Review Committee
on the Intelligence and Security Services
(CTIVD)

ANNUAL REPORT

2011-2012

The annual report covers the period that ended on 31 March 2012.

Table of contents

CTIVD ANNUAL REPORT 2011-2012

Introduction

In the year of 2011 there has been an understandable amount of looking back upon the events of 11 September 2001 and their aftermath. A recurring question was: how can we prevent such things from happening again? Are the intelligence and security services sufficiently equipped for the adequate performance of their tasks? Do they really know what is happening here and everywhere?

The outbreak of what has come to be called the Arab Spring has made it abundantly clear how difficult it is to answer these questions. The collapse within a few months of the regimes in Tunisia, Egypt and subsequently also Libya can only be described as unforeseen.

For the Dutch services these events meant that they had to adjust their areas of attention. North Africa had not been high on their agendas, but now it has clearly gained in importance moved up, partly as a result of the incident of the failed evacuation mission in Libya, which led to a Dutch helicopter crew being detained in that country for some time. Libya was also an affair that put the cooperation between DISS and GISS to the test. In this respect both services slipped up here and there. The authorities involved will undoubtedly draw lessons from these inadequacies.

At the same time, the services naturally did not lose sight of what was happening in their own country and the possible influence of such happenings on national security.

Throughout all these events the Committee has been on the alert to ensure that GISS and DISS would not exceed the limits of their lawful powers when performing their tasks. 'Had not exceeded' is probably more correct, since the Committee performs its oversight task in retrospect, although it aims at keeping as close a track of the services' conduct as possible.

In this connection it is proper to record that in general the conduct of GISS and DISS has borne the scrutiny of criticism very well. Where the Committee held the opinion that this was not the case, which the Committee has always reported in public documents, its criticism was taken

seriously. Although a proper distance must be maintained at all times between an oversight body and the agencies it reviews, the conclusion regarding the present reporting year is again that both services cooperated properly with the Committee wherever this was necessary.

An important point in this connection is, that while it is not the Committee's aim to teach the services a lesson, it does aim at ensuring that they go by the book.

Chapter 1

The reporting year in broad outline

General

The Review Committee for the Intelligence and Security Services (CTIVD, further referred to as: the Committee), reviews whether the intelligence and security services GISS and DISS perform their tasks lawfully. For this purpose the Committee conducts in-depth investigations resulting in review reports, where necessary with secret appendices; it follows certain activities of the services by sample monitoring; and it acts as complaints advisory committee in the case of complaints about the services. The Committee is an independent government body.[1]

The Committee is composed of three members. At present they are:

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

The Committee members all work part-time.

Mr. N. Verhoeven terminated his work as secretary to the Committee and was succeeded in this capacity by Ms. H.T. Bos-Ollermann on 1 February 2012. During the reporting year two new review officers have taken office, so that the staff of the Committee is now composed of five review officers and an administrative adviser.

In-depth investigations

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

Early in 2011 an attempt to evacuate a Dutch national from the Libyan port of Sirte failed. The helicopter crew and two evacuees were captured. When this came up for discussion in parliament, the Committee was asked to investigate the roles of GISS and DISS in the evacuation mission. In addition to issuing a letter to be used in the parliamentary debate in early 2011, the Committee presented the findings of its investigation in the autumn of 2011 in a review report on the roles of DISS and GISS in an evacuation mission in Libya (review report 27).

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

For DISS, the use of *signals intelligence* (Sigint) is an important category of special powers. The Committee investigated the lawfulness of the use of Sigint. This resulted in a review report which describes the procedures followed by DISS and compares them to the parameters set by the law (review report 28, see §2 below and appendix III).

In 2005 the Committee for the first time investigated the official messages sent by GISS to government agencies such as the Public Prosecution Service and the Immigration and Naturalisation Service (review report 9a, see www.ctivd.nl). In the present reporting year the Committee issued a report on its investigation of the official messages issued by GISS since that time. In addition to the official messages to the aforementioned recipients, the Committee also discussed the messages issued to the ministry of Economic Affairs, Agriculture and Innovation and to the chairpersons of political parties, the person charged with forming a new government and the prime minister (review report 29, see §3 below, and appendix VI).

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 DISS (review report 30a). A similar report has been drafted with respect to GISS, which will be issued in the course of 2012.

In the reporting year the Committee made considerable progress with large-scale investigations into the cooperation between DISS and foreign intelligence and security services, the classification of state secrets by GISS and the official messages issued by DISS. The use made by GISS of the wiretapping power and the power to use Sigint is a subject of investigation by the Committee on an annual basis. The review report for the period September 2010 – August 2011 has been drafted and will be issued in the course of 2012. The investigation of the use of these powers since September 2011 is ongoing. Furthermore, the Committee has started a new investigation of long-term agent operations of GISS. The Committee has further announced that it will conduct a follow-up investigation of the performance by GISS of its obligation to notify.

Sample monitoring

The Committee aims at obtaining a wide understanding of the core activities of GISS and DISS. For this purpose it selects subjects which it monitors either systematically or occasionally by sample monitoring. If the Committee finds there is reason to do so, it reports its findings to the management of the service concerned, the responsible minister, or the parliament. Such sample monitoring can also lead to an in-depth investigation.

In the reporting year the Committee used sample monitoring to examine how security screenings were carried out, official messages issued, and applications for inspection of files dealt with.

In the reporting year the Committee also started identifying the fields of activity of the two services to which it will pay greater attention in the near future. In addition, the Committee corresponded with the management of both services about aspects of their policies on granting inspection of files and doing security screenings. So far, the nature of the matters discussed has not given cause to inform the minister concerned and/or parliament.

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 advisory complaint committee. The Committee 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 the minister takes the ultimate decision. If the minister departs from the Committee's advisory opinion, the advisory opinion must be sent to the complainant.

In the reporting year the Committee handled ten complaints, all regarding GISS.

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 three complaints the Committee advised the minister of the Interior and Kingdom Relations to declare the complaint ill-founded. In the first case the complainant was unable to present a prima facie case concerning the matters about which he complained, and the Committee did not find other evidence of any improper conduct of GISS in regard to the complainant either. The second case concerned an official message issued by GISS. The Committee's investigation showed that the information contained in the official message had been provided in conformity with the requirements set by the ISS Act 2002. The third case was a complaint about the performance of a security screening. The Committee established that there had been no improper conduct of GISS in connection with this security screening.

With regard to one complaint the Committee advised the minister of the Interior and Kingdom Relations to declare the complaint well-founded. This complaint concerned a failure to meet a time limit which in the opinion of the Committee caused an unacceptable delay.

With regard to two 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. The Committee's advisory opinion was that the minister declare one complaint partly well-founded and partly ill-founded, and declare one complaint ill-founded. The Committee will again consider these complaints in its next annual report.

In all cases in which the minister concerned did give a decision, she followed the Committee's advisory opinion. The Committee draws attention to the fact that if its advisory opinion is not classified, the minister forwards it in its entirety to the complainant concerned. The Committee considers this a proper procedure, since it makes the wording of the Committee's advisory opinion clear to complainants.

The Committee is free to conduct investigations in reaction to complaints that are not taken up by the minister. An example of a complaint that was not taken up by the minister in the reporting year is the complaint of Mr R. van Duijn. Pending the handling of this complaint by the National Ombudsman the Committee considers it proper to practice restraint and not to conduct an in-depth investigation of its own.

Working procedure of the Committee

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

The Committee points out, however, that several times in the reporting year the minister of Defence exceeded time limits by considerable periods when forwarding the Committee's review reports concerning DISS to the two Chambers of the States General. The minister sent the Sigint report to the two Chambers of the States General more than ten weeks after the statutory time limit had expired. The report on previous recommendations was sent six weeks after the time limit had expired. The minister has not stated any reasons for these considerable delays.

The Committee points out that the statutory six-week period of Article 79(5), ISS Act 2002 is in every respect reasonable, the more so since the minister is already allowed a four-week period to send the Committee a reaction to the report at an earlier stage of the procedure (Article 79(1), ISS Act 2002). The Committee holds that the long periods by which time limits were exceeded in the reporting year are undesirable.

In its previous annual report the Committee mentioned the difficulties it encountered in obtaining access to information at DISS. Meanwhile, its access has improved in accordance with the promises made by the director of DISS. However, the Committee finds that the digital documentation system of DISS is not particularly user-friendly.

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 7 December 2011 the Committee met with the Standing Parliamentary Committee for the Interior and Kingdom Relations to discuss the Committee's annual report and the report on the official messages issued by GISS. On 15 December 2011 the Committee discussed the state-secret aspects of its findings with the parliamentary Committee on the Intelligence and Security Services. The Committee met with the Standing Parliamentary Committee on Defence to discuss the review report on the use of Sigint by DISS on 14 February 2012.

