ANNUAL REPORT 2012 - 2013

OF THE REVIEW COMMITTEE
FOR THE INTELLIGENCE AND SECURITY SERVICES

The annual report closes at 31 March 2013

Table of contents

Introduction 5

Chapter 1 The reporting year in broad outline 7
- General 7
- In-depth investigations 7
- Exploratory monitoring 9
- Complaints 9
- Advisory task 11
- Cooperation of GISS and DISS 11
- Regular contacts 12

Chapter 2 ISS Act 2002 decennial 15

Chapter 3 (De)classification by GISS 17

Chapter 4 International contacts 19

Appendices:
I The Committee (background) 21
II Overview of review reports 29

Review reports issued in the reporting year: 33
III Review report 30b: previous recommendations of the Committee regarding GISS
IV Review report 31: the use by GISS of the power to tap/intercept and the power to select Sigint 35
V Review report 32: the official messages issued by DISS in the period January 2006 up to and including June 2011
VI Review report 33: the classification of state secrets by GISS 55

Symposium of 18 April 2012

ANNUAL REPORT 2012-2013

Introduction

In 2012 the Intelligence and Security Services Act (ISS Act 2002) had been in force for ten years. The Review Committee for the Intelligence and Security Services (CTIVD, further referred to as: the Committee) owes its existence to this Act. The territory in which the intelligence and security services operate is hard to negotiate for outsiders and in many cases even inaccessible, which is all the more reason to set high standards for the oversight of these services.

The Committee therefore found a good reason in the tenth anniversary of the ISS Act 2002 to ask emeritus professor C.J.C.F. Fijnaut, an acknowledged expert in the field, to subject the oversight system created by the ISS Act 2002 to a critical examination, and particularly the Committee's own role within the system. The work done by professor Fijnaut resulted in the publication of Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel [The Oversight of the Intelligence and Security Services: the need for more effective concerted action]. Not only was the study debated at a well-attended conference organised by the Committee in April 2012, it will undoubtedly be frequently consulted in coming years.

In the reporting year the ministry of the Interior and Kingdom Relations and the ministry of Defence did the necessary preparatory work for an amendment of the ISS Act 2002. Having done this, and at the request of the Second Chamber, the ministers then decided to have an evaluation of the ISS Act 2002 carried out first. The ISS Act 2002 Evaluation Committee was set up in February 2013. Based on its knowledge and experience the CTIVD will provide advice to the responsible authorities for the purposes of both the evaluation and the coming amendment of the ISS Act 2002.

From the start the Committee has carried out in-depth investigations at the General Intelligence and Security Service (GISS) and the Military Intelligence and Security Service (DISS) to ascertain whether the respective services performed their tasks within the legal framework set therefore. The wiretapping power, for example, is the subject of an annual in-depth investigation. In the present reporting year the Committee also endeavoured to form a picture of certain specific, often topical, activities of the services in order to be in a

better position to determine the subjects on which it will have to focus its attention in future in-depth investigations. Such exploratory monitoring by means of scans contributes to the efficient use of the Committee's review capacity.

The Committee is not only interested in what the services do, but also in the follow-up given to its reports and the recommendations set out in them. In the reporting year it issued a report in which it examines reactions within GISS to its recommendations in the last ten reports. From now on the Committee aims at conducting a follow-up investigation as early as one year after issuing a report to see to what extent its recommendations have been acted upon.

In this reporting year the Committee could again count on the full cooperation of the services. The Committee always found a willing ear with the ministers concerned and their civil servants. The Committee appreciates the wish of parliament to be kept informed of the findings of the CTIVD by means of regular meetings with the standing committees for the Interior and for Defence and also with the Committee on Intelligence and Security Services.

Chapter 1

The reporting year in broad outline

General

The Committee oversees whether GISS and DISS perform their tasks lawfully. For this purpose the Committee conducts in-depth investigations resulting in public review reports, where necessary with secret appendices; it investigates the core activities of and developments within the services; and it acts as complaints advisory committee in the case of complaints about the services. The Committee is an independent public body.[1]

The Committee is composed of three members. They are at present:

- Mr. A.H. van Delden, chairman
- Mr. E.T. van Hoorn, member
- Mrs. S.J.E. Horstink-von Meyenfeldt, member

The Committee members all work part-time. Committee member Van Hoorn has announced that he will retire with effect on 1 September 2013. The procedure for recruiting a new member has already been started.
The Committee is supported by its staff, composed of a secretary, Mrs. H.T. Bos-Ollermann LLM, five review officers and an administrative adviser.

In-depth investigations

The Committee completed four in-depth investigations in the reporting year.

The Committee regularly investigates to what extent GISS and DISS have implemented the recommendations made by the Committee in its review reports. In the reporting year the Committee issued a report on this subject with respect to GISS (review report 30b, see appendix III).

[1] See appendix I for a more detailed account of the Committee.

In 2010 the Committee decided to carry out annual in-depth investigations of the use of the wiretapping power and the use of Sigint by GISS. For this purpose it examines the exercise of these powers every quarter. The report on the first year (September 2010 – August 2011) has been issued (review report 31, see appendix IV).

In 2006 the Committee for the first time investigated the official messages sent by DISS to government agencies such as the Public Prosecution Service, the Immigration and Naturalisation Service and senior officials at the ministry of Defence. In the present reporting year the Committee issued a report on its investigation of the official messages issued by DISS since that time (review report 32, see appendix V).

At the request of the Second Chamber and the minister of the Interior and Kingdom Relations the Committee investigated the classification of state secrets by GISS. This resulted in a review report which describes the classification and declassification procedures, both in theory and in practice (review report 33, see chapter 3 and appendix VI).

In the reporting year the Committee further worked on the large-scale investigation of the cooperation by DISS with foreign intelligence and security services and on the investigation of a number of long-term agent operations of GISS. These investigations are expected to be completed in 2013. The use made by GISS of the wiretapping power and the power to use Sigint continues to be a subject of investigation by the Committee on an annual basis. The review report for the period September 2011 – August 2012 will be issued in the course of 2013. The investigation of the use of these powers since September 2012 is ongoing.

The Committee thinks it important to monitor the implementation of its previous recommendations. For this purpose it carries out follow-up investigations. The review reports resulting from two follow-up investigations regarding GISS will be issued in the course of 2013. They are the follow-up investigation with regard to GISS' obligation to notify and the follow-up investigation with regard to the official messages issued by GISS concerning holders of or candidates for political office.

In the reporting year the Committee also started an investigation into the use by GISS of several investigation methods involving forensic biology. In addition, the Committee announced its intention to carry out a follow-up investigation of the cooperation by GISS with foreign services.

On 16 April 2012 the Committee received a request from the secretary of the Parliamentary Standing Committee on Defence to review whether the procedure used by DISS to assess whether 78 security clearances that had been issued should be revoked, satisfied the legal requirements. In its reply the Committee stated that in several earlier review reports it had

already discussed the legal framework for this subject.[2] In the case of the aforementioned 78 individual cases the power of reviewing the lawfulness of revocation of the security clearances is reserved to the courts, which will in these cases be able, just like the parties, to fully inspect the information underlying the decision to revoke the security clearance. The fact is that information concerning criminal records is not state-secret information. For this reason the Committee does not think it presents an added-value in reviewing the assessment procedure used by DISS in these individual cases. It therefore informed the Parliamentary Standing Committee on Defence that at this moment it saw no reason to carry out a further in-depth investigation of the procedure followed by DISS with respect to these 78 files.

Exploratory monitoring

The Committee has made it its aim to obtain a broad picture of the core activities of GISS and DISS. It has arranged with the services to be informed by them of important events and developments. The Committee itself also gathers information concerning activities of GISS and DISS. It used to do so by periodically monitoring standard activities. In the past year the Committee used scans to identify and analyse various activities of the services with which it is less familiar. By keeping itself informed of developments at GISS and DISS, the Committee can make sound assessments when it decides which in-depth investigations it will carry out. The Committee also gives consideration to the relevance of a subject to the task performance by the services and to the extent to which a subject touches on relevant legal questions and external interests. It was such exploratory monitoring that gave rise to the investigation of forensic investigation methods used by GISS which the Committee announced in the reporting year.

Complaints

A person who wants to complain about GISS or DISS must lodge the complaint with the minister of the Interior and Kingdom Relations or the minister of Defence, respectively. If the complaint is taken up, the minister calls in the Committee as an independent complaints advisory committee. The Committee then assumes full charge of handling the complaint. It hears persons concerned in the matter and examines the files of the service in question. The Committee submits an advisory opinion to the minister, following which it is the minister who takes the ultimate decision. If the minister departs from the

[2] Reference is made to CTIVD Review Report no. 11a on the lawfulness of the implementation of the Security Screening Act by DISS, *Parliamentary Papers II* 2006/07, 29 924, no. 15 (appendix), §5.4, and CTIVD Review Report no. 30a on previous recommendations of the Committee regarding DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 77 (appendix), §3.3, both available (in Dutch) at www.ctivd.nl.

Committee's advisory opinion, the advisory opinion must be sent to the complainant. If the advisory opinion is classified, things are different. The minister assesses on a case-by-case basis which information can be provided to the complainant. The minister may, for example, decide to declassify information and explain the decision as fully as possible in writing. The Committee recently arranged with GISS that in this situation it will be given the opportunity to ascertain whether its advisory opinion has been correctly represented. In other cases the complainant will, in addition to the decision on the merits of the complaint, receive an invitation for an oral explanation of the decision by the service.

In the reporting year the Committee handled eight complaints, all regarding GISS. With regard to two of the eight complaints the Committee issued an advisory opinion to the minister of the Interior and Kingdom Relations, but the latter has not given a decision yet. Furthermore, the minister of the Interior and Kingdom Relations in this reporting year gave his decisions on two complaints regarding GISS which the Committee had handled in the preceding reporting year.

In all cases the minister concerned followed the advisory opinion of the Committee in the decision. A short description of these complaints follows below.

With regard to four complaints the Committee advised the minister of the Interior and Kingdom Relations to declare the complaint manifestly ill-founded. 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 in each case the complaint was manifestly ill-founded.

With regard to one complaint the Committee advised the minister to declare the complaint partly ill-founded and partly manifestly ill-founded. The complainant alleged that he had cooperated with GISS and that GISS had not paid the promised remunerations. The complainant further alleged that GISS was trying to take his life and had ensured that his benefit payments were discontinued and his dwelling vacated. The Committee came to the conclusion that the part of the complaint in which the complainant alleged that GISS was trying to take his life was manifestly ill-founded. With regard to the other parts of the complaint the Committee concluded on the basis of its investigation that they were ill-founded. There was no evidence of any unlawful or otherwise improper conduct on the part of GISS.

With regard to two complaints the Committee advised the Minister of the Interior and Kingdom Relations to declare the complaint ill-founded.
In the first case, also mentioned in annual report 2011-2012, the complaint was that an investigation conducted by GISS did not fall within its legal powers and that GISS had

wrongfully cooperated with a foreign service. Allegedly, the complainants had been injured thereby. The Committee held the opinion that GISS was authorized by law to conduct the investigation in question and established that there was no evidence of any cooperation with the foreign service mentioned by the complainants.
In the second case the complainants alleged that they were wrongfully kept under surveillance by GISS. The Committee's investigation did not yield evidence of any improper conduct of GISS. The complainants failed to make a plausible case that GISS was involved in the activities they had described.

With regard to one complaint the Committee advised the minister of the Interior and Kingdom Relations to declare the complaint partly well-founded and partly ill-founded.
In this case, also mentioned in the annual report 2011-2012, the complainants alleged that the provision of information regarding one of them to a foreign service had been unlawful and negligent. The Committee concluded that part of the information had been provided unlawfully. This part of the complaint was well-founded. The provision of another part of the information was not unlawful and not negligent. With regard to this part of the complaint the Committee concluded that it was ill-founded.

With regard to two complaints the Committee issued an advisory opinion to the minister of Interior and Kingdom Relations, but the minister has not given any decisions in those cases. The Committee's advisory opinion was to declare one complaint ill-founded and one complaint partly well-founded and partly ill-founded. The Committee will return to these complaints in the next annual report.

Advisory task

Pursuant to Article 64(2)(b) the Committee may advise the minister concerned on request or otherwise. On 1 October 2012 the ministry of the Interior and Kingdom Relations invited contributions to the consultations on the draft proposal to amend Article 13 of the Constitution, concerning the right to privacy of correspondence and telecommunications. The formulation of this right in the Constitution provides the framework for the use of special powers by GISS and DISS. The draft proposal was reason for the Committee to provide an advisory opinion to the minister.

Cooperation of GISS and DISS

In this reporting year, as in previous years, the Committee had the full cooperation of GISS and DISS.

When examining the files at DISS, however, the Committee still encounters some problems and delays. The Committee finds the digital documentation system of DISS hardly user-friendly. As a result the Committee still has to depend partly on the physical delivery of files by DISS. In the investigation of the cooperation of DISS with foreign services the files delivered were not always complete. This was subsequently remedied, at the instigation of the Committee.

Regular contacts

The Committee meets on a regular basis with the Second Chamber of Parliament, the ministers concerned, and the management of GISS and of DISS.

