommendations of the Committee. The spokesperson of GISS has made it known in the media that the DNA database has by now been destroyed.

The Committee itself decides which issues it will investigate. The ministers concerned and parliament may, however, request the Committee to investigate a specific subject, for example in response to incidents or current events. This happens regularly. The investigation that resulted in report no. 41 on Roel van Duijn, for example, was carried out at the request of the minister of the Interior and Kingdom Relations. The same applies e.g. to the current follow-up investigation concerning Mohammed B. (see §3.2). In both cases the request was preceded by numerous parliamentary questions.

3.2 Ongoing investigations

In 2014 the Committee started two investigations at the request of ministers. In addition to these, it is currently working on four other investigations started on its own initiative.

Investigations on request

In the autumn of 2014 the ministers concerned requested the Committee to carry out two large new investigations: one concerning the assassination of Theo van Gogh in 2004 and one in reaction to the crash of flight MH17 on 17 July 2014.

Follow-up investigation Mohammed B.

The minister of the Interior and Kingdom Relations requested the Committee to investigate the actions of GISS from 2 November 2004 onwards in response to the assassination of Theo van Gogh on that day. Ten years later questions are still being asked in the media and by politicians. The Committee announced on 17 November 2014 that it would take up the request. As requested, the Committee is among other things investigating which information about possible accomplices of the murderer Mohammed B. GISS processed after the assassination of Van Gogh. It is also investigating whether this information was provided to the Public Prosecution Office for criminal investigation and prosecution purposes. Furthermore, it is investigating whether GISS destroyed any sound recordings in this context. The Committee will complete the investigation before the summer of 2015. The report will be published in the autumn of 2015.

Investigation arising from the crash of flight MH17

In addition, the ministers of the Interior and Kingdom Relations and of Defence requested the Committee, on 21 November 2014, to investigate the role of GISS and DISS in the decision-making process relating to the safety of air routes. This request originated from the investigation by the Dutch Safety Board into the crash of Malaysia Airlines flight MH17 on 17 July 2014. Questions emerged in the latter investigation about the intelligence positions of GISS and DISS which the Dutch Safety Board wished to have investigated by the Committee. The request was addressed to the Committee because of its experience and its unrestricted access to information. The Committee announced that it would take up the request on 6 January 2015. With the report to be issued the Committee will give insight into the formal consultation structure between the services and the parties that are relevant to aviation safety. It will also identify the actual activities of the two services in sharing information. Furthermore, the investigation will provide an answer to the question what information GISS and DISS possessed about the security situation in Eastern Ukraine prior to the crash of MH17 and what they did with this information. The Committee will complete the investigation in April 2015 and will send its findings directly to the Dutch Safety Board. This Board will publish the Committee's report together with its own report.

Regular investigation programme

In the context of its own regular investigation programme the Committee is, moreover, working on four other investigations. Two investigations concerning the exercise of the power to intercept and sigint, and two concerning the cooperation between GISS, DISS and foreign services.

Power to intercept and sigint

The Committee is investigating the exercise of the power to intercept and sigint for the period 2014-2015, as it did before with respect to earlier periods. In addition, the Committee is specifically investigating two sigint operations of DISS that were carried out in support of the Dutch efforts to combat piracy in the Horn of Africa. The Committee considers it appropriate to investigate these operations separately. The fact is that in its statement of reasons for its exercise of the power to intercept and select DISS did not state in advance at which specific persons or organisations the operations were targeted.

Cooperation with foreign services

The Committee has for some time been investigating the cooperation of DISS with foreign services. It is a comprehensive investigation and has taken a long time to complete, but it is now in its final phase. The report will present an overview of how DISS has put the various forms of cooperation with foreign services into practice in the period 2007-2013. The report will be published in the summer of 2015.

The Committee will also investigate the cooperation between GISS and foreign services. It wants to focus this investigation on some specific current forms of cooperation. The Committee has already announced its investigation but has not yet been able to take it in hand because of the requests to investigate other issues.