On 25 May 2011 the Committee spoke successively with prime minister Rutte, the minister of the Interior and Kingdom Relations Mr. Donner, and Defence minister Hillen. On 24 January 2012 the Committee was introduced to Ms. Spies, the new minister of the Interior and Kingdom Relations. On 30 November 2011 the Committee met with the secretary-general of the ministry of General Affairs, acting among other things in his capacity as coordinator for the intelligence and security services.

Two consultative meetings with the management of GISS and of DISS took place in the reporting year. The matters discussed at these meetings include the reports that had been issued, ongoing investigations and the results of the Committee's sample monitoring reviews.

Furthermore, the Committee had a meeting with the National Public Prosecutors for counterterrorism, who act as a link between GISS and DISS on the one hand and the Public Prosecution Services on the other hand.

Chapter 2

The use of Sigint by DISS

Many of the special powers of GISS and DISS have a highly technical dimension. This is certainly true of the powers used in connection with *signals intelligence* (Sigint), a means for obtaining intelligence from satellite and radio communications. The importance of using these special powers and the Committee's unfamiliarity with the subject gave the Committee reason to investigate the use of Sigint by DISS.

Usually when the Committee investigates the use of a special power, it also examines the lawfulness of individual operations. In the course of the present investigation it became clear that it was not possible to do so straightaway. The Committee therefore chose the option of preparing a review report in which it established parameters. Several factors played a role in this decision.

There is a lack of clarity, for example, about the way in which, and how severely the use of Sigint infringes the right to privacy. For this reason the Committee describes in its report how such infringement should be viewed from the perspectives of the ECHR and the Constitution. The severity of the infringement entailed by the use of Sigint depends on the means used and the concrete circumstances of the individual case. Against this background it becomes clear how the legal framework provided by the ISS Act 2002 can be applied to the use of Sigint.

In the course of the investigation the process of handling Sigint proved to be so extensive, technical and mostly not laid down in writing, that the Committee decided it would first analyse the process before reviewing individual operations. In its report the Committee explains how DISS handles stating the Sigint needs, and the collection, processing and reporting of Sigint. The Committee has established that in several respects the procedures followed by DISS for using Sigint are not in accordance with the requirements set by the ISS Act 2002. For example, DISS obtains permission to use special powers with respect to broad categories of persons and organisations, while the law requires it to apply for such permission for each person or organisation individually. Furthermore, the power of searching (exploring telecommunications) is also used more widely than the law permits. This conflict between law and practice means that either the law or actual practice will have to be adjusted. The Committee suggests examining whether it is necessary, with due regard to the protection of privacy, to give DISS wider powers which are more in line with existing (advisable) practice. It is the responsibility of the legislature to consider this matter carefully.

In addition, the Committee's investigation has shown that DISS states only limited reasons for its use of Sigint. The Committee can only review whether individual operations satisfy the statutory requirements of necessity, proportionality and subsidiarity if adequate reasons have been stated why the use of Sigint is necessary. Since the reasons stated in applications with respect to concrete operations are often insufficiently focused at the person or organisation at which the power is targeted, the Committee was compelled in those cases to refrain from giving an opinion on the lawfulness of the use of Sigint.

In his reaction to the Committee's report the minister stated that all recommendations would be adopted. With regard to improving the substantiation of applications by reasons, however, the minister observed that consideration must be given to practical feasibility, too. He expressed the wish to consult with the Committee on the matter. With respect to other elements the minister also expressed the wish to discuss with the Committee how the recommendations are to be implemented. With regard to the discrepancy between legislation and practice the minister observed that with the passing of time and continuing technological developments, existing legislation has become increasingly constraining. The minister promised that in the course of 2012 he would inform parliament how he and his colleague at the ministry of the Interior and Kingdom Relations envisage dealing with these problems.

In response to the minister's reaction the Committee informed the management of DISS that it had no objections to further consultations. Prior to the consultations, however, the Committee said it would like to receive an explanation from DISS how the service intends to implement the recommendations. DISS replied that it would promptly set about drafting a legislative amendment. The proposal would be presented to the Committee in due course. On 14 February 2012 the Committee explained its report to the Standing Parliamentary Committee on Defence. The questions asked by the Parliamentary Committee were answered by the minister on 12 March 2012 and were to be discussed later in the spring at a general consultative meeting.

Chapter 3

GISS and holders of and candidates for political office

Every once in a while the question arises to what extent the Dutch intelligence and security services engage in investigating politicians, and it also arose in this reporting year.[2] In December 2011 the question was asked whether a minister had requested GISS in 2008 to investigate Member of Parliament Wilders in order to find out more about the publication of the latter's film Fitna.[3] The minister gave a negative answer and added orally that GISS had not used any special powers since there was no threat to national security.[4] By way of general information the minister stated that the tasks of GISS are laid down by law, thus providing the parameters within which investigations are carried out. The ISS Act 2002 describes the tasks in Article 6(2) (s) and does not distinguish between politicians and other persons: if a person gives cause for a serious suspicion that he poses a threat to national security, it is legitimate for GISS to conduct an investigation. The minister observed that since recently an additional safeguard was in place for the proper performance of this task in respect to politicians, namely that the Committee's chairman is informed immediately if GISS uses special powers with respect to a politician.[5]

Sometimes, the question whether objections exist from a national security perspective against (new) holders of political office may also arise within a political party. And if new ministers or vice ministers are to be appointed, this question definitely requires an adequate answer. In this matter GISS has the best information position, but GISS' role in relation to politics is a delicate one: it calls for restraint, and the self-correcting capacity of politics should be the prime consideration.[6] For this reason new holders of political office are not subjected to security screening. However, there is procedure for asking GISS whether, in view of national security, there are objections against a specific holder of or candidate for political office.[7] In the reporting year the Committee investigated how GISS had dealt with such requests for information and how GISS had provided information on holders of or candidates for political office. The Committee's conclusion is that there are structural shortcomings as regards both policy and implementation (review report 29, §7 and §8, see appendix IV).

For some time now the procedure for appointing new ministers or vice ministers has been

---

[2] *Appendix to the Proceedings II* 2011/12, no. 632.
[3] *Appendix to the Proceedings II* 2011/12, no. 874.
[4] *Parliamentary Papers II* 2011/12, 29 924, no. 75, p. 21.
[5] *Parliamentary Papers II* 2011/12, 29 924, no. 75, p. 25.
[6] *Proceedings I,* 17 February 1994, 54, 3974-3975.
[7] In its communication to the political party chairpersons, though, GISS has focused the procedure on candidate members of parliament, see also §7.1 of the Committee's report on the official messages issued by GISS, see appendix IV.

that the person charged with forming a new government, or the prime minister in the case of appointments between elections, requests GISS to do an administrative check in its own digital databases.[8] A candidate for a government post is deemed to have given his consent for such a check by declaring himself to be a candidate. Via the secretary-general GISS provides the result of the check to the person charged with forming a new government or the prime minister. The law requires that GISS provides personal data in writing. The Committee's investigation has shown, however, that in the case dating from 2007 which it investigated no written records were made of the information provision. The Committee is therefore unable to assess whether this information provision, which must be considered an official message, satisfied the statutory requirements. The Committee concludes that both the policy on this category of official messages and its implementation fall seriously short of what is required. It recommends that GISS brings the procedure into line with the statutory requirements.

The chairperson of a political party can also request GISS to do a check in respect of a holder of or candidate for political office belonging to his or her party. GISS may only do such a check and subsequently provide the information found if a number of requirements following from the law are satisfied. The check and the provision of information must be necessary. The Committee holds the opinion that this means that adequate reasons must be stated that and why the political party, after conducting its own investigation, suspects that the holder of or candidate for political office poses a threat to national security. In the five official messages it investigated the Committee established the following shortcomings: in three cases the check should not have been done, in one case information was provided to the party chairperson without legal basis, in one case the information was provided orally and in one case by text message, while pursuant to law the information should have been provided in writing.

Possibly, the political sensitivity of the provision of information concerning holders of or candidates for political office was a reason for following a procedure involving hardly any written records. The Committee points out that it is precisely the political sensitivity that is reason to lay down all the steps in writing. Only when this has been done, will it be possible (at a later date) to establish what was the role played by GISS in this special procedure.

In reaction to the review report the minister of the Interior and Kingdom Relations promised that the policy documents and internal procedures would be adjusted so as to implement the recommendations of the Committee. In the course of the next reporting year the Committee will investigate how its recommendations have been implemented. Since the minister of the Interior and Kingdom Relations has promised to keep the Committee informed of each new provision of information on holders of or candidates for political office, the Committee will also continue monitoring these concrete cases.

[8] When doing an administrative check, the officer examines whether the databases of GISS contain any information, and if so, what information. No security screening is done, therefore, nor are any (special) powers used.

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 attracting a lot of attention abroad. For this reason some of the Committee's review reports are translated into English.