On 20 June 2012 the Committee participated in a round-table conference with the Parliamentary Standing Committee on Internal Affairs discussing the results of the round of talks started by professor Fijnaut on the occasion of the ISS Act 2002 decennial (more will be said about this in chapter 2 of the annual report). On 21 June the Committee discussed the state-secret aspects of its findings with the Parliamentary Committee on the Intelligence and Security Services (ISS Committee). In this reporting year the Committee did not meet with the Parliamentary Standing Committee on Defence.

On 8 May 2012 the Committee met with minister Spies of the Interior and Kingdom Relations and on 13 February 2013 it was introduced to the new minister of the Interior and Kingdom Relations, Plasterk. On 23 May 2012 the Committee met with minister of Defence Hillen and on 19 June 2012 with prime minister Rutte. On 10 October 2012 the Committee's chairman met with the secretary-general of the ministry of General Affairs to discuss the role of the coordinator of the intelligence and security services. The regular meeting of the Committee and the secretary-general of the ministry of General Affairs, the latter also in his capacity as coordinator of the intelligence and security services, took place on 11 December 2012.

Consultations with the management of GISS and the management of DISS took place twice in the reporting year. The topics discussed at these consultations included the reports that had been issued and ongoing investigations of the Committee, as well as important developments and events within the services. There have been occasional contacts about current matters between the management of the services and the Committee's chairman. There are satisfactory consultations between the Committee's staff and the employees of the services about progress of the Committee's work.

Furthermore, the Committee met with the president of the Court of Audit, Stuiveling, on 22 May 2012. The Court of Audit supervises GISS and DISS, in particular at the financial level. At this meeting attention was devoted to the working procedures and investigation agenda of the Court of Audit and the Committee.

On 28 November 2012 the Committee paid a working visit to the National Police Services Agency (*Korps Landelijke Politiediensten* or KLPD), now called the National Unit, at Driebergen. During the visit the Committee was informed of the activities and working procedure of the KLPD, in particular where these touch on the activities of GISS. On a subsequent visit on 6 March 2013 the activities of the Intelligence Service of the National Unit were discussed in greater detail. This service carries out activities for GISS pursuant to Article 60 ISS Act 2002.

Chapter 2

ISS Act 2002 decennial

On 29 May 2002 the Intelligence and Security Services Act (ISS Act 2002) came into force. The Committee found a good reason in the tenth decennial of this Act to ask professor Fijnaut to investigate the functioning of the intelligence and security services oversight system. To this end Fijnaut analyzed the oversight system and interviewed 26 persons who have gained experience with this oversight in the past ten years. Fijnaut laid down his findings in a report entitled *Het toezicht op de inlichtingen- en veiligheidsdiensten: de noodzaak van krachtiger samenspel* [The Oversight of the Intelligence and Security Services: the need for more effective concerted action].[3] On 18 April 2012 in the Old Chamber of Parliament the Committee organised a symposium at which the oversight of the intelligence and security services was the key element. Fijnaut presented his findings in the presence of many officials who are directly or indirectly involved with such oversight. There was a discussion, chaired by Mr Van Schendel, vice-president of the Supreme Court, with a forum consisting of messrs. Aalbersberg, chief constable Amsterdam-Amstelland, Bruning, general secretary of the *Nederlandse Vereniging van Journalisten* (Dutch association of journalists), Hoekstra, former member of the Council of State and former secretary-general of the ministry of General Affairs, and Nooitgedagt, lawyer practising Amsterdam. The audience was involved in a discussion as well.

The Committee looks back on a productive exchange of views. The insights ensuing from the round of talks conducted by Fijnaut merit careful study and critical examination. It is therefore satisfying that the government, urged by parliament, has decided to have the ISS Act 2002 evaluated. The ISS Act 2002 Evaluation Committee was appointed on 1 February 2013. This independent committee, chaired by C.W.M. Dessens, will address the following questions: (1) has the Act had the effects envisaged by the legislature (realisation of the Act's objectives); (2) has the Act in practice proved to be a workable instrument for the performance of the services' tasks; and (3) which problems and points of attention can be identified in the actual application of the Act.[4] At the request of parliament the Evaluation Committee will pay particular attention to the oversight system and the technical adequacy of the powers assigned to the services.

---

[3] The report is available (in Dutch) at www.ctivd.nl under Overige publicaties.

[4] Article 2 of the Order establishing the ISS Act 2002 Evaluation Committee, *Government Gazette* f2013, 4096 and *Parliamentary Papers II* 2011/12, 29 924, no. 91, p. 2.

After the Committee had issued review report no. 28 on the use of Sigint by DISS, the minister of Defence announced that he wished to amend the ISS Act 2002.[5] In the report the Committee established that actual practice at DISS was at odds with the provisions of the ISS Act 2002 in several areas. It was the intention of the minister to adjust the ISS Act 2002 to new technological developments. The proposed amendment to the ISS Act 2002 would also deal with some other issues, including the noncontroversial elements from an earlier proposal to amend the ISS Act 2002.[6] Although the legislative amendment has reached an advanced stage of administrative preparation, the minister has nevertheless decided, on the insistence of parliament, not to submit the proposed amendment until after the evaluation committee has presented its report, i.e. after September 2013.[7]

[5] *Parliamentary Papers II* 2011/12, 29 924, no. 86, p. 3.
[6] *Parliamentary Papers II* 2011/12. 29 924, no. 79, pp. 1-2.
[7] Article 6 of the Order establishing the ISS Act 2002 Evaluation Committee, *Government Gazette* 2013, 4096.

Chapter 3

(De)classification by GISS

Every year GISS and DISS create thousands of documents that are classified state secret. In this respect alone the services already cannot be compared to other public authorities, which have to work with state secrets on a much smaller scale. This leads to many questions in the outside world and sometimes even to incomprehension. Is it right that certain information is classified, i.e. designated as secret? Is GISS classifying too many documents and at a higher level than necessary? And when must state-secret information be destroyed or declassified and made public? At the request of parliament the Committee analyzed the rules on classification and declassification and examined to what extent GISS has been observing the rules.

The rules on the (de)classification of information are laid down in the Civil Service Information Security (Classified Information) Regulations (further referred to as: the "Classified Information Security Regulations"), which apply to GISS, too. The Committee has established that GISS has hardly, if at all, incorporated the general classification rules of the Classified Information Security Regulations in its internal rules. This omission must be remedied. In spite of the absence of such a detailed framework of rules the Committee has come to the conclusion that broadly speaking GISS handles classification correctly, even though there is certainly room for improvement. So there is definitely no evidence of a structural practice of classifying unnecessarily or at too high a level, as has been thought occasionally. However, when GISS provides information to external bodies, for example the Parliamentary Standing Committee on the Intelligence and Security Services, it would be a good thing if it would, as far as possible, indicate for each paragraph which information is state secret. This will make it clear to the recipient, too, which part of the information is subject to the classification.

Any classification of information must be reviewed or terminated after a certain time, in conformity with the Classified Information Security Regulations. The Committee's investigation has shown that GISS has failed to do so. This entails the risk that state-secret information continues to be state-secret for too long.

Articles 43 and 44 of the ISS Act 2002 further provide that after a certain time information of GISS must either be destroyed or transferred to the National Archives. For this purpose a selection list must be drawn up in which it is recorded which data should be destroyed and which are eligible for transfer. In preparing the selection list account must be taken

of the special nature of the activities of GISS, but apart from this the basic principle is that GISS, like other public bodies, cannot endlessly keep its archives in its own hands. The Committee has established that no selection list has been adopted yet and that consequently no information of GISS is being destroyed or transferred to the National Archives yet, either. It turns out that there has been a long-lasting discussion which has brought the entire process to a standstill. The ministry of the Interior and Kingdom Relations, the ministry of Defence, GISS and DISS take the position that the interest of source protection requires that the so-called informer and agent files must be destroyed and may never be considered for transfer. In view of their historical interest the Chief State Archivist and the minister of Education, Culture and Science hold that under certain circumstances it must be possible to transfer informer and agent files. Keeping these files is considered important to make it possible to research from which population groups GISS recruits sources, what was their motivation and for what purpose the sources were deployed. The Committee holds the opinion that there is no legal basis for a categorical refusal to transfer agent and informer files. Based on criteria to be drawn up by the National Archives these files could be assessed. The Committee thinks it likely that a solution can be found in the proposed possibility of transfer in a fully anonymized form. The Committee emphasizes that priority must in any case be given to establishing the selection list. If it is not possible to reach timely agreement on the issue of transferring informer and agent files, that could be arranged separately.

In her reaction to the review report the minister states that in principle she agrees with the conclusions and recommendations of the Committee. However, she first wishes to establish what are the consequences of implementing the recommendations, particularly in terms of finance and personnel. To this end a classification project has been started at GISS.

The Committee is aware that clearing the archives on the basis of destruction, declassification or transfer is a labour-intensive operation and will probably not be given top priority in times of austerity. With regard to future implementation, however, things are different, this calls for priority. Not only because work is piling up and the high storage costs are therefore increasing as well, but in particular because a gain in efficiency can be achieved in e.g. handling applications for inspection and related legal proceedings. If the archives are in order from today on, then legal proceedings can be prevented and a contribution be made to the greatest possible transparency at GISS.

Chapter 4

International contacts

Because of the highly specific nature of its activities, the Committee considers it important to maintain contacts with similar authorities abroad. The structure of the Dutch oversight system and the reports issued by the Committee are indeed attracting a lot of attention abroad. For this reason some of the Committee's review reports are translated into English.

In the reporting year the Committee's chairman made a contribution to a seminar in Ljubljana, Slovenia. The seminar was organised by the Swiss Democratic Control of Armed Forces institute (DCAF), for members of the Kosovar parliament and their staff.

At the end of May the Committee attended the International Intelligence Review Agencies Conference in Ottawa, organised by the Canadian Security Intelligence Review Committee and the Communications Security Establishment Commissioner. After the Conference the Committee visited Washington DC for meetings with, among others, members of the House Intelligence Committee and the House Homeland Security Committee. At the Central Intelligence Agency (CIA) in Langley the Committee met with the Inspector-General and with staff members of the Office of Congressional Affairs.

On 18 July 2012 the secretary and a review officer of the Committee gave presentations on the Dutch oversight system and the Dutch experiences with evaluations at a seminar on oversight evaluation organised by DCAF in Geneva.

On 20 September 2012 the South African Inspector-General of Intelligence, Faith Radebe, visited the Committee. During the visit the two oversight bodies exchanged working procedures and experiences.

On 5 December 2012 DCAF presented a toolkit for overseeing intelligence services in Ljubljana, Slovenia.[8] This toolkit aims at offering handles to countries in which the oversight of the intelligence services is still being developed. The toolkit was made with the help of funds from the Dutch ministry of Foreign Affairs. The Committee's chairman wrote the preface and chaired the meeting at which the toolkit was presented. The meeting was attended by representatives from countries in the Balkan area, and from countries in Northern Europe and from South Africa.

---

[8] See appendix I for a more detailed account of the Committee.

On 25 March 2013 the Committee welcomed the Estonian deputy secretary-general for domestic security policy, Erkki Koort. The Committee explained the Dutch oversight system to him as part of his familiarization with systems for overseeing intelligence and security services.

APPENDIX 1

The Committee (background)

Statutory tasks

The Review Committee on the Intelligence and Security Services commenced its duties on 1 July 2003. The Committee was established pursuant to the Intelligence and Security Services Act 2002 (hereinafter referred to as: the ISS Act 2002), which became effective on 29 May 2002.[9] Article 1 of the Act defines the term 'services' to comprise the General Intelligence and Security Service (GISS) and the Military Intelligence and Security Service (DISS), which fall under the political responsibility of the minister of the Interior and Kingdom Relations and the minister of Defence, respectively. In addition, the oversight task of the Committee covers the coordinator for the intelligence and security services, who is accountable to the prime minister acting in his capacity as minister of General Affairs (see Art. 4 of the ISS Act 2002).

The statutory task of the Committee also includes oversight of officers of the police force, the Royal Netherlands Military Constabulary and the Tax and Customs Administration, insofar as they perform activities on behalf of GISS (see Art. 60 of the ISS Act 2002).

Title 6 of the ISS Act 2002 (Articles 64-84) sets out the composition, task performance and powers as well as other matters pertaining to the Committee. In addition, it refers to other provisions of the Act that pertain to the Committee's tasks and powers, in particular Article 34(2) and Article 55(3).

By virtue of Article 64(2) of the ISS Act 2002 the Committee is charged with:
a. oversight of whether the provisions laid down in or pursuant to the ISS Act 2002 and the Security Screening Act[10] are implemented lawfully;
b. informing and advising the ministers concerned on the findings of the Committee both on request and otherwise;
c. advising the ministers concerned on the investigation and assessment of complaints;
d. advising the ministers concerned, on its own initiative, on the obligation to notify, which is embodied in Article 34 of the Act and which came into effect five years after the ISS Act 2002 came into effect – i.e. on and after 29 May 2007.

---

[9] See Bulletin of Acts and Decrees (*Stb.*) 2002, 148 (most recently amended by Act of 2 November 2006, *Stb.* 574).
[10] Bulletin of Acts and Decrees (*Stb.*) 1996, 525 (most recently amended by Act of 11 October 2007, *Stb.* 2007, 508).

Of the above tasks the one mentioned under a, that of the oversight of the lawfulness of the activities of the services, is in practice by far the most important task for the Committee. In the context of its lawfulness reviews the Committee closely scrutinizes matters like the exercise of special powers by the services. These are powers which infringe or may infringe human rights that are recognised by the Netherlands, in particular the right to protection of privacy, and which may therefore only be exercised subject to strict conditions.