4

Complain

"The Committee's advisory opinion on a complaint can offer a good opportunity to show how the services perform their tasks in actual practice."

Which complaints did the CTIVD handle in 2014-2015?

A person who wants to complain about conduct of GISS or DISS must lodge the complaint with the minister of the Interior and Kingdom Relations or the minister of Defence, respectively. If the minister decides to deal with the substance of the complaint, he calls in the Committee as an independent complaints advisory committee. The Committee then assumes full charge of handling the complaint. It hears the complainant(s) and examines the files of the service in question and/or hears its employees. The Committee assesses whether the conduct of GISS or DISS was proper. Finally, the Committee submits an advisory opinion to the minister, following which it is the minister who decides whether the complaint is well-founded or unfounded.

This chapter first sets out how many complaints the Committee handled in 2014 (§4.1). Next, §4.2 describes the various complaints. §4.3 gives background information about complaints while §4.4 gives background information about the interception of communications from or with lawyers.

4.1 Number of complaints handled

In the review year the Committee handled ten complaints: eight about GISS and two about DISS. It submitted advisory opinions on them to the minister concerned. At the close of the review year the Committee was still processing four complaints about GISS. The table below shows the advisory opinions given by the Committee on each of the ten complaints dealt with.

Table 1 Advisory opinions on complaints dealt with

Aantal klachten over AIVD	Number of complaints about DISS	Advisory opinion
2	–	Manifestly unfounded
3	1	Unfounded
2	1	Partly unfounded, partly well-founded
1	–	Well-founded

With respect to eight complaints the minister concerned adopted the Committee's advisory opinion. With respect to two complaints the Committee submitted its advisory opinion to the minister of the Interior and Kingdom Relations, who has, however, not yet given a decision.

Complaints that were not taken up

In four cases, one about DISS and three about GISS, the minister concerned submitted complaints regarding which the Committee held that there were reasons for not taking up the complaint. In theses cases:

1 an objection procedure or appeal procedure was already pending and handling the complaint had no added value; or
2 the complainant's interest was manifestly insufficient; or
3 the complaint related to conduct dating back more than one year.

Since it is the minister concerned who decides on the admissibility of complaints, the Committee pointed out these reasons to the minister and further did not examine these complaints.

In one case the complainant withdrew his complaint about DISS, because on further consideration it was a complaint about GISS.

4.2 Description of the complaints dealt with

A short thematic description of the complaints dealt with by the Committee in the review year is given below. The descriptions have been anonymized, because the Committee is not free to publicly disclose information on individual complaints. It is up to the minister or the complainant to decide whether or not to do so. The descriptions are based on the information released by the minister to the complainants.

Manifestly unfounded

With respect to two complaints about GISS the Committee advised the minister of the Interior and Kingdom Relations to declare the complaint manifestly unfounded. In the opinion of the Committee it was immediately clear from the relevant complaint notices that there could not be any reasonable doubt about the opinion that the complaints were unfounded.

Duty of care for and guidance of human sources

Two complaints were lodged by (former) human sources of GISS. These persons complained about how GISS had treated them. In one complaint the complainant alleged that GISS had taken insufficient account of his personal circumstances in the guidance given him, that it had not guided him properly and had put him under pressure. With respect to these elements of the complaint, the Committee's examination did not show improper conduct on the part of GISS. This part of the complaint was therefore unfounded. The Committee did, however, establish that GISS should have concluded at an earlier stage that the complainant's personal circumstances called for termination of the collaboration. On this point GISS had not satisfied the requirement of a reasonable evaluation of the respective interests. By failing to do so GISS acted improperly towards the complainant. This part of the complaint was therefore well-founded.

The other complaint was about how GISS had handled its statutory duty to ensure the secrecy and safety of human sources. The Committee established that GISS had failed in fulfilling this statutory duty of care towards this source. Moreover, GISS had acted contrary to commitments made to the source. The Committee therefore found this complaint well-founded in its entirety.