In the reporting year two foreign oversight committees visited the Netherlands. From 9 - 11 May 2011 the Committee entertained the Norwegian parliamentary oversight committee (EOS committee) and on 31 August 2011 the German parliamentarian committee which oversees compliance with legislation on privacy and the protection of communications (*G10 Kommission*) paid us a visit.

On 27 and 28 October 2011 the seventh Conference of the parliamentary committees for the oversight of intelligence and security services of the European Union member states was held in Berlin. Although the Committee is not itself a parliamentary oversight committee, the German *Bundestag* had invited the Committee to the Conference.

On 2 December 2011 an international conference was held at the Clingendael Institute in The Hague on the oversight of intelligence and security services in the Western Balkans. The conference was part of a project financed by the Dutch ministry of Foreign Affairs, organised by DCAF, a centre for security, development and rule of law, and aimed at strengthening oversight in this region. The conference was attended by representatives of over ten countries in both the Western Balkans and Western Europe.

APPENDIX I

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.[1] Article 1 of the Act defines the term 'services' to comprise the General Intelligence and Security Service (GISS) and the Military Intelligence and Security Services (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 minister of General Affairs (see Art. 4 of the ISS Act 2002).

The statutory tasks of the Committee also include oversight of officers of the police force, the Royal Netherlands Military Constabulary and the Tax and Customs Administration, insofar as they perform activities for GISS (see Art. 60 of the ISS Act 2002). A legislative proposal is under preparation which will bring officers of the Immigration and Naturalisation Service (*IND*) within the scope of this Article as well (as part of the so-called Post-Madrid measures).

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[2] are implemented lawfully;
b. informing and advising the ministers concerned on the findings of the Committee (both on request and on its own initiative);
c. advising the ministers concerned on the investigation and assessment of complaints;
d. advising the ministers concerned on the obligation to notify, which is embodied in Article 34 of the Act and which entered into effect five years after the ISS Act 2002 entered into effect – from 29 May 2007, therefore.

---

[1] See Bulletin of Acts and Decrees (*Stb.*) 2002, 148 (most recently amended by Act of 2 November 2006, *Stb.* 574).
[2] Bulletin of Acts and Decrees (*Stb.*) 2002, 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, for example, closely scrutinizes 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 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 (among other things) whether 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 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 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, 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, 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.

Once 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), the ministers concerned and the presidents of the two Chambers are informed of this intention.

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 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 related investigative subjects.
Furthermore, any person involved in the implementation of these two Acts, first of all the employees of the services therefore, 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, in the interest of national security, not be disclosed beyond the Committee.

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 such information as the Committee considers necessary, obviously insofar as they have knowledge of the 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 Standing Parliamentary Committee on Home Affairs and Kingdom Relations and the Standing Parliamentary Committee on Defence. In addition, the Committee has consultative meetings with the Standing Parliamentary Committee of the First Chamber on Home Affairs and Kingdom Relations / General Affairs and on Foreign Affairs, Defence and Development Assistance, 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[3] 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.

Involving 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.

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 the complaint is manifestly ill-founded, however, the Committee may decide not to examine the files. Next, the Committee proceeds to hear the complainant unless it decides 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 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 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.[4] Subsequently, the Committee sends a report of its findings accompanied by an advisory opinion and possibly by recommendations to the minister

[3] 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.

[4] But lawfulness forms part of the standards of proper conduct applied as a criterion in handling complaints. *Parliamentary papers* II 1997-1998, 25 837, B, p. 6.

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 departing from the advisory opinion in his or her reply to the complainant, and also must send the Committee's advisory opinion to the complainant.
In formulating its advisory opinion the Committee must therefore bear in mind that the advisory opinion may be made public.This will inevitably result in the Committee sometimes 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.[5] The Committee likewise holds the opinion that the services must first be given an opportunity to dispose of complaints informally 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 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.[6] In principle the Committee must give an advisory opinion on such complaints as well. 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.[7]

---

[5] *Parliamentary papers II* 1997/98, 25 837, no. 3, p. 7.

[6] 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.

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

APPENDIX II

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 from 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* (*Toezichtsrapport 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)

* Available in English

APPENDIX III

Review report 28: the use of Sigint by DISS

Review Report CTIVD no. 28

On the use of Sigint by DISS

Table of contents

Review Report CTIVD no. 28

On the use of Sigint by DISS

Summary

The Committee's investigation was directed at the lawfulness of the use of the measure of *signals intelligence* (Sigint) by the Defence Intelligence and Security Service (DISS). In this context Sigint means gathering and processing intelligence obtained from satellite and radio communications.The investigation focused on how DISS, when using Sigint, exercises the special powers which the Intelligence and Security Services Act 2002 (ISS Act 2002) confers on DISS. The special powers in question are targeted interception (Article 27, ISS Act 2002), selection after non-targeted interception (Article 27, ISS Act 2002) and searching (Article 26 , ISS Act 2002).

The severity of the infringement entailed by the use of Sigint depends on the measure used and the concrete circumstances of the case. From this perspective, targeted interception of radio traffic is comparable to wiretapping, except that the communications that are intercepted are usually communications between public agencies or organisations. Non-targeted interception of satellite communications and subsequent selection is usually perceived as less infringing but under certain circumstances it can certainly be severely infringing. Searching likewise infringes the freedom of communication which is protected by (constitutional) law.

A decision to use Sigint is based on the intelligence needs stated to DISS by external parties and the resulting internal intelligence needs that are then determined by the teams of the Intelligence department. The use of Sigint also depends on the technical and capacity possibilities and impossibilities at the agencies gathering the intelligence, such as the National Sigint Organisation (NSO) and Sigint detachments.The Committee holds the opinion that the assessment whether the use of Sigint will satisfy the requirements of necessity, proportionality and subsidiarity set by the ISS Act 2002 should already be made when the need for Sigint is determined.The Committee considers it important that these assessments are made by the team that determines the needs.

The Committee takes the position, when use is made of Sigint abroad, that the ISS Act 2002 must be applied by analogy and all procedures prescribed by law must be followed.The Committee can imagine urgent situations in the context of intelligence support to crisis management operations in which immediate action is required and the procedural safeguards embodied in the ISS Act 2002 are not applied.

DISS must ask permission for the use of Sigint measures from the minister of Defence.

The Committee has established that DISS applies for and obtains permission to intercept or select communications of broadly defined categories of persons and organisations, called generic identities. The Committee holds the opinion that this procedure is not consistent with the law. In the case of targeted interception the Committee considers naming generic identities not permissible. This is different in the case of selection after non-targeted interception. Under certain circumstances it can be necessary to apply broad selection criteria in the initial stages of an investigation or in the case of a new area to be investigated. The Committee has established that the statutory rules and practical necessities diverge on this point.

In many cases the reasons stated in substantiation of applications for permission were inadequate. The Committee holds the opinion that it must be assessed with respect to each individual person, organisation or combined group whether the use of Sigint measures is necessary, proportionate and that it is not possible to take less infringing measures. Where a generic identity is named for the selection of satellite communications, it must be assessed why this is (still) necessary. The applications for permission or renewed permission do not or not sufficiently show whether these assessments have been made. Since the Committee has insufficient knowledge of the reasons underlying the exercise of the powers, it cannot give an opinion as to whether the powers have been exercised lawfully.

DISS does not only exercise the power of searching for the purposes of targeted and non-targeted interception, but also in support of selection. The Committee has established that there is only a partial internal description of the operating procedure at DISS with regard to searching for the purpose of the selection process and that it has not been formalised. In the course of its investigation, and also based on interviews held with the persons involved, the Committee has described actual practice at DISS. It holds the opinion that the practice as described should be laid down in a written operating procedure and recommends that DISS does so as soon as possible.

The Committee has established that search activities are carried out for several reasons and with several objectives. It has in any case distinguished the following common practices:

1. Searching the communications bulk to determine whether the desired information can be generated using the selection criteria for which permission has been obtained;
2. Searching the communications bulk to identify or characterise potential targets;
3. Searching the communications bulk for data from which future selection criteria can be derived for the purposes of an expected new investigation area.

The Committee considers the first practice of searching permissible. However, the safeguards built in by DISS to preclude any unlawful exercise of this power do not provide sufficient protection. The Committee holds the opinion that the infringement of (privacy) rights of third parties entailed by the second and third searching practices has no basis in the ISS Act 2002. Consequently, it holds that these practices of searching for selection purposes are not permissible.

DISS cooperates with partner services in the field of Sigint. This cooperation can take various forms. There is, for example, both technical cooperation and cooperation with regard to content. The Committee holds the opinion that certain forms of cooperation constitute technical support within the meaning of Article 59(4), ISS Act 2002. The Committee considers it necessary that DISS assesses in each individual case whether the conditions attached to providing support are satisfied. The Committee further holds the opinion that whenever DISS exercises special powers to support a foreign service, all the legal requirements applying to the exercise of these powers must be satisfied. In the course of its investigation the Committee has not found that this is always the case.