For example: under the ISS Act 2002 (see Articles 20-30 of the Act) the services may only exercise special powers or use special intelligence means if this is necessary for the proper performance by the services of the tasks assigned to them (Article 18 of the Act). In addition, these special powers or intelligence means may only be exercised or used taking due account of the requirements of proportionality and subsidiarity (Articles 31 and 32 of the Act), that is to say that the exercise or use of the powers or intelligence means must be reasonably proportionate to the purpose for which they are exercised or used, while it is not possible to exercise powers or use intelligence means that are less drastic and less intrusive of an individual's privacy, for example the use of public sources. In each of its investigations the Committee carefully assesses whether (among other things) these three requirements have been met.

When investigating the lawfulness of the activities of the services the Committee sometimes comes across operational expediency issues. In the context of the task defined under b. (informing and advising the ministers about its findings) the Committee will inform the ministers concerned of these findings as well. This is in line with the position taken by the government when the bill was debated in parliament, and with the wish expressed by the ministers concerned to the Committee.

Article 80 of the ISS Act 2002 provides that before 1 May of each year the Committee must issue a (public) report on its activities. The report is submitted to both Chambers of the States General and to the ministers concerned: the prime minister acting in his capacity as minister of General Affairs, the minister of the Interior and Kingdom Relations, and the minister of Defence. In order to make the report as much up-to-date as possible, the Committee has provided in Article 10 of its Rules of Procedure that the reporting period runs from 1 April of the previous calendar year until 1 April of the current year.

In accordance with paragraphs (3) and (4) of Article 8 of the ISS Act 2002, which pursuant to Article 80 apply to the annual reports of the Committee as well, these public reports do not mention any data giving an insight into the means the services have used in concrete cases, or into secret sources or into the current level of information of the services, but the minister concerned may confidentially disclose such data to the States General. So far, all annual reports of the Committee, including the present one, have been fully public;

there are no secret appendices. The annual reports are also published on the website of the Committee: www.ctivd.nl

Members and employees of the Committee can only be appointed after they have successfully passed a category A security screening.

The Committee is entirely independent, also financially. It has its own budget, adopted by the same law by which the budgets of the ministry of General Affairs and of the Queen's Office are adopted.

Investigations

The Committee is free to choose the subjects of its investigations. Either Chamber of the States General may request the Committee to conduct a specific investigation (Art. 78(2) of the ISS Act 2002). In the past years the Second Chamber made several such requests to the Committee, through the minister of the Interior and Kingdom Relations. The Committee strives to comply with such requests, and to do so as soon as possible. The Committee attaches great importance to giving the best possible support to the review task of the two Chambers of the States General by means of its investigative activities and reports.

As soon as the Committee has decided to conduct a specific investigation (on its own initiative or at the request of one of the ministers concerned or one of the Chambers of the States General, as the case may be), it informs the ministers concerned and the presidents of the two Chambers of the decision.

In the course of an investigation the Committee examines files, hears individuals and studies the applicable legislation and regulations, both national and international.
The legislator has granted the Committee far-reaching powers for these purposes.

By virtue of Article 73 of the ISS Act 2002, for example, the Committee has direct access to all data processed in the context of the implementation of this Act and of the Security Screening Act. So it has access not only to data contained in documents issued or authorised by the management of the services, but also to any and all documents found present at one of the services which the Committee finds it necessary to inspect for the purposes of an investigation it is conducting and of related investigative subjects.

Furthermore, any person involved in the implementation of these two Acts, so first of all the employees of the services, are required, if so requested, to furnish such information and render such assistance to the Committee as it requires for the proper performance of its task. The only reservation made with respect to this twofold power is that if there

is reason to do so, the services may state which data may not be disclosed beyond the Committee in the interest of national security.

For the purposes of its review task the Committee may summon persons to appear before the Committee as witnesses. Witnesses so summoned are required by law to appear and to provide the Committee with all information the Committee considers necessary, obviously insofar as they have knowledge of such information. If a person refuses to comply with the summons to appear before the Committee, the Committee may issue a warrant to secure this person's presence. The Committee may also hear witnesses on oath or after they have made a solemn affirmation. These far-reaching powers are described in Articles 74 and 75 of the ISS Act 2002.

A review report contains the findings, conclusions and recommendations of the Committee in a specific investigation. These can be useful to the services and the ministers responsible for the services and to the Chambers of the States General in performing their respective tasks.

The Committee regularly consults with the prime minister acting in his capacity as minister of General Affairs, the minister of the Interior and Kingdom Relations, and the minister of Defence.
It also holds regular consultations with the three committees of the Second Chamber that are specifically concerned with the functioning of the intelligence and security services: the Committee on the Intelligence and Security Services, the Parliamentary Standing Committee on the Interior and Kingdom Relations and the Parliamentary Standing Committee on Defence. In addition, the Committee has consultative meetings with the Standing Committees of the First Chamber on the Interior and Kingdom Relations/General Affairs, Foreign Affairs, Defence and Development Cooperation, respectively.
At these consultative meetings there is an intensive exchange of views on the Committee's findings and recommendations as stated in its reports.
Naturally, the Committee has frequent contacts with the management and employees of the two services.

The parliamentary history of the ISS Act 2002 shows that the legislator took the position that it was not advisable to let the Committee send the review reports it has produced directly to the two Chambers of the States General, because the minister had to be able to assess publication of the information presented in the reports against state interests and the interests of national security. For this reason the reports are sent to the States General through the intermediary of the minister concerned, who then adds his or her comments on the report.

Because of this procedure the relevant minister is given two opportunities to respond to a report from the Committee before it reaches the States General. The first time is after the Committee has prepared its report. The minister then has the opportunity to respond to the report and the findings and recommendations it contains within a reasonable period set by the Committee. Subsequently, the Committee adopts the report, whether or not in amended form, and sends it to the Minister for the second time, who must then send it to both Chambers of the States General, together with his or her response, within a (statutory) period of six weeks.

Complaints handling

Any person who wishes to submit a complaint about conduct of the services[11] must first – before filing his complaint with the National Ombudsman – apply to the minister responsible for the service concerned. The Committee plays an advisory role in the minister's handling of such complaints. Before giving a decision whether or not the complaint is well-founded, so Article 83(3) of the ISS Act 2002 provides, the minister must obtain the advisory opinion of the Committee. In this way the Committee acts as a mandatory external advisory body. Division 9.1.3 of the General Administrative Law Act (further referred to as "GALA") is applicable with respect to the advisory role of the Committee. However, in derogation of Article 9:14(2) GALA, the minister concerned may not give the Committee any instructions. This provision has been included in connection with the independence of the Committee.

The involvement of the Committee as a complaints advisory committee means that the Committee takes over the entire investigation into the conduct challenged by the complaint and the procedures to be followed in connection with the complaint, including hearing the complainant and employees of the service involved. On the basis of the documents and its hearing of the complainant, the Committee itself determines the substance and scope of the complaint on which it will give an advisory opinion.

The fact that the Committee is called in as complaints advisory committee means that the Committee assumes full charge of the entire investigation of the conduct against which the complaint is directed and of the complaint handling procedures, including the hearing of the complainant and employees of the service concerned. The Committee itself determines the substance and scope of the complaint on which it is to issue an advisory opinion on the basis of the documents and its hearing of the complainant.

[11] Art. 83(1) of the ISS Act 2002 provides that complaints can be filed about conduct or alleged conduct of the ministers concerned (Interior and Kingdom Relations, Defence, and General Affairs), the heads of the services (GISS and DISS), the coordinator, and persons working for the services and the coordinator.

Immediately after receiving a complaint on which it is to give an advisory opinion, the Committee examines any files that are present at the intelligence and security service concerned. If, however, the complaint is manifestly ill-founded, the Committee may decide not to examine the files. Next, the Committee proceeds to hear the complainant unless it may decide not to do so because the complaint is manifestly ill-founded or the complainant has stated that he or she will not exercise the right to be heard (Article 9:15(3) GALA). As a rule the conduct of the hearing is not undertaken by the full Committee but entrusted by it to the chairman or a member of the Committee, in conformity with Article 9:15(2) GALA. In addition to the complainant, the person to whose conduct the complaint relates is given the opportunity to present his or her view regarding the complaint. The Committee may allow the parties to reply and rejoin.
The Committee may decide to hear witnesses if this is necessary to make a full investigation.

After examining the files and hearing the persons concerned, the Committee assesses whether the conduct of the challenged service towards the complainant meets the standards of proper conduct. For this task the Committee has a broader assessment framework than for its review task, since the latter is restricted to review as to lawfulness.[12] Subsequently, the Committee sends a report of its findings accompanied by an advisory opinion and recommendations, if any, to the minister concerned (Article 9:15 GALA). The minister may depart from the Committee's advisory opinion, but in that case the minister must state the reason for such departure in his or her reply to the complainant, and the Committee's advisory opinion must then also be sent to the complainant.
In formulating its advisory opinion the Committee must therefore bear in mind that the advisory opinion may be made public. Sometimes, this will inevitably result in the Committee using vague and abstract wordings in its advisory opinion.

Before asking the Committee to give an advisory opinion on the merits of a complaint, the minister will first give the service concerned the opportunity to dispose of the complaint informally. This is in keeping with the view taken by the legislator that unnecessary formal and bureaucratic procedures are to be avoided.[13] The Committee likewise holds the opinion that the services must first be given an opportunity to informally dispose of complaints themselves, unless there are indications that this will be in vain.

In its capacity as complaints advisory committee the Committee does not have an advisory task within the meaning of Article 83 of the ISS Act 2002 until the minister has received a formal complaint. However, the minister is not required to call in the Committee for

[12] Lawfulness does, however, form part of the standards of proper conduct applied as a criterion in handling complaints. *Parliamentary papers II* 1997-1998, 25 837, B, p. 6.
[13] *Parliamentary papers II* 1997/98, 25 837, no. 3, p. 7.

all formal complaints. The minister is not required to obtain the advisory opinion of the Committee if a complaint is inadmissible pursuant to Article 9:4 GALA or if it is not taken up pursuant to the provisions of Article 9:8 GALA. The requirement to call in the Committee only applies if the assessment whether a complaint is well-founded calls for a substantive assessment. In other words: the minister is not required to obtain the advisory opinion of the Committee if he refrains from giving a decision on the conduct. Manifestly ill-founded complaints, on the contrary, are not excluded from the minister's obligation to consider all complaints.[14] In principle the Committee must give an advisory opinion on such complaints. In these cases, however (and also if the complainant has stated that he does not wish to exercise the right to be heard), Article 9:10 GALA releases the Committee from the obligation to hear the complainant.[15]

[14] Contrary to the National Ombudsman (see. Art. 9:23, first sentence and under b, GALA), the rules of the General Administrative Law Act apparently require the minister to consider manifestly ill-founded complaints.

[15] *Parliamentary papers II* 1997/98, 25 837, B, p. 4.

APPENDIX 2

List of review reports

Review report on the investigation by DISS into incidents that may harm Defence (*Toezichtsrapport inzake het onderzoek van de MIVD naar voorvallen die Defensie kunnen schaden*) (CTIVD no. 1, 2004)

Review report on the investigation by GISS into radicalisation processes within the Islamic community (*Toezichtsrapport inzake het AIVD-onderzoek naar radicaliseringsprocessen binnen de islamitische gemeenschap*) (CTIVD no. 2, 2004)

Review report on a counter-terrorism operation by DISS (*Toezichtsrapport inzake een contra-terrorisme operatie door de MIVD*) (CTIVD no. 3, 2004)

Review report on the investigation by GISS into developments within the Moluccan community in the Netherlands (*Toezichtsrapport inzake het AIVD-onderzoek naar de ontwikkelingen binnen de Molukse gemeenschap in Nederland*) (CTIVD no. 4, 2005)

Review report on the investigation by DISS into the proliferation of weapons of mass destruction and their means of delivery* (*Toezichtsrapport inzake het MIVD-onderzoek naar proliferatie van massavernietigingswapens en overbrengingsmiddelen*) (CTIVD no. 5a, 2005)

Review report on the investigation by GISS into the proliferation of weapons of mass destruction and their means of delivery* (*Toezichtsrapport inzake het AIVD-onderzoek naar proliferatie van massavernietigingswapens en overbrengingsmiddelen*) (CTIVD no. 5b, 2005)

Review report on the investigation by GISS into radical animal rights activism and left-wing extremism* (*Toezichtsrapport inzake het AIVD-onderzoek naar radicaal dierenrechtenactivisme en links-extremisme*) (CTIVD no. 6, 2006)

Review report on the performance of a counter-terrorism operation by GISS (*Toezichtsrapport inzake de uitvoering van een contra-terrorisme operatie van de AIVD*) (CTIVD no. 7, 2006)

Review report on the deployment by DISS of informers and agents, more in particular abroad* (*Toezichtsrapport inzake de inzet door de MIVD van informanten en agenten,*

meer in het bijzonder in het buitenland) (CTIVD no. 8a, 2006)

Review report on the deployment by GISS of informers and agents, more in particular abroad* (*Toezichtsrapport inzake de inzet door de AIVD van informanten en agenten, meer in het bijzonder in het buitenland*) (CTIVD no. 8b, 2006)