Interception of communications

In one complaint the complainant alleged that GISS had wrongfully intercepted his communications. The Committee's examination showed, however, that there had been no improper conduct of GISS towards the complainant. The complaint lacked any factual basis. This meant that the conduct that was the subject of the complaint had no basis in the facts as established by the Committee's examination. Consequently, the complaint was unfounded.

Interception of communications and approaching persons close to the complainant

One complaint about DISS was that DISS had intercepted the complainant's communications and had approached persons close to the complainant. With regard to interception the Committee concluded that there had been no improper conduct of DISS regarding the complainant. This part of the complaint lacked any factual basis. The conduct that was the subject of the complaint had therefore no basis in the facts as established by the Committee's examination.

With regard to approaching persons the Committee concluded in the first place that DISS had reasonable cause to investigate the complainant. The Committee held, however, that DISS then went too far when, for the purpose of its investigation, it approached several persons close to the complainant. This approaching of persons severely infringed the complainant's privacy. According to the Committee less onerous means were available to gather the information needed for the investigation. Consequently, DISS had not satisfied the standards of proportionality and reliability. As a result the service had failed to sufficiently respect the complainant's privacy. Therefore, this part of the complaint was well-founded.

Interception of communications from or with lawyers

In four complaints the complainants alleged that confidential communications from or with a lawyer had been intercepted. The complainants were either lawyers themselves or were in contact with a lawyer, for instance as a client.

The Committee's examination of three of these complaints, two about GISS and one about DISS, showed that there had been no improper conduct of the service in question towards the complainants. The complaints therefore lacked any legal basis. This meant that the conduct that was the subject of the complaints had no basis in the facts as established by the Committee in its examination. The Committee held these complaints to be unfounded.

One complaint about GISS was about direct and indirect (via clients or other persons) interception of communications of lawyers and the absence of safeguards in GISS' internal procedures for direct and indirect interception. In the Committee's opinion the complaint about direct interception of communications of lawyers was unfounded. The Committee came to a different conclusion, however, with respect to the indirect interception of communications of lawyers. It established that GISS had wrongly worked out certain conversations between clients and lawyers. It was evidently obvious that these communications could not be considered relevant to any investigation of GISS. The Committee held that GISS had thus acted contrary to the proportionality standard of proper conduct. This element of the complaint was partly well-founded. The Committee further established that the internal procedure for direct interception was covered by adequate safeguards. This element of the complaint was unfounded. The procedures for indirect interception, however, were not based on established policy and consequently lacked safeguards. This element of the complaint was well-founded.

See §4.4. for further background information on the interception of communications between lawyers and their clients.

4.3 Background information: informing the complainant about the outcome of the complaint handling

After the Committee has examined a complaint, it sends its findings and advisory opinion to the minister concerned. As stated above, it is the minister who then decides on the complaint. The minister also decides which information about the Committee's advisory opinion and about his own decision on the complaint he will provide to the complainant. If the information contained in the Committee's advisory opinion is not classified as state secret, the minister will in practice send the advisory opinion to the complainant in its entirety. Things are different if the information contained in the advisory opinion is classified as state secret. Then the minister will assess in each individual case which information he may provide to the complainant. The minister may e.g. decide to declassify information and explain his decision on the complaint in writing as fully as possible. Another possibility is that of sending the complainant not only the decision whether or not the complaint is well-founded; but also an invitation to come and inspect the advisory opinion at the ministry or at the service's office, or to come and have the decision orally explained by the ministry or the service. If the minister departs from the Committee's advisory opinion, he is required by law to send it to the complainant.

On several occasions in the review year the Committee suggested that the minister of the Interior and Kingdom Relations or the minister of Defence give complainants information which up to then had been classified as state secret, by declassifying this information. These complaints concerned situations in which the Committee took the view that particular importance should be attributed to the interest of the complainant, for example where the complainant had himself collaborated with GISS and complained about the way he had been treated. There were also cases in which the Committee held that the interest of public accountability and awareness/recognisability must take precedence over regular confidentiality policy. An example is a complaint that touches upon a subject of current public debate in the context of which it is desirable to obtain clarity as to what the services are or are not doing. A complaint may then present an excellent opportunity to show how the services perform their tasks in actual practice. In the Committee's opinion it will not harm national security if additional information is provided to the complainant by way of exception. With respect to some complaints about GISS the minister of the Interior and Kingdom Relations did not follow these suggestions.