In its report the Committee establishes several times that the statutory rules pertaining to the powers of DISS in the field of Sigint are not consistent or are even at odds with existing (advisable) practice at DISS. The Committee suggests examining whether it is necessary, with due regard to the protection of privacy, to give DISS (and GISS) wider powers which are more in line with existing (advisable) practice. It is the responsibility of the legislature to consider this matter carefully. The Committee points out that it is essential for those involved in the process that the methods followed by the service(s) in actual practice are clearly described and laid down in written procedures. The Committee urgently recommends that this is done as soon as possible.

Review Report CTIVD no. 28

On the use of Sigint by DISS

1. Introduction

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 *signals intelligence* (further referred to as: Sigint) by the Defence Intelligence and Security Service (DISS). On 5 November 2008 the Committee, pursuant to Article 78(3), ISS Act 2002, informed the minister of Defence and the presidents of the two Chambers of the Dutch parliament of the intended investigation.

This report has a secret appendix.

The investigation took longer than usual. The limited capacity of the Committee and the choice to give priority to other investigations delayed progress with the investigation of the use of Sigint by DISS.

The review report was drafted by the Committee on 13 July 2011. On 11 August 2011 the Committee received the reaction of the minister of Defence to the draft report. In response to the minister's reaction the Committee decided to transfer some passages from the public review report to the secret appendix. The review report was adopted by the Committee on 23 August 2011.

2. Organisation of the investigation

The Committee's investigation was directed at the lawfulness of the use of the measure of Sigint by DISS. In this context Sigint means gathering and processing intelligence obtained from satellite and radio communications. At DISS, this task is performed by the Sigint department.

In its investigation the Committee aimed at giving attention to the entire process of Sigint handling within the DISS organisation. For the purposes of the investigation the umbrella term 'handling' includes among other things the statement of Sigint needs and the collection, processing, reporting and exploitation of Sigint. Because of the large scope of the handling process and the

highly technical nature of the subject matter, the Committee has chosen the option of first making an analysis of the process. In doing this it disregarded certain rather technical elements of Sigint handling. The Committee does not preclude the possibility of a future follow-up investigation into the use of Sigint by DISS in which it will investigate aspects of Sigint handling in greater detail. The Committee is considering the possibility of calling in the assistance of a technical expert in that case.

The Committee's investigation focused on how DISS, when using Sigint, exercises the special powers conferred on it by the ISS Act 2002. These special powers are the power of targeted interception of telecommunications (Article 25, ISS Act 2002), the power of selection after non-targeted interception of telecommunications (Article 27, ISS Act 2002) and the power of exploring communications, also known as *searching* (Article 26 , ISS Act 2002).

The Committee has opted to prepare a review report in which it establishes parameters without discussing individual operations, contrary to its usual procedure. It is the intention of the Committee, when some time will have passed, to start an investigation of how DISS applies these parameters.

The Committee has opted to exclude some (sub)elements related to the use of Sigint by DISS from this investigation. À brief discussion of these elements will follow below.

Usually, the signals forming the source for gathering intelligence are communications between two parties. This is called *communications intelligence* (or: Comint). But DISS can also collect intelligence from another type of signals, for example radar signals. This form of gathering intelligence is known as *electronic intelligence* (or: Elint). Comint and Elint together make up Sigint. Since the interception and further processing of Elint does not infringe privacy rights or other fundamental rights, the Committee with further leave the subject of Elint out of consideration. With a view to readability the Committee will use the umbrella term of 'Sigint', but the report actually deals with Comint only.

The task of obtaining Sigint is executed by the National Sigint Organisation (NSO). One of the tasks of NSO is to intercept satellite and radio communications for DISS (and for the General Intelligence and Security Service (GISS)). For this purpose DISS submits requests to NSO. More detailed rules for this cooperation have been laid down in the Covenant concerning the interception of non-cable-bound telecommunications by the National Sigint Organisation.[1] The manner in which NSO and DISS (and GISS) together implement the Covenant and the cooperation it entails would call for an entirely separate investigation. The Committee has therefore decided not to include this subject in the present investigation.

[1] Netherlands Government Gazette (*Staatscourant*) 2007, no. 129, p. 8.

Cooperation of DISS with foreign intelligence and security services in the area of Sigint plays an important role in the handling process. In the present investigation the Committee devoted attention to the lawfulness of a specific form of cooperation with foreign services. The Committee did not examine other, mainly relational, aspects of the cooperation with foreign services in the context of this investigation. These aspects will be discussed in the Committee's forthcoming review report on the cooperation of DISS with foreign intelligence and/or security services.

DISS also exercises its powers abroad to collect Sigint for use in deployments of the Dutch armed forces, for example the mission in Afghanistan. It does so via detached posts abroad, known as Sigint detachments. In the present investigation the Committee devoted attention to the activities undertaken by DISS in this context in a general sense and to the manner in which it applies the parameters set by the ISS Act 2002 for the use of Sigint by DISS. The Committee has not, however, investigated the handling of Sigint by any specific detachment abroad.

The Sigint process is a very technical process. A number of the systems used by DISS or NSO are designed to incorporate certain safeguards in the process. This review report mentions several examples of such technical safeguards. The Committee notes that it has not further investigated the functioning of these systems in actual practice.

The Committee reviewed the files at DISS covering the period from early 2007 until the end of 2010. For the purposes of its review the Committee observed international rules and guidelines for handling Sigint, which are binding on DISS.

In addition to reviewing files, the Committee interviewed officials of DISS, including managers, legal experts, analysts, linguists and other employees of the Sigint department as well as the Information department and the Legal Affairs department of DISS. The Committee also talked with the Legal Affairs department of the ministry of Defence, with a representative of NSO and with a legal expert of GISS.

The review report has the following structure. Section 3 discusses a number of provisions of the European Convention on Human Rights (ECHR) and the Dutch Constitution. In this context the Committee pays attention to the infringing nature of the measure of Sigint and the background against which the powers of DISS should be examined. The significance and scope of the power of targeted interception (Article 25, ISS Act 2002), the power of selection after non-targeted interception (Article 27, ISS Act 2002) and the power of searching (Article 26, ISS Act 2002) are discussed in section 4. Section 5 outlines the review framework laid down in the ISS Act 2002. Sections 6 through 9 deal with the different aspects of the process of handling Sigint at DISS. These are, successively, the statement of Sigint needs, the collection of Sigint in the practical and legal sense, the processing of Sigint, and finally the reports on and exploitation of Sigint. In these sections the Committee also discusses the problem areas it identified in the relation between the legal framework and actual practice at DISS. The Committee's conclusions and recommendations

are presented in section 10. The Committee concludes the review report with a final observation in section 11.

The Committee points out that the complexity of the subject matter together with the wish to write a comprehensible review report occasionally induced it to present a simplified picture of actual practice.

3. The ECHR and the Constitution

In the course of its investigation the Committee became aware of diverging views on how and to what extent the use of Sigint infringes the right to privacy. The Committee noticed that not all persons who handle Sigint on a daily basis fully appreciate the extent to which this measure infringes rights. Furthermore, the extent of infringement is usually linked to the possible or actual results of using the measure. Legal experts frequently use the term *potential* infringement of the right to privacy by the use of Sigint. It was also argued before the Committee that as a rule there is no serious infringement because 'real-time' listening-in is not possible with Sigint, and that often no note is taken of the content of the communications until after their transmission, i.e. after the communications have reached their destination. It was also argued that usually only part of the total of communications of a specific person or organisation can be received and recorded and that moreover the communicating parties remain totally unaware of being intercepted.

The Committee considers it advisable to bring greater clarity about the infringement resulting from the use of Sigint by DISS. For this purpose the Committee will discuss the right to privacy protected by Article 8 of the ECHR and the corresponding case law, and the right to privacy protected by Article 10 and, by extension, Article 13 of our Constitution. These provisions form the basis of how the special powers of DISS have been embodied in the ISS Act 2002 and they constitute one of the sources of the parameters to be observed by DISS when using Sigint.

Sections 4 and 5 contain a more detailed discussion of the special powers and the review framework (necessity, proportionality and subsidiarity) embodied in the ISS Act 2002.

3.1 Protection of privacy in the ECHR

The right to protection of privacy is enshrined in Article 8 of the ECHR. Based on case law of the European Court of Human Rights[2], the next section will consider what this right means and under which circumstances restrictions of this right are justified for the purposes of national security.

[2] The full texts of the judgments of the European Court to which this section refers can be found at www.echr.coe.int using the HUDOC search engine.

3.1.1 Interference with the exercise of the right to privacy

Article 8(1) ECHR provides that everyone has the right to respect for his private and family life, his home and his correspondence. The scope of this right to privacy has been elaborated in the judgments of the European Court on Article 8 ECHR. It is an extensive body of case law and covers a multitude of areas, such as spatial privacy (e.g. the right to inviolability of the home), relational privacy, the right to correspondence and information privacy (including personal data processing). There are, however, only a limited number of cases decided by the European Court in which secret investigations by an intelligence and/or security service interfered with the exercise of the right to privacy in the interests of national security.