Review report on the official messages issued by GISS in the period January 2004 - October 2005* (*Toezichtsrapport inzake de door de AIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot oktober 2005*) (CTIVD no. 9a, 2006)

Review report on the official messages issued by DISS in the period from January 2004 - January 2006* (*Toezichtsrapport inzake de door de MIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot januari 2006*) (CTIVD no. 9b, 2006)

Review report on the investigation by GISS into the leaking of state secrets* (*Toezichtsrapport inzake het onderzoek van de AIVD naar het uitlekken van staatsgeheimen*) (CTIVD no. 10, 2006)

Review report on the implementation of the Security Screening Act by DISS (Toezichtsrapport inzake de uitvoering van de Wet veiligheidsonderzoeken door de MIVD) (CTIVD no. 11a, 2007)

Review report on the implementation of the Security Screening Act by GISS (*Toezichtsrapport inzake de uitvoering van de Wet veiligheidsonderzoeken door de AIVD*) (CTIVD no. 11b, 2007)

Review report on the Counter-Terrorism Infobox (*Toezichtsrapport inzake de Contra Terrorisme Infobox*) (CTIVD no. 12, 2007)

Review report on the exchange of information between GISS and the Immigration and Naturalisation Service (*Toezichtsrapport inzake de uitwisseling van gegevens tussen de AIVD en de IND*) (CTIVD no. 13, 2007)

Review report on the investigation by GISS into unwanted interference by foreign powers (including espionage) (*Toezichtsrapport inzake het onderzoek van de AIVD naar de ongewenste inmenging van vreemde mogendheden (waaronder spionage)*) (CTIVD no. 14, 2007)

Review report on the conduct of employees of DISS in Iraq when questioning detainees (*Toezichtsrapport inzake het optreden van MIVD-medewerkers in Irak bij het ondervragen van gedetineerden*) (CTIVD no. 15, 2007)

Review report on the cooperation between GISS and the Regional Intelligence Services and the Royal Netherlands Military Constabulary, respectively (*Toezichtsrapport inzake de samenwerking tussen de AIVD en de Regionale Inlichtingendiensten resp. de Koninklijke marechaussee*) (CTIVD no. 16, 2008)

Review report on the assessment processes at GISS with respect to Mohammed B. (*Toezichtsrapport inzake de afwegingsprocessen van de AIVD met betrekking tot Mohammed B.*) (CTIVD no. 17, 2008)

Review report on the fulfilment by GISS of the commitments made by the minister of the Interior and Kingdom Relations in response to the recommendations of the Committee (*Toezichtsrapport inzake de nakoming door de AIVD van de toezeggingen van de Minister van BZK op de aanbevelingen van de Commissie*) (CTIVD no. 18A, 2008)

Review report on the fulfilment by DISS of the commitments made by the minister of Defence in response to the recommendations of the Committee (*Toezichtsrapport inzake de nakoming door de MIVD van de toezeggingen van de Minister van Defensie op de aanbevelingen van de Commissie*) (CTIVD no. 18B, 2008)

Review report on the application by GISS of Article 25 of the ISS Act 2002 (wiretapping) and Article 27 of the ISS Act 2002 (selection of non-directional interceptions of non cable-bound telecommunications* (*Toezichtsrapport inzake de toepassing door de AIVD van art. 25 ISS Act 2002 (aftappen) en art. 27 ISS Act 2002 (selectie van ongericht ontvangen niet-kabelgebonden telecommunicatie)*) (CTIVD no. 19, 2009)

Review report on financial and economic investigations by GISS (*Toezichtsrapport inzake financieel-economische onderzoeken door de AIVD*) (CTIVD no. 20, 2009)

Review report on the security screening by GISS of the (former) chief of the Zeeland Police Force Mr F.P. Goudswaard (*Toezichtsrapport inzake het veiligheidsonderzoek van de AIVD naar de (voormalige) korpschef van de Politie Zeeland dhr. F.P. Goudswaard*) (CTIVD no. 21, 2009)

Review report on the cooperation of GISS with foreign intelligence and/or security services* (*Toezichtsrapport inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten*) (CTIVD no. 22A, 2009)

Review report on the conduct of DISS with respect to a former agent (*Toezichtsrapport inzake het handelen van de MIVD jegens een voormalige agent*) (CTIVD no. 23, 2010)

Review report on the performance by GISS of the obligation to notify* (*Toezichtsrapport*

inzake de uitvoering van de notificatieplicht door de AIVD) CTIVD no. 24, 2010)

Review report on the conduct of DISS with respect to two suspended employees (*Toezichtsrapport inzake het handelen van de MIVD jegens twee geschorste medewerkers*) (CTIVD no. 25, 2010)

Review report on the performance by GISS of the foreign intelligence task* (*Toezichts¬rapport inzake de uitvoering van de inlichtingentaak buitenland door de AIVD*) (CTIVD no. 26, 2011)

Review report on the roles of DISS and GISS in an evacuation mission in Libya (*Toezichtsrapport inzake de rol van de MIVD en de AIVD bij een evacuatiemissie in Libië*) (CTIVD no. 27, 2011)

Review report on the use of Sigint by DISS* (*Toezichtsrapport inzake de inzet van Sigint door de MIVD*) (CTIVD no. 28, 2011)

Review report on the official messages issued by GISS in the period October 2005 – May 2010* (*Toezichtsrapport inzake de door de AIVD uitgebrachte ambtsberichten in de periode van oktober 2005 tot en met mei 2010*) (CTIVD no. 29, 2011)

Review report on previous recommendations by the Committee concerning DISS (*Toezichtsrapport inzake eerdere aanbevelingen van de Commissie betreffende de MIVD*) (CTIVD no. 30a, 2012)

Review report on previous recommendations by the Committee concerning GISS (*Toezichtsrapport inzake eerdere aanbevelingen van de Commissie betreffende de AIVD*), (CTIVD no. 30b, 2012)

Review report on the use by GISS of the power to tap/intercept and the power to select Sigint* (*Toezichtsrapport inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*) (CTIVD no. 31, 2012)

Review report of the CTIVD on the official messages issued by DISS in the period January 2006 – June 2011 (CTIVD no. 32, 2012)

Review report of the CTIVD on the classification of state secrets by GISS* (*Toezichtsrapport van de CTIVD inzake de rubricering van staatsgeheimen door de AIVD*) (CTIVD no. 33, 2012)

* Available in English

APPENDICES III – VI

Review reports issued in the reporting year

APPENDIX III Review report on previous recommendations by the Committee concerning GISS (*Toezichtsrapport inzake eerdere aanbevelingen van de Commissie betreffende de AIVD*), (CTIVD no. 30b, 2012)

APPENDIX IV Review report on the use by GISS of the power to tap/intercept and the power to select Sigint* (*Toezichtsrapport inzake de inzet van de afluisterbevoegdheid en van de bevoegdheid tot de selectie van Sigint door de AIVD*) (CTIVD no. 31, 2012)

APPENDIX V Review report of the CTIVD on the official messages issued by DISS in the period January 2006 – June 2011 (CTIVD no. 32, 2012)

APPENDIX VI Review report of the CTIVD on the classification of state secrets by GISS* (*Toezichtsrapport van de CTIVD inzake de rubricering van staatsgeheimen door de AIVD*) (CTIVD no. 33, 2012)

* Available in English

Review Report CTIVD no. 31

On the use by GISS of the power to tap/intercept and the power to select Sigint

Table of contents

Summary 37

1. Introduction 39

2. The Committee's investigation 39

3. General picture 4 42
   - 3.1 Article 25 ISS Act 2002 43
   - 3.2 Article 27 ISS Act 2002 43

4. Substantiation of the reasons for applying article 25 ISS Act 2002 45

5. Investigation of radicalisation trends 47

6. The power to tap or intercept and third parties 49

7. Consultation with DISS 50

8. Conclusions and recommendations 51

Review Report CTIVD no. 31

On the use by GISS of the power to tap/intercept and the power to select Sigint

SUMMARY

The Committee's investigation was directed at the lawfulness of the use by GISS of the power to tap/intercept and the power to select Sigint in the period from September 2010 until the end of August 2011. These powers are embodied in articles 25 and 27 of the ISS Act 2002 and may only be used if it is necessary to do so for the performance of the security task or the foreign intelligence task of GISS. The law prescribes, moreover, that the use of these powers must be proportional and the least onerous of the measures available and must meet the requirements of due care laid down in the ISS Act 2002.

The Committee has established that GISS takes well-considered decisions when using the power to tap/intercept. It has not found any unlawful conduct in the operations it investigated. This deserves a compliment given the large number of operations investigated by the Committee. On some points, however, the Committee has established a lack of due care, in particular as regards the substantiation of the reasons for operations.

GISS can only adequately substantiate the reasons for an operation if it takes account of all the available relevant information. Only then can it assess with due care whether the privacy infringement entailed by the use of the power to tap/intercept is in fact necessary and proportional and satisfies the requirement of subsidiarity. In one case the Committee established that contraindications concerning the threat emanating from a target had not been included in the reasoning. The Committee also draws attention to the fact that for the sake of efficiency in its intelligence work GISS occasionally uses parallel sets of reasons with different secrecy classifications. It is the opinion of the Committee that this is at odds with the importance of careful and unambiguous substantiation of reasons.

The Committee has established that when GISS investigates radicalisation trends, it is not always clear that the persons or organisations with respect to which the power to tap or intercept is used actually give cause for serious suspicion that they pose a threat to national security. The Committee recognizes the importance of investigating such trends, but emphasizes that in doing so GISS must continuously evaluate the use of special powers with respect to these persons or organisations. In one case the Committee established that GISS used special powers for several years without obtaining clarity about the threat emanating from the persons involved. It is the opinion of the Committee that particularly in the final period of this investigation the use of the power to tap or intercept approached

the borderline of what is permitted by law. In one case GISS used special powers with respect to a person who wished to publish a certain message of which, so GISS believed, it could not be excluded that it might be taken as an incitement to activism or violence. The Committee considers this wording too broad, since the use of a special power must be based on a serious suspicion of threat.

In one case the Committee has established that GISS used the power to tap while there were important reasons to consult with DISS prior to using the power. If GISS had done so it might not only have been able to obtain operationally relevant information but could also have prevented that the two services worked on the same operational matters independently of each other.

The Committee refrains from giving an opinion on the lawfulness of the selection of Sigint by GISS, just as it did in two earlier reports in which the subject came up for consideration. When using this power GISS often does not explain to whom the numbers and technical characteristics belong and why these telecommunications should be selected. These problems appear to be inherent to selection of Sigint, the Committee recently also established this fact in regard to DISS. The substantiation requirements of the ISS Act 2002 are stringent, however, since the selection of Sigint entails examination of the content of communications of persons and organisations. In review report no. 28 on the use of Sigint by DISS, which was published at the end of 2011, the Committee set out the legal framework for the entire process of Sigint handling and presented starting points for improving the substantiation of the reasons for the use of special powers. In the next in-depth investigation of the use by GISS of the power to tap/intercept and the power to select Sigint the Committee will therefore investigate to what extent GISS has improved the substantiation of the reasons underlying the selection of Sigint.

Review Report CTIVD no. 31

On the use by GISS of the power to tap/intercept and the power to select Sigint

1. Introduction

Article 25 of the ISS Act 2002 confers power on GISS to tap/intercept communications. Article 27 ISS Act 2002 confers power to select non-directional interceptions of non cable-bound telecommunications (Sigint). Pursuant to its review task under article 64 of the Intelligence and Security Services Act 2002 (further referred to as: ISS Act 2002), the Review Committee for the Intelligence and Security Services (further referred to as: the Committee) investigated the use of these two special powers by the General Intelligence and Security Service (GISS). On 8 September 2010 the Committee, pursuant to article 78(3), ISS Act 2002, informed the minister of the Interior and Kingdom Relations and the presidents of the two Chambers of the Dutch parliament of the intended investigation.

On 15 February 2012 the Committee completed the investigation by drafting its report. In conformity with article 79 ISS Act 2002 the minister of the Interior and Kingdom Relations was given the opportunity to react to the findings laid down in the review report. On 27 March 2012 the Committee received the minister's reaction. This led to a few minor changes, after which the review report was adopted on 11 April 2012.

This report has a secret appendix.

2. The Committee's investigation

In February 2009, the Committee reported to the Second Chamber of Parliament for the first time on its investigation of the application by GISS of articles 25 and 27 ISS Act 2002 (review report 19).[1] After the publication of this report the Committee continued monitoring the exercise of these powers on a quarterly basis. Monitoring serves as a means to keep a finger on the pulse and in principle does not result in a report to the Second Chamber. In September 2010 the Committee decided to convert the monitoring into an annual in-depth investigation. The reason for this decision was that by announcing an

[1] CTIVD review report no. 19 on the application by GISS of article 25 of the ISS Act 2002 (tapping) and article 27 of the ISS Act 2002 (selection of non-directional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), available at www.ctivd.nl.

investigation and reporting on its findings the Committee would be able to give the Second Chamber a better understanding of the Committee's activities and findings regarding this important part of the work of GISS. The Committee will report on this subject on an annual basis. The present report is based on the investigation of the lawfulness of the application by GISS of articles 25 and 27 ISS Act 2002 in the period from September 2010 until the end of August 2011.