4.4 Background information: interception of communications from or with lawyers

The handling of some of the complaints described in §4.2 attracted quite a lot of political and social attention. This happened after publications by the complainants about how their complaints about the interception of communications from or with lawyers had been dealt with. As stated above, the Committee itself cannot explain its advisory opinions on individual complaints. It can, however, outline the framework against which it reviews the conduct of the services when it examines these complaints about the interception of communications from or with lawyers. Furthermore, the Committee thinks it important to give some background information for the discussion on the subject, also with a view to the forthcoming amendment of the ISS Act 2002. You will find this information below.

The ISS Act 2002 lacks safeguards for persons enjoying professional privilege

The ISS Act 2002 does not contain specific safeguards for persons enjoying professional privilege (persons who have a professional obligation of confidentiality, e.g. lawyers or physicians). The Act does not distinguish between persons who do, and persons who do not enjoy professional privilege. This may create the impression that GISS and DISS need not take account of professional privilege when they exercise special powers. Criminal law and the European Court of Human Rights ECHR), however, do make this distinction. Professional privilege is considered a general principle of law which the public authorities must take into account; and so must the intelligence and security services.[1]

[1] Zie over het strafrecht bijvoorbeeld HR 1 maart 1984, LJN AC9066, NJ 1985, 173, arrest *Ogem-Notaris Maas* (notariële geheimhouding). Over de rechtspraak van het EHRM zie onder andere EHRM 25 maart 1992, nr. 13590/88 *(Campbell t. Verenigd Koninkrijk*).

The Committee developed an assessment framework for the interception of the communications of persons enjoying professional privilege

Since the entry into force of the ISS Act 2002 the Committee has for this reason developed a separate assessment framework for the interception of communications of persons enjoying professional privilege in a number of review reports. As professional privilege is a general principle of law, this must be reflected in how the services exercise their special powers. The Committee holds that within the existing legal framework, the interception of conversations with persons enjoying professional privilege must be subjected to more stringent requirements than those applying with respect to other conversations. To safeguard professional privilege, policy and practice must meet the following criterions:

- Exercising the power of interception against a person enjoying professional privilege himself such as a lawyer (direct interception) requires the existence of concrete indications that a direct threat to national security exists.[2]
- Exercising the power of interception against a person enjoying professional privilege himself (direct interception) requires the services to assess whether the interest of the proper performance of their tasks carries greater weight than the interest of professional privilege (more stringent proportionality test).[3]
- Prior to exercising the power of interception against a target while it is foreseeable that he will be in contact with a person enjoying professional privilege (indirect interception), the services must state reasons for that which they will do with the communications between the target and the person enjoying professional privilege.[4]
- The above assessments must be laid down in writing in the document stating the reasons for exercising the power of interception.[5]
- If the services wish to prolong the exercise of the power of interception, they must apply to the minister concerned for permission to do so every month[6] instead of every three months.

---

2 *Parliamentary Papers II* 2014/15, 30977 no. 107 (appendix).

3 *Parliamentary Papers II* 2014/15, 30977 no. 107 (appendix).

4 CTIVD review report no. 40 on the use by GISS of the power to intercept and the power to select sigint, September 2012-August 2013, *Parliamentary Papers II* 2014/15, 29 924, no. 116 (appendix), §10, available at www.ctivd.nl.

5 CTIVD review report no. 19 on the application by GISS of article 25 ISS Act 2002 (interception) and article 27 ISS Act 2002 (selection of untargeted interception of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §8, available at www.ctivd.nl.

6 CTIVD review report no. 10 on the investigations by GISS into the leaking of state secrets, *Parliamentary Papers II* 2006/07, 29 876, no. 19 (appendix), sections 8 and 9, available at www.ctivd.nl.