The Court gave its first ruling on this subject in *Klass v. Germany*[3]. One of the issues to be decided by the Court was whether national legislation allowing the authorities to open mail, read telegraph communications and record and listen in to telephone conversations constituted interference with the exercise of the right to privacy as enshrined in Article 8 ECHR. The Court ruled that each of the permitted measures, applied to an individual, will result in an interference with the individual's right to privacy. According to the Court this is also true for recording and listening in to telephone conversations, which are covered by the notions of private life and correspondence in spite of the fact that Article 8 ECHR does not expressly mention them. The Court then rules that the mere existence of legislation can constitute an interference with the exercise of the right to privacy of the parties concerned:

> "Furthermore, in the mere existence of the legislation itself there is involved, for all those to whom the legislation could be applied, a menace of surveillance; this menace necessarily strikes at freedom of communication between users of the postal and telecommunication services and thereby constitutes an "interference by a public authority" with the exercise of the applicants' right to respect for private and family life and for correspondence."[4]

The European Court confirmed this reasoning in *Malone v. the United Kingdom*.[5] The Court considered that it was not necessary to further examine the applicant's complaint that his correspondence and telephone conversations had been intercepted for several years. The mere existence of a law and a practice that constitute and allow a system of secret surveillance of communications constitutes an interference with the exercise of the applicant's rights under Article 8 ECHR, quite apart from the measures actually used with respect to the applicant. In this case the Court also ruled that traffic data, i.e. data which does not relate to communication content, are also protected by Article 8 ECHR:

---

[3] ECHR 6 September 1978 (*Klass a.o.* v. *Germany*).
[4] ECtHR 6 September 1978 (*Klass a.o.* v. *Germany*) § 41.
[5] ECtHR 2 August 1984 (*Malone* v. *United Kingdom*) § 64.

> "[…] a meter check printer registers information that a supplier of a telephone service may in principle legitimately obtain, notably in order to ensure that the subscriber is correctly charged or to investigate complaints or possible abuses of the service. By its very nature, metering is therefore to be distinguished from interception of communications, which is undesirable and illegitimate in a democratic society unless justified. The Court does not accept, however, that the use of data obtained from metering, whatever the circumstances and purposes, cannot give rise to an issue under Art. 8. The records of metering contain information, in particular the numbers dialled, which is an integral element in the communications made by telephone. Consequently, release of that information to the police without the consent of the subscriber also amounts, in the opinion of the Court, to an interference with a right guaranteed by Art. 8."[6]

In *Weber and Saravia v. Germany*[7] and *Liberty v. the United Kingdom*[8] the European Court confirmed that non-targeted interception of telecommunications and subsequent selection based on key words or selection criteria fell within the scope of Article 8 ECHR. The Court repeated its finding that the mere existence of the legislation in question can constitute an interference with the exercise of the right to privacy of persons to whom the legislation may be applied.

In *Liberty* the Court emphasizes, moreover, that the existence of certain powers, in particular the powers to examine, use and store intercepted communications, constitutes an interference with the exercise of the applicants' rights.[9] In *Weber and Saravia* attention is drawn to the fact that statutory provisions making it possible to destroy data and the provisions preventing notification of the persons concerned also lead to the finding of an interference with the exercise of the applicants' rights under Article 8 ECHR.[10]

In *Weber and Saravia* the Court confirms the further finding that providing the intercepted data to others constitutes a separate interference with the exercise of Article 8 ECHR:

> "[…] the transmission of data to and their use by other authorities, which enlarges the group of persons with knowledge of the personal data intercepted and can lead to investigations being instituted against the persons concerned, constitutes a further separate interference with the applicants' rights under Article 8 […]."[11]

In *Kennedy v. the United Kingdom*[12] the Court repeats its reasoning of the aforementioned cases. Furthermore, the Court finds that in assessing whether there is an interference with the

---

6 Idem, § 84.
7 ECtHR 29 June 2006 (*Weber and Saravia* v. *Germany*), decision on admissibility.
8 ECtHR 1 July 2008 (*Liberty a.o.* v. *United Kingdom*).
9 ECtHR 1 July 2008 (*Liberty a.o.* v. *United Kingdom*), § 57.
10 ECtHR 29 June 2006 (*Weber and Saravia* v. *Germany*) decision on admissibility, § 79.
11 ECtHR 29 June 2006 (*Weber and Saravia* v. *Germany*) decision on admissibility, § 79.
12 ECtHR 18 May 2010 (*Kennedy* v. *United Kingdom*).

exercise of the right to privacy as a result of the mere existence of legislation permitting secret surveillance measures, the Court must have regard to the availability of any remedies at the national level to challenge the exercise of these powers.[13]

It can be concluded from the foregoing that in cases involving secret investigations by an intelligence and/or security service the Court will readily find interference with the exercise of the right to privacy.

3.1.2 Justification of the interference

Article 8(2) ECHR gives a rule about restricting the right to privacy:

> "There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security […]."

So interference with the exercise of the right to privacy is justified if the requirements mentioned in paragraph (2) are satisfied. The European Court has elaborated these requirements in its extensive case law on Article 8 ECHR. The main features are discussed below.

'in accordance with the law'

The requirement that the interference must be 'in accordance with the law' means first of all that the interference must have a basis in domestic law. The word 'law' must be interpreted broadly in this context. The Court understands the term law in its substantive sense, not its formal one.[14]

The European Court imposes two quality requirements on the domestic law in which the interference must have a basis: it must be accessible and foreseeable.[15] Accessibility means that the rules on which the infringing acts are based must have been adequately published or announced.[16] However, the accessibility of these rules need only be guaranteed to persons to whom the rules are specifically relevant.[17] The point of foreseeability of the law is that it must be sufficiently clear and precise. Because the risk of abuse of powers is inherent to secret investigations, the foregoing is all the more cogent where the technology available for use is

---

[13] ECtHR 18 May 2010 (*Kennedy* v. *United Kingdom*), § 124.
[14] ECtHR 26 April 1979 (*Sunday Times* v. *United Kingdom*) § 47; ECHR 24 April 1990 (*Kruslin* v. *France*) § 29; EXHR 24 April 1990 (*Huvig* v. *France*) § 28.
[15] ECtHR 26 April 1979 (*Sunday Times* v. *United Kingdom*) § 49; ECHR 25 March 1983 (*Silver a.o.* v. *United Kingdom*) § 85; ECHR 24 April 1990 (*Kruslin* v. *France*) § 27; ECHR 24 April 1990 (*Huvig* v. *France*) § 26.
[16] ECtHR 25 March 1983 (*Silver a.o.* v. *United Kingdom*) § 87; ECHR 26 March 1987 (*Leander* v. *Sweden*) § 53.
[17] ECtHR 28 March 1990 (*Groppera Radio AG a.o.* v. *Switzerland*) § 68.

continually becoming more sophisticated.[18] In assessing whether the criterion of foreseeability is satisfied, practices laid down in internal instructions may be taken into account to the extent that they have been made known to the person(s) concerned.[19]

According to the Court the degree of the required clarity and preciseness of the law depends on the particular subject matter. Rules in the context of national security, for example the power to intercept communications or to conduct secret investigations, cannot give individuals the same degree of clarity and preciseness as rules in other fields.[20] Rules in the context of national security often confer a certain measure of discretion on the public authorities. This is sometimes inevitable. The Court has held that with a view to the rule of law these rules must in such cases indicate the scope of discretion.[21] In addition, there must be sufficient safeguards in the legal system to protect individuals against arbitrariness.[22]

The criterion of sufficient safeguards against arbitrary interference by the public authorities requires in the first place that the law must in any case be so clear that individuals can understand in which circumstances and on which conditions the authorities may exercise a particular infringing power.[23] In addition, the Court attaches importance to the existence of adequate legal procedures so that alleged arbitrary interference can be challenged in court.[24]

In the aforementioned cases of *Weber and Saravia* v. *Germany* and *Liberty* v. *the United Kingdom* the Court specifically applied these basic principles to the challenged domestic law which permitted non-targeted interception of telecommunications and subsequent selection on the basis of key words and selection criteria. The Court mentions a number of minimum safeguards which the Court had developed in earlier judgments on targeted interception of telecommunications. These are the minimum safeguards that must be present to avoid abuses of power.