Every quarter, applications for permission to apply articles 25 and 27 are bundled and submitted to the minister of the Interior and Kingdom Relations.[2] Urgent new operations requiring a speedy start are submitted to the minister on an ad-hoc basis. The Committee carried out its investigation on a three-monthly basis shortly after the requested permission had been granted by the minister. It did so by examining the bundle of applications submitted to the minister[3], as well as the urgent ad hoc applications submitted separately. In the bundle of applications every operation is mentioned, including the name and the communications data of the person or organisation with respect to whom or which the special power is to be used and it gives a brief explanation of the reason for the request to use the power (article 25(4) and article 27(4) ISS Act 2002). The quarterly examination of the bundle of applications enabled the Committee to obtain an overview of all means used pursuant to articles 25 and 27, ISS Act 2002, in the review period. These bundles of applications do not, however, give exhaustive reasons substantiating the necessity, proportionality and subsidiarity of using the special power in question.

For each operation a separate document has been prepared within the GISS organisation before the application for permission is submitted to the minister, which contains the full reasons for applying for permission to use or continue to use articles 25 and 27 ISS Act 2002, or for terminating their use. This document, which is addressed to the head of GISS, also contains an explanation of the operational context, a presentation of recent findings and, in the case of continuation or termination, the results obtained by the use of the special power in the preceding period. Based on this documents managers either agree or refuse to agree to the use of the special power, and in-house lawyers of GISS give their opinion (see section 4 for further details).

In view of the great number of operations it was impossible for the Committee to examine all these documents. When examining the applications the Committee gave special attention to operations that stood out, either because of anomalies or a lack of clarity in the explanation, or because the operation focused on special categories of persons (non-

[2] An exception is the selection of key words relating to a specified subject, which are established annually. See article 27(3)(c) in conjunction with paragraph (5) ISS Act 2002.

[3] These bundled applications for permission are also known as "three-monthly collective decisions"

targets[4], third parties, professionals entitled to privilege, minors etc.). In the case of these operations the Committee examined the underlying documents, including the application for permission with the comprehensive substantiation of reasons and the detailed records of the intercepted conversations. These documents are stored in the internal digital system of GISS, to which the Committee has unrestricted access.

In addition, the Committee devoted attention to operations classified top secret or otherwise accessible to a smaller circle of persons than usual. These operations are not stored in the internal digital system of GISS and constitute highly sensitive material. To make its investigation as comprehensive as possible the Committee requested GISS to provide the documents concerning these operations separately. In the course of the review period the Committee established that the proportional number of operations classified top secret or otherwise subject to restricted access was much higher than the number received from GISS. Upon the Committee's request GISS subsequently provided the documents on the operations identified by the Committee after all. The explanation given by GISS for the initially incomplete information provision was that with a view to the *need to know* principle the service did not keep a central list of operations that were classified top secret.[5] Indeed, GISS could not guarantee that it had now delivered all operations in the review period that were classified top secret or otherwise made accessible to a smaller circle of persons than usual to the Committee. The argument given by GISS does not justify the absence of a list of these operations in which special powers had been used. It is the opinion of the Committee that keeping proper records is not at odds with the need to know principle. In addition, the absence of proper records had the result that GISS failed to fully inform the Committee. At the Committee's request the GISS unit responsible for supervising operations was then charged with the task of henceforth maintaining the list in question. Since then, the Committee has not established any further cases of incomplete information.

In addition to investigating the files, the Committee held quarterly interviews with the head of the GISS unit responsible for supervising operations. At these interviews the Committee was given an explanation of the weighting and prioritization of investigations and resources by GISS and how all this affected the application of articles 25 and 27 ISS Act 2002. The Committee also spoke about individual operations and investigations with a number of functionaries at GISS, and it submitted a number of questions in writing.

---

[4] *Non-targets* are persons in the environment of a target, but not themselves targets of GISS. In certain circumstances it is possible to use special powers in respect of non-targets.

[5] The *need to know* principle means that data are only made available internally to the extent necessary for the proper performance of the tasks assigned to the functionary in question (article 35 ISS Act 2002).

The Committee's investigation focused on the lawfulness of tapping/interception and of the selection of Sigint by GISS and for this purpose the Committee reviewed all the operations it investigated against the current legal framework. In doing so the Committee also kept in mind its findings and recommendations on the subject set out in its previous review report. In its investigation the Committee did not engage in an assessment of political and professional choices regarding the designation of the areas of attention of GISS. It did, however, inform itself about the operational decisions taken by GISS and their effect on the application of articles 25 and 27, among other things by means of the aforementioned interviews with the head of the GISS unit responsible for supervising operations.

In the present report, the Committee has chosen to build on its review report 19, in which it investigated the same subject with respect to an earlier period. As regards the general legal framework and the internal procedures of GISS this means that it is sufficient for the Committee to refer to the detailed descriptions in review report 19. The present review report does not devote attention to how GISS has implemented the recommendations of review report 19, since this is already done in the report on the performance of the commitments made by the minister of the Interior and Kingdom Relations in reaction to the Committee's recommendations, which report will be published in the near future. But the present report does set out the general developments observed by the Committee in the review period (section 3). In this context it will in particular discuss the situations encountered in this period where questions arose regarding the observance of the legal framework in connection with the application of articles 25 and 27 ISS Act 2002. Section 4 discusses some cases in which GISS failed to state adequate reasons for tapping. Section 5 discusses some aspects of the use of taps/interception in the investigation of radicalisation trends. Section 6 deals with the use of the power to tap/intercept in respect of third parties. In section 7 the Committee considers a case in which GISS did not consult with DISS while this would in fact have been advisable. Section 8 contains the conclusions and recommendations of the Committee.

3. General picture

In every quarter of the review period the Committee perceived shifts in the application of articles 25 and 27 ISS Act 2002. Operations were terminated and started and there were frequent changes of focus both within investigations and between investigations. The Committee has established that a change in operational prioritization soon affects the application of articles 25 and 27 ISS Act 2002. Generally, their application corresponds with the areas of attention identified by GISS.

3.1 Article 25 ISS Act 2002

During its investigation the Committee kept track of the number of persons and organisations in respect of which article 25 ISS Act 2002 was applied. Often, several taps are running with respect to one person or organisation.[6] The number of persons or organisations with respect to whom or which article 25 ISS Act 2002 was applied in the period from September 2010 until the end of August 2011 increased by approximately 30%. The increase was caused mainly by a growing number of operations for the purposes of performing the foreign intelligence task. The Committee has also noted an increase in the number of operations classified top secret or otherwise subject to restricted access. This point is discussed in greater detail in the secret appendix.

The Committee has established, as it did in the preceding review report on the subject, that GISS takes well-considered decisions when applying article 25 ISS Act 2002. The Committee has not found any unlawful procedures in the operations it investigated. This deserves a compliment given the large number of operations.

On some points, however, the Committee has established a lack of due care, in particular in the matter of substantiating the reasons for operations. It will discuss this in greater detail in sections 4 and 6. As regards the aforementioned special categories of persons to which the Committee devoted special attention, only the application of article 25 ISS Act 2002 to locations or connections belonging to third parties requires further consideration in section 6. In the secret appendix the Committee gives a more detailed discussion of several instances of lack of due care established by the Committee in the substantiation of the reasons for applying article 25 ISS Act 2002 with respect to one special category of persons.

3.2 Article 27 ISS Act 2002

In the course of the period from September 2010 until the end of August 2011 the number of operations in which article 27 ISS Act 2002 was applied increased strongly. This can be explained among other things by the increasing technical possibilities and increasing familiarity with this special means of intelligence. The increase is noticeable in all investigation areas in which the service makes use of article 27 ISS Act 2002.

---

[6] This means that the figures noted down by the Committee differ from the tapping statistics provided by the minister of the Interior and Kingdom Relations to the Second Chamber in 2010, see *Parliamentary Papers II* 2009/10, 30 517, no. 21.

Use of the power of selection on the basis of non-directional interceptions of non cable-bound telecommunications (further referred to as: selection of Sigint) is subject to the same legal rules as the use of taps or microphones since both procedures involve the targeted examination of the content of the communications of persons and organisations.[7] In review report 19 the Committee established that GISS did not handle the selection of Sigint with due care. Frequently, it did not state to whom the numbers and technical characteristics belonged and why these telecommunications should be subjected to selection. As a result the Committee came to the conclusion that it had insufficient knowledge of the reasons underlying the selection, so that it was unable to assess the lawfulness of the exercise of the power of selection pursuant to Article 27(3)(a) and (b), ISS Act 2002. The Committee urgently recommended that GISS specifically substantiate the reasons for the selection criteria in the applications for permission to start or to continue using these special powers.[8] In her reaction to this report the minister of the Interior and Kingdom Relations stated that she agreed with the Committee, but that she was at the same time concerned about the practical feasibility of the recommendation. The minister promised that GISS would consult with the Committee on the matter.[9] In review report 26 on the performance by GISS of the foreign intelligence task the Committee established that when GISS applied article 27 ISS Act 2002 in performing this task, applications often did not specify to whom a characteristic belonged and why it was important to possess the information to be obtained through this specific characteristic. It became clear to the Committee, however, that as Sigint operations continued longer, GISS was better able to state to whom the characteristics belonged and to substantiate why the use of the means in respect of these persons was justified. The Committee emphasized that GISS should seriously seek to specify the person or organisation targeted with Sigint as soon as possible.[10] In review report 28 on the use of Sigint by DISS the Committee subsequently elaborated the legal framework for the entire process of Sigint handling. In that review report, too, the Committee was compelled to come to the conclusion, this time with regard to DISS, that it could not express an opinion on the lawfulness of the application of article 27 because it had insufficient knowledge of the reasons for applying the special power.[11]

---

[7] *Parliamentary Papers II* 1997/98, 25 877, no. 3, pp. 44-45.

[8] CTIVD review report no. 19 on the application by GISS of Article 25 of the ISS Act 2002 (tapping) and Article 27 of the ISS Act 2002 (selection of non-directional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix) §7, available at www.ctivd.nl.

[9] *Parliamentary Papers II* 2008/09, 29 924, no. 29, pp. 5 and 6.

[10] 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, available at www.ctivd.nl.

[11] CTIVD review report no. 28 on the use of Sigint by DISS, *Parliamentary Papers II* 2011/12, 29 924, no. 74 (appendix), §8.3.4, available at www.ctivd.nl.

In the present investigation the Committee examined the Sigint operations and has arrived at the same findings as in review reports 19 and 26. Once again, therefore, it refrains from expressing an opinion on the lawfulness of the selection of Sigint by GISS.

In the next in-depth investigation of the use by GISS of the powers to tap/intercept and to select Sigint the Committee will examine to what extent the substantiation of the reasons for selection of Sigint has improved. The Committee takes the position that with the legal framework and the starting points provided by the Committee, in particular in review reports 19 and 28, GISS should be able to adequately substantiate the reasons for using this power. The Committee understands that an amendment of the ISS Act 2002 is being prepared which will among other things include an adjustment of the provisions on the use of Sigint. The Committee is awaiting the proposed amendment with interest. However, these developments do not change the fact that GISS must satisfy the requirements set by the current ISS Act 2002 for the selection of Sigint.

4. Substantiation of the reasons for applying article 25 ISS Act 2002

When a team of GISS wishes to use a tap or microphone pursuant to article 25 ISS Act 2002, it prepares a detailed substantiation of the reasons for such use. In this substantiation it demonstrates the necessity, proportionality and subsidiarity justifying the use of this special power, as required by articles 18, 31 and 32, ISS Act 2002.[12] The (legal) tenability of these reasons is assessed within GISS by, successively, the team leader, a legal expert of the unit responsible for supervising operations, the head of the operational unit concerned and the head of GISS.

The number of taps and microphones for which the minister must grant permission is great. The minister of the Interior and Kingdom Relations has no departmental support staff for assessing the use and the applicable legal assessment framework. The bundle of applications which the minister receives every three months includes a summary of the more detailed internal substantiation of reasons. This summary deals only briefly with the necessity, proportionality and subsidiarity of using the special powers. This underlines the importance of the internal assessment procedure at GISS since in this procedure the relevant factors are indeed explained and explicitly assessed against the legal review

[12] See for a description of these assessment criteria for the use of special powers CTIVD review report no. 19 on the application by GISS of article 25 ISS ACT 2002 (tapping/interception) and article 27 ISS ACT 2002 (selection of non-directional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §4, available at www.ctivd.nl.

framework. As stated above in section 3.1, the internal substantiation of reasons shows that GISS takes well-considered decisions with regard to using the power to tap or intercept. This thorough internal recording of the reasons stated for the application of article 25 ISS Act 2002 is essential for the Committee's review work.

It is the opinion of the Committee that it is only possible to assess necessity, proportionality and subsidiarity if all the available relevant information is used in making the assessment. This includes operational findings as well as the relative seriousness of the measure compared to other intelligence means and the processing possibilities of the team concerned. For example, if due to a shortage of audio processers a tap cannot be listened to, the tap cannot contribute to achieving the purpose for which GISS used the power to tap and the tap cannot be deemed necessary. And if operational data show that the threat emanating from the target has diminished, then continuing tapping may no longer be proportional. In the internal substantiation of reasons such relevant information is usually mentioned and taken into account. The Committee came across one case in which contraindications regarding the threat emanating from a target were not included in the substantiation of the reasons for continuing a tap. This was the second investigation discussed in section 5. GISS had, however, provided these contraindications to the authorities concerned and they were evidently considered reliable. The Committee therefore holds the opinion that the substantiation of the reasons for this tap was incomplete and consequently lacked due care. In the opinion of the Committee adequate reasons could have been stated. It was therefore a procedural shortcoming without involving any unlawful application of article 25 ISS Act 2002 in the substantive sense.