- Working out telephone conversations with persons enjoying professional privilege is likewise subject to a more stringent proportionality test: prior to working out telephone conversations the services must assess for each individual conversation whether the interest of the proper performance of their tasks carries greater weight than the interest of professional privilege.[7]
- These procedures must be laid down writing in a policy document.[8]

This is the framework against which the Committee examines complaints about the interception of communications of a person enjoying professional privilege, for instance a lawyer, under the current ISS Act 2002.

Developments in the context of the intended amendment of the ISS Act 2002

The government recently presented a bill introducing the requirement of an independent assessment prior to the exercise of special powers against journalists, if these powers are exercised for the purpose of tracing journalists' sources.[9] Lawyers advocate introducing a similar independent assessment prior to the exercise of special powers against lawyers. They also advocate introducing a number-recognition system as used in criminal law. This system ensures that in principle conversations with lawyers cannot be intercepted. The Committee is closely following these developments.

7 CTIVD review report no. 10 on the investigations by GISS into the leaking of state secrets, *Parliamentary Papers II* 2006/07, 29 876, no. 19 (appendix), sections 8 and 9, available at www.ctivd.nl, *Parliamentary Papers II* 2014/15, 30977 no. 107 (appendix).

8 CTIVD review report no. 10 on the investigations by GISS into the leaking of state secrets, *Parliamentary Papers II* 2006/07, 29 876, no. 19 (appendix), sections 8 and 9, available at www.ctivd.nl, *Parliamentary Papers II* 2014/15, 30977 no. 107 (appendix).

9 Parliamentary Papers II 2014/15, 34 027, no. 5.

5

"The government wishes to increase the services' powers of interception"

What is important in amending the Intelligence and Security Services Act?

The Intelligence and Security Services Act 2002 has now been in effect for thirteen years and is on the eve of being drastically amended. In December 2013 the ISS Act 2002 Evaluation Committee (also known as the Dessens Committee) came to the conclusion that the existing statutory powers were no longer sufficient and should therefore be increased. The evaluation committee tied the increase of powers to enhanced statutory safeguards of privacy and strengthened oversight.[10] A first government reaction to the evaluation report in March 2014 was followed in November 2014[11] by a more detailed explanation of the new interception regime envisaged by the government.[12] The bill is expected to be presented for internet consultation in May 2015. The Committee would like to see all actors in the oversight system, from parliament to civil society, contribute to this discussion on the practical necessity of increasing the services' powers. During the internet consultation process the Committee will contribute its comments on the concrete legislative texts and explanatory notes. In preparation for these comments and having regard to all the aforementioned publications and international developments in the field of intelligence and security services and their oversight, the Committee raises the following questions and issues.

[10] Evaluatie Wet op de inlichtingen- en veiligheidsdiensten 2002. Naar een nieuwe balans tussen bevoegdheden en waarborgen, December 2013.

[11] *Parliamentary Papers II* 2013/14, 33 820, no. 2.

[12] *Parliamentary Papers II* 2013/14, 33 820, no. 4.

1. Is the house now sufficiently in order?

In the course of its investigations the CTIVD has noticed that GISS and DISS are very much aware of the importance of privacy protection. In this sense the house is reasonably in order. There has been no systematic collection of data in disregard of the law. Nevertheless, the quality of the substantiation of the need to exercise special powers and of the reporting on such exercise is a recurring cause for concern. In fact, under the current ISS Act 2002 the services have not yet been able to establish a procedure that ensures their consistent compliance with the statutory safeguards when selecting from untargeted interception (sigint).[13] The Committee therefore wonders how the government thinks the services can achieve such compliance in the case of their having new and wider powers.