> "In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating

---

[18] ECtHR 29 June 2006 (*Weber and Saravia* v. *Germany*) decision on admissibility, § 93; ECHR 2 September 2010 (*Uzun* v. *Germany*), § 61.
[19] ECtHR 25 March 1983 (*Silver a.o.* v. *United Kingdom*) § 88; ECHR 26 March 1987 (*Leander* v. *Sweden*) § 51.
[20] ECtHR 2 August 1984 (*Malone* v. *United Kingdom*) § 67; ECHR 26 March 1987 (*Leander* v. *Sweden*) § 51.
[21] ECtHR 25 March 1983 (*Silver a.o.* v. *United Kingdom*) § 88.
[22] ECtHR 2 August 1984 (*Malone* v. *United Kingdom*) § 67.
[23] ECtHR 2 August 1984 (*Malone* v. *United Kingdom*) § 68; ECHR 24 Apr l 1990 (Kruslin/France) §§ 33 and 35; ECtHR 24 April 1990 (*Huvig* v. *France*) §§ 32 and 34.
[24] ECtHR 4 May 2000 (*Rotaru* v. *Rumania*) § 59.

the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed […]"[25]

In *Liberty* the Court states expressly that though it is true that these requirements were first developed in connection with powers targeted at specific individuals, there are no grounds that prevent the application of the same requirements to rules relating to more general powers.[26] Therefore, national legislation for non-targeted interception and selection must in any case include rules regarding the nature of the activities that may give cause to take the measure of interception, the categories of persons whose communications may be intercepted, a limitation on the duration of interception, procedures for examining, using and storing intercepted data, the precautions to be taken when communicating the data to other parties and the circumstances in which the data may or must be erased or destroyed.

'necessary in a democratic society'

The second requirement is that of necessity in a democratic society. This requires first of all that the interference must be based on a justified interest. According to the European Court the concept of 'necessity' must be interpreted neither too narrowly nor too broadly. In principle it is the task of the State itself to make an initial assessment whether the interference serves a justified interest.[27]

One element of the required necessity is that the interference must be proportionate to the protection of the aim which the interference is intended to achieve.[28] This means that the interference with the exercise of the right must be in reasonable proportion to the legitimate aim pursued. The interference may not be such as to cause the erosion of the essence of the right. And when a less infringing measure will suffice (also known as the principle of subsidiarity), the interference is not proportionate either.[29]

In keeping with the subsidiary nature of the Strasbourg mechanism, the State is allowed a certain margin of appreciation with regard to both necessity and proportionality.[30] In *Klass*, mentioned above, the Court expressly refers to this margin and finds that it is not for the Court to assess which measure should be taken to protect e.g. national security. This does not mean, however, that the State can simply adopt whatever measure it deems appropriate. The Court states in this judgment that whatever system of measures is adopted, adequate and effective guarantees

[25] ECtHR 29 June 2006 (*Weber and Saravia* v. *Germany*) decision on admissibility, § 95; ECHR 1 July 2008 (*Liberty a.o.* v. *United Kingdom*) § 62 and 63.
[26] ECtHR 1 July 2008 (*Liberty a.o.* v. *United Kingdom*) § 63.
[27] ECtHR 7 December 1976 (*in recent years*) par 48 and 49; ECtHR 26 April 1979 (*Sunday Times* v. *United Kingdom*) § 59.
[28] ECtHR 7 December 1976 (*Handyside* v. *United Kingdom*) § 49.
[29] ECtHR 2 October 2001 (*Hatton a.o.* v. *United Kingdom*) § 97.
[30] ECtHR 7 December 1976 (*Handyside* v. *United Kingdom*) §§ 48 and 49.

against abuse are required.[31] In subsequent judgments, too, the Court allows the State a fairly wide margin of appreciation in the context of the proportionality test in relation to taking measures in the interests of national security, provided there are adequate guarantees against abuse.[32]

In *Weber and Saravia* the Court likewise acknowledges the State's wide margin of appreciation in the area of national security. Referring to *Klass*, the Court goes on to find as follows:

> "Nevertheless, in view of the risk that a system of secret surveillance for the protection of national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there exist adequate and effective guarantees against abuse […]. This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them, and the kind of remedy provided by the national law […]."[33]

So the assessment whether adequate guarantees exist depends on all the circumstances of the case, including the nature, the scope and the duration of the power, the grounds on which the power may be exercised, the authorities that are competent to authorise, exercise and supervise the power, and the remedy available to individuals in the national legal system.

It may be concluded that the justification of the interference with the exercise of the right to privacy depends on the actual circumstances of the case. The Court reviews both the quality of the legislation that allows the interference with privacy and the necessity and proportionality of the exercise of the infringing power. Because the State has a fairly wide margin of appreciation with regard to both aspects for reasons of the protection of national security, the Court attaches great importance to the existence of adequate and effective guarantees against abuse.

The case law of the Court gives few starting points for assessing the extent to which the exercise of a power constitutes interference with the exercise of the right to privacy.

3.2 Protection of privacy in the Constitution

The Constitution's main rule on privacy is laid down in the first paragraph of Article 10, which contains a general provision that everyone shall have the right to respect for his privacy. This paragraph further provides that restrictions may be laid down by or pursuant to Act of Parliament. This means that the exact scope of protection of privacy is regulated in greater detail in other laws, such as the ISS Act 2002.

---

[31] ECtHR 6 September 1978 (*Klass a.o.* v. *Germany*) §§ 46 and 48-50.
[32] ECtHR 26 March 1987 (*Leander* v. *Sweden*) §§ 59 and 60; ECHR 2 August 1984 (*Malone* v. *United Kingdom*) § 81.
[33] ECtHR 29 June 2006 (*Weber and Saravia* v. *Germany*) decision on admissibility, § 106.

Article 13 of the Constitution contains a specific elaboration of part of privacy protection. It provides that the privacy of correspondence (§2) and of the telephone and telegraph (§2) is inviolable. Particularly the privacy of the telephone and telegraph is relevant to the present investigation. Restrictions on the privacy of the telephone and telegraph require the prior authorisation from the competent authority. The ISS Act 2002, for example, includes a provision that Sigint measures may only be taken after the minister concerned has given his permission to do so.

The privacy of the telephone and telegraph enshrined in Article 13 of the Constitution protects the sender of a communication transmitted via the telephone or telegraph against examination of the communication's content by the party entrusted with transmitting it or by any party who has access to the communication via the transmitter. Because persons sometimes become aware of the communication for technical reasons, the privacy rule also includes the prohibition to communicate the content of the communication to third parties. The privacy of the telephone and telegraph protects sealed communications. This means that the sender must have taken the necessary measures to keep the communication secret. The communication is only protected during its transportation. Everything falling outside the transmitting process and whatever is attributable to this process does, however, enjoy the protection of the general right to privacy.[34]

Traffic data, that is signals data relating to the transportation of communications, falls outside the scope of protection of the privacy of the telephone and telegraph, Traffic data is protected by Article 10 of the Constitution to the extent it can be considered to be personal data.

In 1997 a discussion arose about how the Constitution should regulate the protection of communications. The direct reason for this discussion was a statement by the minister of Justice that the privacy of correspondence did not protect e-mail. It was considered necessary also to protect communications by other means than those currently mentioned in the Constitution.

The government proposed an amendment of Article 13 of the Constitution which introduced the concept of 'confidential communications'.[35] It was aimed at using a technology-independent norm which would cover both existing and future means of communication. The proposed Article 13 would protect closed forms of communication both within and outside the transportation stage. The closed nature of a communication was to follow from the objectified will of the sender to share the communication exclusively with the addressee. The idea was that this will could be deduced from a certain measure of security. E-mail, for example would have to be encrypted.

The proposed amendment met with a critical reception. The Second Chamber of Parliament repeatedly amended the proposal. The First Chamber did not support it. The minister of the Interior then established a committee that was to issue recommendations on fundamental rights

[34] *Parliamentary Papers II* 1975/76, 13 872, nos. 1-5.
[35] *Parliamentary Papers II* 1997/98, 25 443 nos. 1-2.

in the digital age. In 2000 the committee, chaired by professor Franken, presented a report which among other things contained a recommendation to amend Article 13.[36] This proposal likewise introduced the concept of confidential communication, defined as a communication for which the sender, on the grounds of his wish for confidentiality, has chosen a means of communication giving him a reasonable expectation of confidentiality.

In response to the report the government came with a new amendment proposal which endorsed the greater part of the recommendations of the Franken Committee.[37] The government proposal, however, restricted the right to confidential communication to communications entrusted for transportation to a third party, so that it applied only in the transportation stage.

Both the recommendations of the Franken Committee and the government proposal met with fierce criticism. Not only did opinions differ about the juristic object, but the theoretical elaboration of the right and the possible restrictions also gave rise to discussions. In professional literature the 'confidential communication' approach of the former proposals was opposed by advocates of the transportation approach.[38] The latter approach is based on the principle that constitutional protection should not be given to the confidential nature of communication content, but to the communication channel. The rationale of this view is that senders of communications must be able to rely on it that communications can be safely entrusted to a transporter for transportation, regardless of the nature of the communication. It is precisely this entrustment to another party that implies extra vulnerability for the sender. According to this approach, the confidentiality of communication extends to cover traffic data as well.