In the course of its investigation the Committee came across a procedure according to which GISS prepares two parallel sets of reasons for the application of article 25 ISS Act 2002 in one operation. One set of reasons is classified top secret and accessible only to the minister and the staff members bearing direct responsibility. There is also another set of reasons, classified secret, which is accessible to a broader group within the service. This procedure is more efficient for GISS than classifying the entire operation top secret since working with secret documents is easier than working with top secret documents (see section 2). This procedure has the consequence, however, that the secret set of reasons is incomplete and therefore inherently faulty. In addition, this procedure promotes a lack of due care and makes the Committee's review work more difficult. For example, GISS itself has stated that it cannot retrieve in which cases in the review period this procedure was followed. In one operation, moreover, the Committee was unable to establish whether the staff members involved in the internal assessment procedure were aware of the fact that there was also a top-secret set of reasons. In the secret appendix to this report the Committee will discuss this course of events in greater detail. In reaction to the report prepared by the Committee the minister announced that GISS would henceforth introduce safeguards to prevent carelessness, including the safeguard of actively informing

the Committee whenever this procedure is applied. The Committee holds the opinion, however, that this use of two parallel sets of reasons is still at odds with the interest of careful and unambiguous substantiation of reasons. The Committee therefore recommends changing the internal procedures and not applying the procedure in question, except in cases in which it can be demonstrated that its application is necessary.

5. Investigation of radicalisation trends

GISS may only use special powers for the purposes of performing the security task and the foreign intelligence task (article 6(2)(a) and (d) in conjunction with article 18, ISS Act 2002). For the purposes of the security task GISS may conduct an investigation if persons or organisations, because of the objectives they pursue or through their activities, give cause for serious suspicion that they pose a threat, briefly stated, to national security (article 6(2)(a) ISS Act 2002).[13] These persons are also known as targets. An important part of the investigations conducted by GISS on the basis of the security task consists of investigating radicalisation trends. In this type of investigation the threat emanating from persons and organisations is often not yet clear or concrete. GISS is not only expected, however, to identify concrete terrorist threats but also to keep track of radicalisation trends. The wide approach to terrorism that has been chosen is also directed at forms of radicalisation which, though not leading directly to terrorist violence, may nevertheless have a disrupting effect on society.[14] The Committee recognizes the importance of the radicalisation investigations of GISS. The Committee considers it its task to critically assess, when GISS has used special powers for the purposes of investigating radicalisation issues, whether the statutory criterion of serious suspicion of threat to national security is satisfied. When investigating the radicalisation investigations of GISS in the review period the Committee came across a number of operations where it was not immediately evident that the person against whom or the organisation against which the special powers were

---

[13] The foreign intelligence task is formulated more broadly. GISS may investigate persons and organisations if it is necessary to do so for the purposes of investigations concerning other countries pursuant to the Designation Order of the prime minister. No serious suspicion of a threat to national security is required, a national security interest suffices. In reports 19 and 26 the Committee established, based on judgments of the ECtHR, that additional requirements apply to the use of special powers. For the privacy infringement to be justified, a *potential harm to national security* must be established. See CTIVD review report no. 19 on the application by GISS of article 25 ISS ACT 2002 (taps) and article 27 ISS ACT 2002 (selection of non-directional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §3.3 and 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), §3.5.1. The reports are also available at www.ctivd.nl.

[14] AIVD (GISS), *Van dawa tot jihad. De diverse dreigingen van de radicale islam tegen de democratische rechtsorde,* December 2004, p. 6 and *Radicale dawa in verandering.* De opkomst van islamitisch neoradicalisme in Nederland, October 2007, p. 10, both available at www.aivd.nl.

used did in fact give cause for such serious suspicion. This was reason for the Committee to examine these operations more closely.

The Committee examined one case, for example, in which GISS worked for several years on an investigation based on its security task in order to establish the nature of the threat emanating from the secret activities of a number of persons. GISS had indications of influence and financing from abroad. During this investigation attention was devoted to different activities and various special powers were used, including operations pursuant to article 25 ISS Act 2002. GISS did not succeed, however, in obtaining clarity as to the threat emanating from the persons involved. The use of special powers has been terminated by now. It is the opinion of the Committee that particularly in the final period of this investigation the use of the power to tap or intercept approached the borderline of what is permitted by law. If during several statutory three-month periods no - or hardly any - confirmation of the serious suspicion of the threat to national security is obtained, as in the case discussed here, then after some time it is no longer justified to use the special powers. The Committee recognizes that in those cases it is difficult to make an assessment, but emphasizes the importance, in these cases, of continuously and critically evaluating the use of special powers. This is even more cogent if no - or hardly any - data is obtained that confirm the serious suspicion.

The Committee also came across an investigation concerning a person who wished to publish a certain message.[15] When GISS started the investigation, only limited information was available about the content of the intended publication. In the substantiation of the reasons for the investigation GISS stated that the expected publication would at the least have a radicalising and anti-integration effect and that it could not be excluded that the message would be seen as an incitement to violence. This concern was increased by relevant recognized international contacts of the person concerned. GISS wished to use telephone taps with respect to the person concerned in order to obtain knowledge of the content and objective of the message and of the date of publication. The Committee has established that at the start of the investigation GISS possessed information giving sufficient evidence for a serious suspicion of threat to national security. This information related to the nature and purport of the publication and to the time at which it was to be made public. In addition, the requirements of necessity, proportionality and subsidiarity were met. In this case, therefore, the Committee considers the use of a telephone tap to have been lawful. It draws attention, however, to the latitude which the wording of the reasons leaves for using this special power in comparable cases. It stated that it cannot be *excluded* that the message will be seen as an incitement to activism or serious disturbance

[15] To prevent misunderstandings: this is not about the publication of the film Fitna by member of parliament Wilders.

of public order, or in the worst case scenario as an incitement to violence. This wording is very broad. It is quite possible that a message will confirm the receivers of the message in their radical or even violent ideas. However, the (mere) possibility of a threat to national security is insufficient to justify the use of telephone taps, a serious suspicion must have been established. The Committee also considers this important because individuals may in principle assume that their privacy will not be infringed merely because they wish to express their ideas. It is only when the publication may incite to e.g. radicalisation or the use of violence that it is lawful to use special powers. The Committee therefore recommends that in cases like those discussed above GISS exercises restraint in using special powers.

6. The power to tap or intercept and third parties

When GISS conducts an investigation pursuant to the security task it may happen that the application of article 25 ISS Act 2002 to locations or connections belonging to the target produce insufficient results, for example because the target is highly security conscious. In such cases GISS frequently starts using the powers at locations and in respect of connections of a third party who cannot be considered a target since this person himself does not give cause for serious suspicion that he constitutes a threat to national security.

There are two possible scenarios for the application of article 25 ISS Act 2002 to a location or connection not belonging to a target. Either a target is using these locations or connections although they are not his, or a target is not using them, but the person to whom the location or connection belongs does use them and may, through his activities, produce information about the target.

In the first scenario the application for permission is made in the name of the target since he is the person (or one of the persons) using the location or connection. In its review report no. 19 the Committee said that the substantiation of the reasons for using the power must expressly devote attention to the fact that the means of communication belongs to a third party. GISS must also exercise restraint in working out information relating to the acts of this third party.[16] In addition, when applying for renewal of permission with a view to the results obtained by the use of the power GISS must assess whether the interest of keeping the target under surveillance still outweighs the infringement of the third party's privacy

[16] On this issue also see review report no. 19 on the application by GISS of article 25 ISS ACT 2002 (tapping) and article 27 ISS ACT 2002 (selection of nondirectional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §6.2.2, available at www.ctivd.nl.

rights. Information about a third party collected by using the power can be considered bycatch which may only be worked out with great restraint. The Committee established that in a number of cases in the review period in which GISS applied article 25 ISS Act 2002 to a place or connection belonging to a third party, it failed to properly include the third party's interests in its substantiation of the reasons for applying the article. The Committee considers this a lack of due care. Especially so if several operations under article 25 ISS Act 2002 are ongoing with respect to one single target, including a tap or microphone at a location or connection belonging to a third party. In such cases GISS provides one set of reasons for all these taps combined, without devoting specific attention to the interest of the third party. GISS must, however, explain for each individual tap why it meets the requirements of necessity, proportionality and subsidiarity. This applies specifically where a tap or microphone is used at a place or in respect of a connection belonging to a third party. It is the opinion of the Committee that in the cases in which it established that the substantiation of reasons was inadequate, adequate substantiation of reasons would in fact have been possible. The shortcomings were therefore procedural without involving any unlawful application of article 25 ISS Act 2002 of a substantive nature.

In the second scenario GISS aims at examining the activities of a person in respect of whom no serious suspicion exists that he is a threat to national security, a so-called non-target. The Committee judges this to be a very onerous means which GISS may only use with very great restraint.[17] In the review period the Committee found that GISS does in fact exercise adequate great restraint in using this means when applying article 25 ISS Act 2002.

7. Consultation with DISS

The Committee conducted a more detailed investigation of one operation in which a tap was used in a case in which there were only very limited indications that the person concerned constituted a threat to national security. After lengthy consideration the Committee can understand the assessment made by GISS in this case. It does hold the opinion, however, that this operation is a borderline case.

One factor playing a role in this operation was the existence of weighty reasons to consult with DISS before using the tap. It was an operational situation in which GISS should have seriously considered the fact that DISS, too, had information that was relevant for the

[17] Review report no. 10 on the investigation by GISS into the leaking of state secrets, *Parliamentary Papers II* 2006/07, 29 876, no. 19 (appendix), §5, and review report no. 19 on the application by GISS of article 25 ISS ACT 2002 (tapping/interception) and article 27 ISS ACT 2002 (selection of nondirectional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §6.2.2, available at www.ctivd.nl.

investigation. The Committee asked GISS why it did not contact DISS in order to obtain the information. GISS replied that there were two operational reasons for not approaching DISS. First, the investigation was in an early stage and there were still many operational uncertainties. GISS thought that it was not proper to contact DISS until it had become clear that there was a threat to interests to be protected by DISS. Secondly, GISS feared that prior consultation with DISS would entail a risk of failure for its own operational plans.

The Committee, having regard to the requirements of subsidiarity and due care and the interest of close cooperation between GISS and DISS, holds the opinion that in such a case it is desirable to consult with DISS before taking the step of using a tap. The fact is that GISS, by consulting with DISS, may not only obtain operationally relevant information, but can also prevent that both services are working on the same operational matters independently of each other. Where there is close cooperation between GISS and DISS, moreover, the services may be expected to be able to find arrangements to prevent the mutual exchange of information from harming each other's operational plans.

8. Conclusions and recommendations

8.1 The Committee has established, as it did in the preceding review report on the subject, that GISS takes well-considered decisions when applying article 25 ISS Act 2002. The Committee has not found any unlawful procedures in the operations it investigated. This deserves a compliment given the large number of operations. (section 3.1)

8.2 On some points, however, the Committee has established a lack of due care, in particular in the matter of substantiating the reasons for operations. The Committee holds the opinion that in the cases of faulty substantiation of reasons adequate substantiation of the reasons would in fact have been possible. These cases are therefore a matter of *procedural* shortcomings without involving any unlawful application of article 25 ISS Act 2002 in the *substantive* sense. (section 3.1)

8.3 With respect to one special category of persons that is discussed in greater detail in the secret appendix to this report, the Committee has established several instances of lack of due care in substantiating the reasons for applying article 25 ISS Act 2002. (section 3.1)

8.4 In regard to the application of article 27 ISS Act 2002 the Committee has arrived at the same findings as in review reports 19 and 26. Once again, therefore, it refrains from expressing an opinion on the lawfulness of the selection of Sigint by GISS. (section 3.2)

8.5 It is the opinion of the Committee that it is only possible to assess necessity, proportionality and subsidiarity if all the available relevant information is used in making the assessment. The Committee came across one case in which contraindications regarding the threat emanating from a target were not included in the substantiation of the reasons for continuing a tap. GISS had, however, provided these contraindications to the authorities concerned and they were evidently considered reliable. The Committee therefore holds the opinion that the substantiation of the reasons for this tap was incomplete and consequently lacked due care. (section 4)

8.6 In the course of its investigation the Committee came across a procedure according to which GISS prepares two parallel sets of reasons, one classified secret and the other top secret, for the application of article 25 ISS Act 2002 in one operation. This procedure has the consequence, however, that the secret set of reasons is incomplete and therefore inherently faulty. In addition, this procedure promotes a lack of due care and makes the Committee's review work more difficult. In one operation in which this procedure was followed the Committee was unable to establish whether the staff members involved in the internal assessment procedure were aware of the fact that there was also a top-secret set of reasons. The minister has announced that GISS will henceforth introduce safeguards to prevent carelessness, including the safeguard of actively informing the Committee whenever this procedure is applied. The Committee holds the opinion, however, that this use of two parallel sets of reasons is still at odds with the interest of careful and unambiguous substantiation of reasons. The Committee therefore recommends changing the internal procedures and not applying the procedure in question, except in cases in which it can be demonstrated that its application is necessary. (section 4)