2. To what extent is increasing the interception powers effective and necessary?

The Committee considers it a shortcoming that up to the present there has been almost no debate on the necessity of increasing the powers of the services. The main focus of the debate is placed too readily on the lawfulness of the acts of the services and less on the efficiency or effectiveness of the interception powers. The discussion may thus never go beyond the finding that nowadays 90 percent of communications goes via the cable and that therefore the 'traditional' power of untargeted interception of satellite communications (the remaining ten percent) is no longer enough. But can this finding alone and by itself carry the conclusion that the powers of the services must be increased? Is it not necessary, before one can come to this conclusion, to have a picture of the effectiveness and/or the lack thereof of the existing powers? On the international level, too, this is a question which continues to be a matter of concern, without however eliciting any definite answers.[14] The starting point should be that it must first be convincingly demonstrated that new powers are necessary because the present powers are insufficient before considering an increase of the statutory powers. The test of effectiveness also finds support in the test of legitimacy which article 8 of the European Convention on Human Rights prescribes for reasons of privacy protection. This test must not only assess the damage to national security that will be prevented, but also the harm that the powers of interception will cause to individual persons.

---

[13] CTIVD review no. 35 on the exercise by GISS of the power to intercept and the power to select Sigint, *Parliamentary Papers II* 2012/13, 29 924, no. 101 (appendix), §3.2 and §6; CTIVD review report no. 31 on the exercise by GISS of the power to intercept and the power to select Sigint, *Parliamentary Papers II* 2011/12, 29 924, no. 86 (appendix), §3.2; CTIVD review report no. 28 on the use by DISS of Sigint, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), §8.3; CTIVD review report no. 26 on the lawfulness of the performance by GISS of the foreign intelligence task, Parliamentary Papers II 2010/11, 29 924, no. 68 (appendix), §5.4; CTIVD review report no. 19 on the application by GISS of article 25 ISS Act 2002 (interception) and article 27 ISS Act 2002 (selection of non cable-bound telecommunications acquired by untargeted interception), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §7. All reports are available at www.ctivd.nl.?

[14] See e.g.: Privacy and Civil Liberties Oversight Board, *Report on the Telephone Records Programme Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, 23 January 2014, https://www.pclob.gov/library.html, p. 11; US National Research Council, *Bulk Collection of Signals Intelligence: Technical Options*, January 2015, http://www.nap.edu/catalog.php?record_id=19414, Conclusion 1; SURVEILLE Paper Assessing Surveillance in the Context of Preventing a Terrorist Act, FP7-SEC-2011-284725, published on 29 May 2014; UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, report 23 September 2014, A/69/397, §§51, 52.

3. How can the privacy of innocent citizens be protected as much as possible?

The government wishes to increase the powers of untargeted interception. This means that the services will on a larger scale intercept communications of persons who are not targets of the intelligence and security services. This calls for additional obligations and safeguards. In spite of being untargeted, the interception should be 'targeted' as much as is possible. The data should be filtered right from the first phase of interception. The separation of relevant and non-relevant communications should be made as soon as possible after interception. Storage periods of non-relevant communications must be short and must be specifically laid down by law. Destruction of such communications should mean that the data is really and definitely destroyed. And access and use of the intercepted data must be made subject to conditions and restricted by both organisational and technical means.

4. What are the minimum requirements that must apply to the oversight of the (increased) powers of interception?

The Dessens evaluation committee makes the increase of powers conditional on reinforced oversight. It recommends in particular that the Committee's findings of lawfulness or unlawfulness must be given binding force. The government is explicitly not following this recommendation. Notably, it puts its faith in broadening the scope of the current requirements that the ministers responsible for the performance of their tasks by the services must themselves grant permission for interception, and not in strengthening independent assessment of applications. The position and powers of the Committee are strengthened only in the field of complaints handling. International judgments appear to indicate, however, that this does not suffice to meet human rights standards in the area of privacy protection. In order to settle the issue the Committee has commissioned Leiden University to conduct a scientific study of the minimum requirements set by international law on oversight in this field. The results of the study will be published on the Committee's website in May 2015.

6

"An overstrong culture of secrecy not only creates scope for unacceptable practices, it may also give rise to myths and misunderstandings among citizens."