In the 2007 coalition agreement, the fourth cabinet headed by Balkenende unfolded its plans for strengthening the Constitution, a subject on which a State Committee was to issue recommendations. The State Committee on Constitutional Reform was established by royal decree of 3 July 2009. This committee, too, faced the question whether Article 13 of the Constitution was to protect communication means or communication content. The State Committee on Constitutional Reform recommended that Article 13 of the Constitution be formulated thus, that everyone has the right to confidential communication, regardless of the means used to communicate.[39] The cabinet's reaction to the report has been long in forthcoming.[40]

In the ongoing discussion since 1997, privacy of the telephone and telegraph has been replaced by a more comprehensive confidentiality of communication, based on confidentiality of either the communication or the transportation of the communication. The ultimate outcome of the

---

[36] Report of the Committee on Fundamental Rights in the Digital Age, 24 May 2000.

[37] *Parliamentary Papers II*, 2000/01, 27 460 no. 1.

[38] See i.a. E.J. Dommering, "De nieuwe Nederlandse Constitutie en de informatietechnologie", *Computerrecht* 2000-2004, p. 177-185; L.F. Asscher, "Trojaans hobbelpaard. Een analyse van het rapport van de commissie Grondrechten in het Digitale Tijdperk", *Mediaforum* 2000-7/8, pp. 228-233.

[39] Report of the Government Committee on Constitution Reform, November 2010, pp. 85-88.

[40] *Parliamentary Papers II* 2010/11, 31 570, no. 19.

discussion will have consequences for the manner in which the protection of communication will be regulated in specific laws; and therefore also for how the powers to take Sigint measures will be regulated in the ISS Act 2002. Questions may be raised, for example, about the position taken by the legislature when drafting the ISS Act 2002, that non-targeted interception does not infringe privacy, in particular not the privacy of the telephone and telegraph, as long as data content is not examined yet (see section 4.2). If one takes the approach that the privacy of the telephone and telegraph relates to the protecting the confidential transportation of communications, it can be said that the right to confidential transportation is infringed as soon as a communication is intercepted and that there has therefore been infringement of the privacy of communication as protected by the Constitution.

For DISS (and GISS) it is desirable that the discussion described above will lead to a clear decision on the constitutional protection of communication. Up to now, however, the decision-making process about amending Article 13 of the Constitution has stagnated. The current Article 13 of the Constitution protects closed communications during their transportation. This interpretation of the privacy of communication was in fact the starting point for drafting the ISS Act 2002 and the manner in which the powers to use Sigint have been laid down in the Act. For the purposes of this review report the Committee has followed this interpretation.

4. The infringing special powers

4.1 The power to take the measure of targeted interception

Article 25(1), ISS Act 2002, confers power on DISS to intercept, receive, record and tap, in a targeted process, any form of conversation, telecommunication or data transfer by a computer system while using a technical device, regardless of where this takes place. The legislature has opted to draft this provision in rather general terms so that it can be held to include for example electronic communication.[41] The first paragraph further confers power to undo the encryption of the conversations, telecommunications or data transfer.

Article 25 does not distinguish between cable-bound and non-cable-bound communication. Consequently, targeted interception by DISS of both forms of communication is permitted. The Sigint department exercises the power with respect to non-cable-bound communication. This refers in particular to *High Frequency* (HF-) radio communications.

In many cases[42] it is evident that the exercise of the power of targeted interception of *inter alia* HF traffic infringes the right to privacy protected by Article 8 ECHR. The severity of the

[41] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 41.

[42] Military data traffic is an exception on this point.

infringement depends on the actual circumstances of the case and is comparable to the severity of the infringement of privacy caused by telephone tapping. In this context account must be taken of the fact that HF traffic usually concerns communications between public services or organisations, which are less privacy sensitive than if telephone communications between two individuals are tapped.[43] This depends, however, because it is impossible to determine the subject of the communications in advance. It can be argued, moreover, that because of the fact that communication lines in a public service or organisation are used by several persons, the privacy of a greater number of individuals is infringed than would be the case with telephone taps against individual targets. DISS exercises the power of targeted interception with respect to individuals as well.

The power of targeted interception may only be exercised if the minister of Defence has given the director of DISS permission to do so (Article 25(2)). If the communication or data transfer does not take place at or using locations in use by Defence, the Defence minister's permission to exercise the power must be given with the agreement of the minister of the Interior and Kingdom Relations (paragraph (3)).[44] Article 25(2) formulates two exceptions to this requirement. DISS does not require the agreement of the minister of the Interior and Kingdom Relation for targeted interceptions of non-cable-bound telecommunications coming from or intended for a foreign country (mainly HF radio traffic). No permission is required at all for targeted interceptions of military data traffic since this is a "continuous activity" which "is evidently necessary for the proper performance by DISS of its tasks and with respect to which imposing the requirement of permission has no added value whatsoever"[45]

The legislative history contains an explanation that in actual practice military data traffic is identified as follows. Because of the nature of their mission, military units using radio communications will seek to disguise their operation or manoeuvres. Radio links used for command purposes will be designed to disclose as little information as possible. In order to achieve this, the military uses procedures and connection protocols that differ from the regular procedures and protocols used internationally. Knowledge of these military procedures and protocols is collected by analysing them. This knowledge, together with geo-location of radio transmitters and measurement of transmitted signals, makes it possible to identify military data traffic.[46]

---

[43] The ECtHR has ruled that activities of a professional or business nature can also be considered to fall within the scope of private life. ECtHR 25 October 2007 (*Van Vondel* v. *Nederland*), § 48:"The Court reiterates that the term "private life" must not be interpreted restrictively. In particular, respect for private life comprises the right to establish and develop relationships with other human beings; furthermore, there is no reason of principle to justify excluding activities of a professional or business nature from the notion of "private life". There is therefore a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"." See also ECtHR 2 September 2010 (*Uzun* v. *Germany*), §§ 43-48.

[44] The bill proposing the Post-Madrid measures replaced the agreement requirement with respect to this Article by the requirement that the minister of the Interior and Kingdom Relations or the head of GISS on his behalf must give his consent. This bill has meanwhile be withdrawn.

[45] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 20-21.

[46] Idem.

Pursuant to Article 25(4), ISS Act 2002, an application for permission submitted by the director of DISS to the minister of Defence must in any case state:

a) the power to be exercised and, if applicable, the number;
b) data concerning the identity of the person or organisation against whom or which the power will be exercised;
c) the reasons for the application.

If the application is not for interception based on a number as referred to under a) but for interception based on a technical characteristic (frequency), then according to the legislative history the technical characteristic need not be mentioned. Persons and organisations usually communicate at several and changing frequencies. The requirement of stating the technical characteristic would in practice have the result that DISS would repeatedly have to submit new or supplementary applications. This would create an undesirable and unworkable situation.[47]

According to the legislative history the reasons stated for the desired exercise of the power must not only make it clear why the person or organisation is being investigated having regard to the mandate of the service (necessity), but also why the service particularly wishes to take the measure indicated in the application and why another and – in view of the circumstances of the case – less infringing measure will not suffice (subsidiarity). The information provided in the application must enable the minister to take a responsible decision whether or not to grant permission. Permission is granted for a period of up to three months and may be renewed each time. According to the legislature this means that if it is deemed necessary to continue exercising the power in question after the expiry of the three-month period, the head of the service must again apply for permission.[48]

Paragraph (6) gives rules for cases in which the identity data of the person or organisation against whom or which the power will be exercised is not known at the time the application for permission is submitted to the minister. In those cases permission will only be granted subject to the condition that the data in question will be supplied as soon as possible.

Section 7.2 below describes how DISS exercises the power of targeted interception in actual practice.

4.2 The power to take the measure of non-targeted interception and subsequent selection

Pursuant to Article 27(1), ISS Act 2002, DISS is authorised, using a technical aid, to intercept

[47] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 18-19.
[48] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 43.

by non-targeted interception and to record non-cable-bound telecommunications. 'Non-targeted' interception means that the interception is not directed at communications originating from a specific person or organisation or linked to a technical characteristic, but that, for example, all data traffic transmitted via a specific satellite channel is, as it were, plucked from the air and then stored on computers.[49] Article 27 does not confer the power to take the measure of non-targeted interception of cable-bound telecommunications.

Pursuant to Article 27(2) , ISS Act 2002, no permission as referred to in Article 19 is required for exercising the power of non-targeted interception. At that stage the content of the telecommunications is not examined yet so that according to the legislature there is no infringement yet of privacy, in particular not of the privacy of the telephone and telegraph. According to the legislature such infringement does not occur until the moment the data is selected. With respect to this power the legislature observed that it saw little added value in imposing the requirement of permission. Such a requirement would only relate to the satellite channel transmitting the data to be intercepted and would have hardly or no meaning regarding content.[50]

DISS cannot do anything with the intercepted and recorded telecommunications, except that it may undo any encryption of the data (Article 27(1), ISS Act 2002). The possibilities for selecting telecommunications are laid down in paragraphs (3) to (6) of Article 27, ISS Act 2002. These provide for the possibility of selection on the basis of (a) data regarding the identity of a person or an organisation, (b) a number or a technical characteristic, and (c) key words relating to a specified subject (paragraph (3)).