8.7 The Committee has established that in the investigation of radicalisation trends it is not always evident that the person against whom or the organisation against which special powers are used do in fact give cause for serious suspicion that they pose a threat to national security. If during several statutory three-month periods no - or hardly any - confirmation of the serious suspicion of the threat to national security is obtained, then after some time it is no longer justified to use the special powers. The Committee recognizes that in those cases it is difficult to make an assessment, but emphasizes the importance, in these cases, of continuously and critically evaluating the use of special powers. This is even more cogent if no or hardly any data is obtained that confirm the serious suspicion. (section 5)

8.8 In one case, in the context of a radicalisation investigation, GISS applied article 25 ISS Act 2002 for several years in order to establish the nature of the threat emanating from the secret activities of a number of persons. GISS did not succeed, however, in

obtaining clarity as to thus threat. The use of special powers has been terminated by now. It is the opinion of the Committee that particularly in the final period of this investigation the use of the power to tap or intercept approached the borderline of what is permitted by law. (section 5)

8.9 In one case in the context of its radicalisation investigations GISS used article 25 ISS Act 2002 in respect of a person who wished to publish a certain message. The Committee has established that at the start of the investigation GISS possessed limited information which did, however, offer sufficient leads for a serious suspicion of threat to national security. Although the Committee holds the opinion that the use of a telephone tap was lawful, it draws attention to the latitude which the wording of the reasons leaves for using this means in comparable cases. It is stated that it cannot be excluded that the message will be seen as an incitement to activism or serious disturbance of public order, or in the worst case scenario as an incitement to violence. This wording is very broad. The (mere) possibility of a threat to national security is insufficient to justify the use of telephone taps, a serious suspicion must have been established. The Committee also considers this important because individuals may in principle assume that their privacy will not be infringed merely because they wish to express their ideas. It is only when the publication may incite to e.g. radicalisation or the use of violence that it is lawful to use special powers. The Committee therefore recommends that in cases like the above GISS exercises restraint in using special powers. (section 5)

8.10 The Committee has established that GISS, when applying 25 ISS Act 2002 to a place or connection belonging to a third party but being used by a target, failed in a number of cases to properly include the third party's interests in its substantiation of the reasons for applying the special power. The Committee considers this a lack of due care. Especially so if several operations under article 25 ISS Act 2002 are ongoing with respect to one single target, including a tap or microphone at a location or connection belonging to a third party. In such cases GISS provides one set of reasons for all these taps combined, without devoting specific attention to the interest of the third party. GISS must, however, explain for each individual tap why it meets the requirements of necessity, proportionality and subsidiarity. This applies specifically where a tap or microphone is used at a place or in respect of a connection belonging to a third party. (section 6)

8.11 The Committee has established that GISS exercises adequate great restraint in applying article 25 ISS Act 2002 in respect of *non-targets.* (section 6)

8.12 In one case the Committee has established that GISS applied article 25 ISS Act 2002 while there were weighty reasons to consult with DISS before using a tap. In this

case there were only limited indications that the person concerned posed a threat to national security. After lengthy consideration the Committee can understand the assessment made by GISS in this case. It does hold the opinion, however, that this operation is a borderline case. The Committee, having regard to the requirements of subsidiarity and due care and the interest of close cooperation between GISS and DISS, holds the opinion that in such a case it is desirable to consult with DISS before taking the step of using a tap. The fact is that GISS, by consulting with DISS, may not only obtain operationally relevant information but can also prevent that both services are working on the same operational matters independently of each other. Where there is close cooperation between GISS and DISS, moreover, the services may be expected to be able to find arrangements to prevent the mutual exchange of information from harming each other's operational plans. (section 7)

Thus adopted at the meeting of the Committee held on 11 April 2012.

Review Report CTIVD no. 33

On the classification of state secrets by GISS

Table of contents

Summary 57

13. Conclusions 61

Review Report CTIVD no. 33

On the classification of state secrets by GISS

SUMMARY

In performing its task the General Intelligence and Security Service (GISS) handles information which is to a considerable extent state secret information. State secret information concerns the interests of the State or its allies. It is imperative to prevent state secret information from coming to the knowledge of unauthorized persons. State secret information must be designated as state secret in the prescribed manner. Designating information as state secret is known as classification. The Review Committee for the Intelligence and Security Services (further referred to as: the Committee) has investigated whether GISS applies the classification of state secrets correctly.

When classifying information GISS must work within the applicable legal framework. The Committee refers in particular to the provisions of the Civil Service Information Security (Classified Information) Regulations (further referred to as: the "Classified Information Security Regulations"). It is important to recognize that information should only be classified as state secret if it is necessary in the interest of the State or its allies. This principle implies that GISS should aim at classifying as little information as possible. The Committee emphasizes that the principle is not only based on cost-saving reasons, but may also have the effect of promoting transparency.

The Committee has established in the course of its investigation that GISS has hardly elaborated the general rules embodied in the Classified Information Security Regulations in its internal rules. The internal rules are outdated, not widely available within the organisation or fail to provide a sufficient basis to go upon in actual practice. The Committee considers it important that GISS lays down a more detailed, practice-oriented elaboration of the classification guidelines. It points out that the Classified Information Security Regulations require such elaboration as well. The Committee thinks it important that GISS, when adopting detailed rules, gives particular attention to the criteria for the different classification levels.

In spite of the absence of an internal detailed legal framework the Committee has come to the conclusion that the classification process generally proceeds correctly. This holds particularly true for the classification of operational information, i.e. information directly relating to the performance by GISS of its task. In the Committee's opinion the state secret

classification by GISS of information relating only indirectly to the performance of its task is more debatable, in particular in the field of personnel policy at GISS.

The Committee has established that in particular the dividing line between state secret - CONFIDENTIAL and state secret - SECRET can be said to be rather fluid and to a certain extent subjective. In particular with respect to internal products the use of either the one or the other classification level has hardly any practical consequences.

In view of this situation the Committee considers advisable that GISS aims at greater internal awareness of the classification process. A detailed, practice-oriented internal framework can have added value in achieving this. The Committee has also seen reason to recommend that the structural internal supervision at GISS of classification practice will be enshrined more firmly in the organisation.

In regard to the external provision of state secret information, i.e. state secret information provided to end-users outside GISS, the Committee observes that it has found that it is not always clear to end-users what is the state secret element in the information. If GISS would, as far as possible, indicate for each paragraph whether or not it is state secret, this will also lead to greater recognition of the added value by the end-user. At the same time it will prevent erosion of the security regulations, because there is a risk that the security regulations will be applied less strictly if it is not clear why information must be kept secret.

The Committee has established that GISS usually does not state on classified documents what is the classification expiry date. The Classified Information Security Regulations provide for a maximum classification period which varies from ten to twenty years, depending on the type of information. The Committee points out that this is a maximum classification period and that a shorter classification period should be applied whenever possible. The Committee considers advisable that GISS states for each document what is the expiry date of the classification. Expiry dates can be based on classification guidelines to be set out in detail.

In this context the Committee has further established that GISS lacks a structural declassification programme. GISS does not examine the possibility of adjusting or terminating the classification of information after some time. The Committee points out that the Classified Information Security Regulations do in fact impose this active obligation on GISS and that GISS has also included the relevant provision in its own internal rules. In practice, the classification of information is only revised in the context of issuing an official message or dealing with applications for inspection of information processed by or on behalf of the services (known as applications for inspection of files).

The Committee has furthermore established that the service has still not adopted a selection list based on which it can proceed to transfer records to the National Archives or destroy data that are no longer relevant. The ongoing discussion on the subject which has been at a deadlock for years will have to be decided. The Committee considers advisable to adopt a partial selection list with regard to points on which there is no division of opinions. Because there is no selection list, GISS must keep all data in a durable form. This applies to both digital data carriers and paper records. Eventually, this will obviously lead to considerable storage costs. The Committee thinks it likely that the high storage costs will, at any rate in the future, exceed the costs of an active declassification programme, for example in the form of additional manpower.

The Committee is aware that it is difficult to find the right balance between secrecy and transparency. It is not easy for an intelligence and security service to operate inherently and necessarily with a high degree of secrecy, while at the same time providing the transparency required to maintain the trust of society. The Committee perceives an increasing demand in society for greater transparency, also from the intelligence and security services. In addition, with increasing frequency and intrusiveness information provided by GISS to external end-users is subjected to review by the courts for transparency.

13 Conclusions and recommendations

THEORY

13.1 GISS must protect its sources, particularly with a view to their safety. It is the opinion of the Committee that the duty to ensure the secrecy of sources applies exclusively in respect of *human* sources of GISS. A technical source, such as a telephone tap, is not a source within the meaning of article 8(3)(b) ISS Act 2002. (section 3.4.1)

13.2 It is the opinion of the Committee that state secret nature of the methods used by GISS is not permanent and that a connection can be seen to exist with the protection of its current level of knowledge. In the Committee's opinion the use of a special power by GISS is only state secret in nature if the information about the use is relevant to an ongoing investigation of GISS or if it reveals the level of technical knowledge of GISS. If the fact that a special power has been used with respect to a target no longer has any relevance whatsoever to any ongoing investigation, this puts an end to its state secret nature. (section 3.4.2)

13.3 Information should only be classified as state secret if the information in question relates to an ongoing investigation of GISS or if it is relevant to another ongoing investigation of GISS. The Committee holds that if this is not the case, there is no necessity to classify the information as state secret. (section 3.4.3)

13.4 Personal data that are relevant to any ongoing investigation must be classified as state secret to protect the current level of knowledge. Although the law does not contain a similar provision relating to administrative matters, the Committee holds the opinion that the same rule applies to information other than personal data. (section 3.5)

PRACTICE

Internal policy and practice at GISS

13.5 The Committee has established that some GISS staff members assume that the need to classify information and the application of the *need to know* requirement serve the

same purpose, in the sense that they will use a higher classification level to ensure that the information does not come to the knowledge of too many persons *within* GISS. The Committee holds the opinion that classification is not the appropriate means for achieving the latter. Instead, GISS should work with authorized access groups to maintain the *need to know* principle (compartmentalisation). **It recommends that GISS brings this principle clearly into the limelight within the organisation and ensures that no unnecessarily high classification level is assigned to information for the above reason if the nature of the information itself does not require the higher classification level.** (section 6.1)

13.6 The Committee has established that in practice GISS, when classifying information, does not state the expiry date of the classification. The Committee considers this procedure to be contrary to the provisions of the Classified Information Security Regulations. **It recommends that when GISS classifies information it states at the same time, in conformity with article 5(4) of the Classified Information Security Regulations, when the classification can in principle be terminated.** (section 6.1)

13.7 **The Committee recommends that GISS updates the classification list in such a way as to give it practical added value. GISS should moreover ensure that the classification list is widely available within the service and is actively brought to the attention of its employees.** The Committee believes that the security officer can play a role here. The Committee also draws attention to the task of the secretary-general of the ministry of the Interior and Kingdom relations, who is charged pursuant to article 13 of the Classified Information Security Regulations with supervising correct compliance with the Classified Information Security Regulations. (section 6.1)

13.8 The Committee has established that the issue of guidelines for classifying specific types of information, for example certain operational plans or tapping records, is addressed in internal documents on an occasional basis. It is the opinion of the Committee that at GISS such guidelines have not been documented in a sufficiently accessible manner. (section 6.1)

13.9 The Committee has established that a need is felt at GISS at staff level for a more detailed specification of the classification rules. **The Committee recommends that GISS, paying regard to the foregoing including the basic principles derived from case law, provides an elaboration of the Classified Information Security Regulations tailored to practical needs, which as far as possible provides concrete handles for the classification of documents produced by GISS. These detailed rules should pay particular attention to the different classification levels and the criteria applying to each of them.** (section 6.1)

13.10 The Committee observes that GISS has established that certain end-users will take a higher classification level more seriously and that it is therefore worthwhile to use higher classification levels. The Committee can understand this operational principle, but holds the opinion that it is not in conformity with the Classified Information Security Regulations. (section 6.2)

13.11 **The Committee considers it proper for GISS to enshrine the central supervision of consistent application of the classification rules more firmly in the organisation than is presently the case.** (section 6.2)

13.12 The Committee holds that it is not conducive to consistent classification throughout the service that the considerations for classifying a document are but poorly set out in the written opinions of the Supervisory Department. **It recommends adjusting the procedure to make it possible to meet the Classified Information Security Regulations' objective of examining information after some time to see whether it may be declassified and to facilitate decision-making on this point.** (section 6.2)

Classification of operational information

13.13 The Committee has established that by far the most part of the information laid down by GISS does in some way or other give an idea of its sources, methods and/or its current level of knowledge. The Committee observes in this context that it follows from the explanatory memorandum to article 6 of the Classified Information Security Regulations, that if only one passages contains state secret information, the entire document must be classified as state secret. It is therefore the opinion of the Committee that in by far the most cases the state secret classification of operational information was in conformity with legislative and regulatory provisions. (section 7)

13.14 The Committee has established that GISS classifies as state secret both the use of special powers in specific cases and the circumstances connected with such use, e.g. the operational parameters. The Committee considers this to be in conformity with the legislative and regulatory rules. (section 7.1.1)