What is the position taken by the CTIVD, now and in the future, on the matter of secrecy?

One of the explanations why Edward Snowden caused such a commotion with his revelations lies in the strict secrecy surrounding the work of intelligence and security services. It was in fact thanks to this secrecy that the American intelligence services NSA could develop large-scale interception practices. Although a judge appointed for the purpose had given permission for the interceptions behind the scenes, it subsequently transpired that there was no legal basis for the procedure. It was only after the revelations that a supervisory body was given the opportunity to describe and assess the practices in a public report.

CTIVD reports are published

The Dutch Intelligence and Security Services Act 2002 contains a provision, included at the request of parliament, that the reports of the Committee must be published. This provision has had great significance, among other things for the quality of the process of political accountability for the performance of tasks by the services. In its public reports the Committee not only explains how the law must be interpreted and applied in individual cases, but also provides insight into the policies of the services and their operational practice. The Committee only attaches a secret appendix to a report if it can properly substantiate the necessity of secrecy. This proactive publication of reports by the Dutch oversight body attracts international attention. Long before Snowdon's revelations the Committee was already publishing detailed reports on procedures for untargeted interception and on cooperation with foreign intelligence and security services. It also had these reports translated into English for international dissemination.

Openness calls for meticulous care

Openness in the midst of the traditional culture of secrecy of intelligence and security services requires insight and creativity. An oversight body has to know the ins and outs of the rationale for secrecy and of the applicable conditions. Intelligence and security services can only be effective if they carry out their operations in secrecy. They need leeway so that they can be quicker and more inventive than those who pose a threat to national security. The drive for openness may not interfere with this leeway without good reason.

In the course of the years the Committee has gained a lot of expertise in finding a balance between the importance of openness and the importance of national security. It bears in mind that the services must be able to carry out their investigations in appropriate secrecy. At the same time the parliament and the public must acquire an insight into how the services interpret the statutory frameworks within the limits of which they must operate.

Greater transparency would have been possible

The transparency pursued by the Committee in the review year was not achieved without a struggle. Publication of its findings was often preceded by discussions with the intelligence and security services and the responsible ministers, respectively. At these meetings the parties frequently achieved a satisfactory balance, but not always. Under current law the minister concerned has final say by virtue of his responsibility for national security.

In the review year, for instance, the Committee wanted to publish with respect to how many persons and organisations GISS had exercised the power to intercept, in order to give society some understanding of the scale of these privacy-infringing activities. The minister of the Interior and Kingdom Relations, however, blacked out these figures in the Committee's review report and thus made them illegible. The minister held that these figures provided insight into the current method used by GISS and must therefore be classified state secret. The Committee did not and still does not agree. The figures give an idea of the scale at which these special powers were exercised, while the outside world cannot deduce from them against which (categories of) persons and organisations the power was actually exercised. Moreover, publishing figures happens in neighbouring countries on an annual basis.

Another point of debate is how much can be disclosed to persons who complain about conduct of GISS or DISS. Situations are conceivable (and have occurred) in individual cases where the interest of public accountability and awareness must take precedence over the regular policy of secrecy. The Committee discussed this above in §4.3.

An overstrong culture of secrecy not only creates scope for unacceptable practices, it may also give rise to myths and misunderstandings. As Snowden's revelations have shown, this may eventually come to work against the intelligence and security services themselves. The Committee will continue its efforts to achieve a good balance between openness and secrecy.

7

"In the view of the Committee, this can be the start of a strong network of like-minded oversight bodies, which develops common standards and contributes to enhanced international transparency and debate."

How does the CTIVD cooperate internationally?

The Committee maintains close contacts with its fellow oversight bodies abroad. It exchanges knowledge, experience and investigation methods, for instance at international conferences. In July 2014, for example, it participated in the biennial International Intelligence Review Agencies Conference in London. The Committee also visited Brussels, London and Berlin for bilateral contacts and received fellow oversight bodies from Switzerland, Germany, Belgium, Norway and Sweden.

click **here** for more information

For the Committee, events in 2014 once again underlined the importance of international cooperation between oversight bodies. This chapter presents the Committee's vision of this subject and also how it intends shaping the cooperation.

Limits to national oversight

The Committee points out that more and more often the question is raised in international forums whether national oversight is still sufficient. The work of intelligence and security services extends beyond national borders; operations are carried out together with other services and exchanging information is a commonplace procedure. The mandate of national oversight bodies is limited to the information about such cooperation that is available at the own national service. This makes it difficult to examine what foreign services do with data provided by a national service. Often, it is not possible for an oversight body to ascertain whether the data which the national service receives from abroad was collected lawfully. A national oversight body can only examine whether the national service provided or received information lawfully. This limit on what national oversight can do is also referred to as an 'accountability deficit'.

Is international oversight possible?

Bridging this deficit is not easy. It has been suggested to draft an international 'intelligence codex' containing the basic rules for the work of intelligence and security services. An international oversight body would then monitor compliance with the codex. Especially the latter proposal will easily be a bridge too far in the world of national security. Cooperation between intelligence and security services is a complex process, which takes place on the basis of strict conditions. It is dictated by sovereignty and national interests. It is not to be expected that states will be willing to accept restraints on this most delicate element of their sovereignty.

A cautious start: strengthening relations between national oversight bodies

Another, more feasible approach is that of strengthening relations between national oversight bodies. They can further develop the present exchange of knowledge, experience and investigation methods, for example by coordinating their annual plans and identifying cross-border issues in the process. At the same time they can together choose a theme which each national oversight body is to examine that year, each within its own jurisdiction. For example: which means does the national service use for the surveillance of departing jihadists? And what role does international cooperation play in the matter? After identifying a theme, the oversight bodies can further coordinate the planning and structure of their review activities. If subsequently each oversight body records its findings in a public report, the reports can be compared and joint lessons learned. All this can be done without disclosing any state secrets.

Such a strengthening of relations between national oversight bodies seems a modest way of addressing the accountability deficit. In the vision of the Committee, however, it can be the start of a strong network of like-minded oversight bodies, which develops common standards and contributes to enhanced international transparency and debate. The Committee is taking the initiative in this development and has already discussed this option with several fellow oversight bodies. The responses have been positive. In the coming period the Committee wishes to further explore how it can in this way strengthen international oversight.

8

How was the CTIVD organised in 2014-2015?

In early 2014 the Committee was partly renewed. Harm Brouwer took office as chair and Aad Meijboom joined the Committee as a new member. Liesbeth Horstink-Von Meyenfeldt ensures continuity with her extensive experience as a member of the Committee.

Harm Brouwer
Chair

Liesbeth Horstink-Von Meyenfeldt
Member

Aad Meijboom
Member

The Committee is supported by an office consisting of a secretary to the Committee, six review officers and an administrative secretary. The Ministry of General Affairs is the managing ministry which provides management support to the Committee. The Committee has the full cooperation of the managing ministry. The Committee itself decides on the expenditure of its financial resources. Since 2002 the Committee has had a budget of around one million Euros per year.

At the end of 2014 the Committee informed the ministry of General Affairs that it needed more financial resources. The Committee notes that with the increasing number of investigations on request, it has insufficient capacity to carry out its own investigation programme. In addition, the Committee has insufficient funds to cover current costs and lacks the financial means to invest in stronger oversight, including investment in the technological development of its oversight. Starting in 2016 an amount of 0.5 million Euros will be added to the Committee's budget on a structural basis to strengthen the security chain. In principle, this will be sufficient to cover expected costs for the next few years.

This development of the Committee is separate from the reinforcement of oversight that will be necessary if the interception powers of GISS and DISS under the ISS Act 2002 are increased. The government has proposed such an increase of powers following the Dessens evaluation report.

Anna van Saksenlaan 50 | 2593 HT Den Haag
The Netherlands
T +31 70 315 58 20 | **F** +31 70 381 71 68
E info@ctivd.nl | www.ctivd.nl