13.15 The Committee holds the opinion that a multi-year overview of tap statistics cannot be considered state secret information. (section 7.1)

13.16 In addition to the concrete use of special powers GISS also classifies other operational assessments and characteristics of an investigation as state secret information. Examples are the designation of targets, action plans, team assignments

and prioritizations, exploitation policy and the details of cooperation with foreign counterparts. The Committee holds the opinion that such data, which relate to methods for the secret collection of operational information, are rightly classified as state secret. (section 7.1.1)

13.17 The Committee observes that there are bounds to the possibility of designating a method as state secret information. It holds the opinion, for example, that this requires an up-to-date, unknown method. Its unknownness can lie in the person with respect to whom the method is used, or be connected in a general sense to the method itself being unknown, for example in connection with the technical capacities of the service. In the opinion of the Committee the necessity to keep secret the methods used by GISS is in all cases subject to erosion by the mere lapse of time. (section 7.1.1)

13.18 The Committee holds the opinion that GISS generally classified information relating to human sources as state secret in conformity with the legislative and regulatory rules. (section 7.1.2)

13.19 The Committee observes that the necessity to protect sources, and therefore the necessity to classify, depends on the context in which the information was provided to GISS. The covert nature of contacts between source and GISS employee is particularly relevant here. The Committee has established that GISS also classifies as state secret reports of meetings in connection with the performance of its security-promoting task pursuant to article 6(2)(c) ISS Act 2002. The Committee holds the opinion that the state secret nature of such meetings is far from evident. (section 7.1.2)

13.20 GISS finds a connection between breaches of professional integrity within GISS and their supposed negative influence on the willingness of (future) sources to provide information to GISS. The Committee holds the opinion that such a connection should not be assumed too readily and that a categorical refusal to allow an application for inspection of files on the grounds of source protection is not in conformity with the legislative and regulatory rules. (section 7.1.2)

13.21 The Committee holds the opinion that the notification forms sent by the Regional Intelligence services to GISS pursuant to article 62 ISS Act 2002 are often wrongly classified as state secret. The Committee holds the opinion that the mere fact that information is communicated to GISS does not by definition mean that it is state secret information. (section 7.1.2)

13.22 The Committee holds the opinion that GISS generally implements the classification of information relating to current level of knowledge correctly. (section 7.1.3)

13.23 The Committee has established that GISS assigns state secret classification to certain analyses of the regular media. It did so to a collection of relevant media reports without linking them to specific operational investigations. The Committee holds the opinion that classifying this information as state secret is not in accordance with the legislative and regulatory rules. (section 7.1.3)

13.24 The Committee holds the opinion that in the case of official messages issued to the ministry of Economic Affairs, Agriculture and Innovation the general interest of national security must outweigh the individual interest which the exporter concerned has in examining the official messages. (section 7.2.1)

13.25 In by far the most cases the Committee holds the opinion that GISS rightly classified as state secret the Short Information Reports and Special Intelligence Analyses it issued. In a few cases the Committee holds the opinion that GISS could not reasonably have taken the decision to classify the reports as state secret. The Committee holds the opinion that the purport of the reports in question is so general that they cannot reasonably be classified as state secret. In those cases, moreover, it may be assumed that it was quite well-known that GISS was investigating the countries in question. (section 7.2.2)

13.26 **The Committee recommends that GISS, where necessary, states in a document that even though a report does not contain state secret content, it must nevertheless be classified as state secret because of its investigation subject.** (section 7.2.2)

13.27 The Committee draws attention to the fact that one single passage containing state secret information will have the result that the entire document must be classified as state secret. **The Committee recommends that where possible GISS states in such cases for each paragraph whether it is state secret.** (section 7.2.2)

13.28 The Committee holds the opinion that in general the products in the context of the Surveillance and Protection System are correctly classified as state secret. It has established that in the case of threat and risk analyses GISS adopted at least the classification level of the application of the Surveillance and Protection Coordinator. The Committee considers this to be the correct basic principle. If the nature of the information gives cause to do so, it can be classified at a higher level. The Committee holds the opinion that in the cases in which GISS assigned a higher level it rightly decided to do so. (section 7.2.3)

13.29 The Committee holds the opinion that the Surveillance and Protection System products issued on the initiative of GISS (threat reports or threat assessments) were in general rightly classified as state secret. In respect of a number of threat reports the Committee holds the opinion that state secret classification is not necessary.

In the opinion of the Committee the mere fact that the threat report contains the assessment of GISS without this being traceable to state secret sources or without revealing the actual level of knowledge, does not constitute sufficient grounds to classify the report as state secret. (section 7.2.3)

13.30 The Committee holds the opinion that Surveillance and Protection System products, particularly threat reports, are eminently suitable for being made subject to a classification expiry date that is linked to a specific event. Article 6(1) of the Classified Information Security Regulations expressly provides for this possibility. In many cases the threat report mentions an increased threat around a certain event. The Committee holds the opinion that in such cases the classification can be linked to how the event develops. (section 7.2.3)

13.31 The Committee holds the opinion that internal reports in the context of the security-promotion task should not be automatically classified as state secret because these reports are intended for internal use only. The same applies to internal reports of background interviews with journalists, concerning publications by GISS for example. (section 7.2.4)

13.32 The Committee has established that GISS also assigns state secret classification to other external contacts, for example reports received at the front office of GISS and reports of general consultations with third parties. The Committee holds the opinion that in many cases there is no necessity for such classification and recommends that GISS will not classify such information if it is not necessary. (section 7.2.4)

13.33 The Committee holds the opinion that GISS usually decides in a correct manner not to inform the person concerned of certain information in connection with a refusal to issue a certificate of no objection, because the refusal is based on the state secret nature of the information. In the cases in which GISS refrained from mentioning state secret information, the Committee holds the opinion that GISS classified this information as state secret on correct grounds. (section 7.3)

13.34 The Committee holds the opinion that screening reports are rightly classified as state secret, even if they do not include information obtained from sources. (section 7.3)

13.35 The Committee has established that where the personal data of an intended holder of a confidential position are linked to the specific position, this information is classified as state secret. The Committee holds the opinion that this is hardly consistent with the unclassified "Screening Application Form" which is filled out by the employer of the person concerned and on which he fills out this information as well. (section 7.3)

Classification of other information

13.36 The Committee has established that in many cases GISS classified as state secret information relating to the personnel policy at GISS. The Committee has established that it concerns information that is not unique for an organisation like GISS. The Committee holds the opinion that in many cases it can be doubted whether it is necessary to classify this type of information as state secret. (section 8.1)

13.37 The Committee holds the opinion that in a number of cases GISS wrongly classified legal memorandums as state secret. (section 8.2)

Classification levels

13.38 Information reports are classified state secret - CONFIDENTIAL, unless there are operational reasons for using a higher classification level. In that case an internal guideline at GISS requires that the assessment leading to the higher classification level must be recorded in a retrievable manner. The Committee has established that in many cases no such assessment record exists. **It recommends that GISS ensures that such records are kept.** (section 9.2)

13.39 The Committee has established that there are some operational reports from which the identity of the source can be inferred. The Committee holds the opinion that this is inconsistent with the very stringent view of source protection taken at GISS. The Committee holds the opinion that such information should only be mentioned in the agent source file and recommends that GISS ensures that this is the case. The Committee holds the opinion that all information that can be traced back (directly) to the source must be stored in the agent source file. If it is necessary to include the information in the operational report, the classification of the operational report must be adjusted. (section 9.2)

13.40 A number of the persons interviewed said that they used a higher classification level to prevent (too) wide distribution of the information within GISS or to prevent end users of a GISS product from being careless about handling the security regulations. The Committee holds the opinion that this means that the information is classified at too high a level. The appropriate means for preventing information from being too widely distributed within GISS is to take adequate measures limiting access to the information and not the use of higher classification levels. **The Committee recommends that GISS enshrines this principle in its internal regulations.** (section 9.3)

13.41 The Committee has found that in many cases the default classification in the template is viewed as an established fact. The Committee holds the opinion that it

must be assessed for each individual document what is the appropriate classification level and that the default classification can be no more than an indication. The classification of the document must be determined on the basis of the information included in the document. It is the opinion of the Committee that there is insufficient evidence that such individual assessments take place. (section 9.4)

13.42 The Committee has established that in many cases there is a high degree of similarity between the reasons stated in the application for permission to wiretap and the reasons stated for obtaining telephone traffic data with respect to the same person or organisation. In the opinion of the Committee the fact that the reasons for using a telephone tap are mentioned cannot give cause for applying a different classification level than the classification level assigned to the substantiated application for telephone traffic data. The Committee therefore holds the opinion that in this respect the classification is inconsistent and recommends that GISS remedy the inconsistency. **The Committee recommends addressing this issue in the classification guidelines to be drafted.** (section 9.4)

13.43 **The Committee recommends linking the classification level of the use of special powers to the necessity of keeping secret the investigation of a specific person, organisation or phenomenon.** For certain investigation subjects this necessity will be greater and will therefore necessitate a higher classification level. All special powers used in respect of a specific investigation subject will have to be classified at the same level. This principle means that it is not the nature of the special powers that will affect the classification level, but only the subject in respect of whom or which the special power is used. (section 9.4)

13.44 **The Committee recommends that GISS starts consulting with DISS about the practical problems entailed by handling Sigint/Comint information.** (section 9.4)

Destruction and declassification

13.45 The Committee recognizes the great importance of protecting the human sources of GISS. The Committee holds the opinion, however, that a categorical refusal to transfer agent and informer files to the National Archives lacks a legal basis. The Committee holds the opinion that GISS may be required to assess on a case-by-case basis whether the interest of source protection prevents transfer to the National Archives. The Committee does not exclude that in some cases the interest of source protection no longer plays a role in transferring files to the National Archives. In general, the Committee considers a twenty-year ban on transferring agent and informer files to be relatively short. In many cases disclosure of the relationship

with GISS may still endanger the safety of human sources, which bars disclosure of these data. After a period of 75 years, however, the Committee believes this to be conceivable only in very rare cases. **It recommends that GISS further examines the possibility of transferring files in a fully anonimized form, in conformity with a proposal to such effect of the minister of Education, Culture and Science.** (section 10.1)

13.46 The Committee has established that in actual practice GISS does not have a structural active declassification programme in place. The Committee holds the opinion that GISS is thus acting contrary to the Classified Information Security Regulations, article 44 ISS Act 2002, and its internal regulations. (section 10.2)

13.47 The Committee has examined a closed investigation by GISS which has not yet been the subject of an application for inspection and in respect to which the possibility of declassification has not yet been examined. The Committee holds the opinion that the information included in such files can in many cases be declassified without any problems. (section 10.2)

13.48 The Committee holds the opinion that GISS, when processing applications for inspection of files, can pursue greater openness particularly in the matter of declassifying the methods used in the past by the legal predecessor(s) of GISS. (section 10.2.)

13.49 The Committee recognizes that it is not inconceivable that an information report will give an idea of the identity of the source. Operational reports in particular are likely to do so. In such cases GISS will have to be careful about declassifying the information or refrain from declassification. The Committee holds the opinion that GISS must assess on a case-by-case basis whether the data in question considered separately or in combination with each other give an idea of the identity of the source. (section 10.2)

13.50 Based on the selection list serving as a basis for transferring or destroying files GISS can establish which data are to be destroyed and which records will eventually be eligible for transfer. In the opinion of the Committee it will not be necessary to examine whether data earmarked for destruction can be declassified. (section 10.3)

13.51 **The Committee recommends paying more up-front attention to the temporal nature of classification and the grounds on which the decision to classify information as state secret was taken.** (section 10.3)

13.52 **The Committee considers it advisable for GISS to structure the preparation of records in such a way as to anticipate at this early stage, where possible,**

the transfer or destruction of the elements of the records about which there is agreement between the ministry of the Interior and Kingdom Relations and the ministry of Education, Culture and Science. (section 10.3.)

Permanent Parliamentary Committee on Intelligence and Security Services (Permanent ISS Committee)

13.53 **The Committee recommends that where possible GISS states for each individual paragraph of all information provided to the Permanent ISS Committee whether it is state secret.** (section 11)

13.54 The picture obtained by the Committee is that the information from GISS provided to the Permanent ISS Committee was in most cases rightly classified as state secret information. In a number of cases it is the opinion of the Committee that the state secret classification was not necessary. (section 11)

13.55 The Committee holds the opinion that in two cases a memo of an interview with a chairperson of a political group in the Second Chamber was wrongly classified as state secret. (section 11)

13.56 In the opinion of the Committee a letter concerning the ongoing discussion about the selection lists between GISS and DISS on the one hand and the National Archives of the other has been wrongly classified as state secret. The letter merely sets out the legal framework for source protection by GISS and further mentions the transfer or destruction, respectively, of certain data. (section 11)

13.57 The Committee holds the opinion that the covering letter concerning the screening of the antecedents of (candidate) political office holders was wrongly classified as state secret. (section 11)

13.58 The Committee holds the opinion that information that has been provided to the Public Prosecution Service in a public official message has thereby been declassified. This means that it is unnecessary to classify as state secret the information presented to the Permanent ISS Committee. (section 11)

Review Committee on the Intelligence and Security Services

Anna van Saksenlaan 50

2593 HT The Hague

Internet: www.ctivd.nl

E-mail: info@ctivd.nl