Selection of data under (a) or (b) constitutes 'targeted' selection of data. The legislature therefore provided that this must be governed by the same rules as those governing targeted interception pursuant to Article 25, ISS Act 2002: the head of the service must first apply for the minister's permission before data may be selected using any of the criteria mentioned. The application for permission must satisfy a number of minimum requirements, the same as those applying to targeted interception. Article 26(4) provides with regard to selection based on – briefly stated – name or number that the application must in any case contain the information referred to under (a) or (b) on which the selection is to be based, and also the reason why selection is necessary. Permission is granted for a period of three months and may be renewed each time (paragraph (4)).[51]

It is evident that the exercise of the power of selection results in infringement of the right to privacy as protected by Article 8 ECHR. The severity of the privacy infringement resulting from the 'targeted' selection of data depends on the actual circumstances of the case and cannot be simply equated with the severity of the infringement of privacy by the measure of telephone

[49] Idem, p. 44.
[50] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 44.
[51] Idem, pp. 44-45.

tapping. One factor playing a role is that selection after non-targeted interception does not result in all communications of a specific person or organisation being intercepted and recorded, but only those found in the bulk and therefore intercepted 'by chance'. This does not change the fact that selection after non-targeted interception can in fact be severely infringing. When a service can pick up the communications of many different satellites and has the capability to filter the communications bulk, it is potentially very well possible to intercept all communications from a specific person or organisation. The difference with telephone tapping is the moment of examining communication content. In the case of telephone tapping this usually happens *real time*, i.e. at the time the communications are transmitted, while in the case of selection after non-targeted interception the service does not examine communication content until later. This distinction is rather flimsy too, though, since the service frequently does not listen to the telephone tap recordings until later, while in the case of selected communications it is not always certain that the addressee has already read a communication at the time DISS examines its content.[52]

A different regime applies to the selection of data under (c) (key words): permission may be granted for a maximum period of one year and may be renewed every year. The legislature chose a different regime for the selection of data under (c) because it does not involve any targeted search for data relating, for example, to a specific, real person whose privacy may be directly infringed. It is simply a selection of data which may be important for investigations of DISS in a general sense, for example the proliferation of chemical weapons.[53]

An application for permission must in any case contain a detailed description of the subject and the reason for selection (paragraph (5)). According to legislative history these requirements safeguard that the minister has the necessary understanding of the matter when deciding whether to grant permission. The key words relating to the subjects have no added value for such understanding. As a rule, a list of key words relating to a subject will consist of (combinations of) specific technical terms and designations in various languages. Since the key words may change frequently, the law also provides that the key words may be determined by the head of the service or by an officer designated by him on his behalf (paragraph (6)). Lists are prepared in such a way as to result in optimal use of the selection system to find the desired information. In practice, lists of key words will be prepared by analysts who are subject experts. The power to determine the key words is, however, vested in the head of the service or an officer designated by him.[54] Under the DISS Submandating and Authorisation Decree 2009 the head and the analysts of the Sigint department are authorised to determine key words.[55] It was further decided in the legislative history that the power of selection under (c) must be exercised very selectively (mainly restricted to satellite traffic) and with restraint.[56]

---

[52] An e-mail communication, for example, can be left unread in the inbox for a long time.
[53] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 45.
[54] *Parliamentary Papers II* 2000/01, 25 877, no. 14, pp. 33-34.
[55] *Official Gazette* no. 7168, Article 3(1), subparagraphs (e) and (j).
[56] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 45.

Article 27(7), ISS Act 2002, provides that one or both Chambers of the States-General and the Review Committee will be confidentially informed about any grants of permission to select on the basis of key words, and also of the subject and reason for taking the measure of selection.

Article 27(8), ISS Act 2002, provides that permission for the selection by DISS of data from telecommunications having both their origin and destination in the Netherlands will be granted by agreement with the minister of the Interior and Kingdom Relations.

It is not excluded that data not selected on the basis of the selection criteria, whose content the service is therefore unable to actually inspect, may nevertheless contain relevant information which on the basis of selection criteria to be determined subsequently would be selected after all. Such subsequently determined selection criteria may follow from information derived from other sources of a service or be derived from data intercepted and recorded at a later time.[57]

An example from the legislative history. When searching on the basis of key words, the service sometimes selects communications which show that a ship is carrying chemicals or goods that can be used for the production of weapons of mass destruction, though it is not clear from the intercepted communications who is the supplier or the buyer of the goods. Using new key words derived from the intercepted communications, the service can then examine whether it is possible to find supplementary information about supplier and buyer in data traffic it had already intercepted before, but had not selected. Sometimes, moreover, it is possible to establish in this way whether the relationship between supplier and buyer has already existed for some time. If the service should have to destroy the data originating from telecommunications intercepted and recorded pursuant to Article 27(1), ISS Act 2002, immediately after the first selection, it would not be able to do a subsequent selection – as outlined above – giving a possibility of further enlarging and supplementing information that is relevant to current investigations. The legislator considered this an undesirable situation. Subject to conditions, the service should have the opportunity to do such a subsequent selection, which therefore implies a certain period of retention of the data in question.[58]

Pursuant to Article 27(9), ISS Act 2002, data obtained from non-targeted interception which has not been selected may be retained for further selection purposes for up to one year. This is made subject to two conditions. Selection may only take place in the context of an investigation based on a reason as referred to in paragraph 4(b) or in relation to a subject as referred to in paragraph 5(a) in respect of which permission had been granted at the time the data in question was intercepted and recorded (paragraph 9(a)). The legislature did not consider it advisable for such data to become available for selection in the context of investigations by a service not yet ongoing at the time the telecommunications were intercepted and recorded; the reason for this is that the telecommunications were intercepted for the purposes of investigations that

[57] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 26-27.
[58] Idem.

were ongoing at the time of interception. In addition, further selection must also be urgently necessary for the proper execution of the investigation concerned (paragraph 9(b)). According to legislative history, these conditions were included because unrestricted and unconditional further selection of intercepted data is unlawful. It is barred by Article 8 ECHR.[59]

In connection with the Committee's recommendation to include a statutory provision allowing an extension of the retention period of Article 27(9)[60], an amendment was included in the bill proposing the post-Madrid measures. The amendment provided for an extension of the period from one year to three years.[61] The bill has by now been withdrawn.

Article 27(10), ISS Act 2002, provides that paragraph (9) applies by analogy to data that has not yet been decrypted, with the proviso that the one-year retention period does not begin to run until the time of decryption.

Section 8.3 below will describe how DISS exercises the power of selection after non-targeted interception in actual practice.

4.3 The power of searching

Article 26, ISS Act 2002, regulates interception and recording of non-cable-bound telecommunications having their origin or destination in other countries, using a technical device and based on a technical characteristic for the purposes of exploring the communications. This is the power of 'searching'. Searching is used to try and find out what is the nature of telecommunications sent at particular frequencies (technical characteristics) and who is the person or organisation sending the telecommunications (sender identity). It includes surveying HF radio traffic and satellite communications. Only a small part of this traffic is relevant to the performance by DISS of its tasks. Searching is therefore also aimed at establishing whether the traffic comprises telecommunications which the service needs to examine for the proper performance by DISS of its tasks. In order to be able to establish this, the content of the telecommunications must be examined. The legislature has expressly permitted this in Article 26(1), ISS Act 2002.[62] Pursuant to Article 26(1), ISS Act 2002, moreover, the power to search also includes power to undo encryption of the telecommunications.

A distinction must be made between searching for the purpose of targeted interception and searching for the purpose of non-targeted interception. These concern searching of HF radio traffic and searching of satellite communications, respectively.

---

[59] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 26-27.

[60] Review report no. 5A on the investigation by DISS into the proliferation of weapons of mass destruction and their means of delivery, adopted by the Committee on 10 August 2005, available at www.ctivd.nl, section 4.2.5.

[61] *Parliamentary Papers II* 2005/06, 30553, no. 3, p. 30.

[62] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 21-22.

4.3.1 Searching for the purpose of targeted interception

When searching HF radio traffic, the searcher examines random samples of communication content and follows transmissions for brief periods only. The activity cannot be compared with tapping. In the legislative history, searching HF radio traffic was compared with turning a radio knob to find out which organisation is transmitting at which frequency.[63] The minister of Defence explained at the time that there is a very essential difference between searching for the purpose of knowing what is available on the market, so that information will be available at the very moment it has to be obtained for a specific purpose, and targeted collection of information. He stated that when a service is really listening in and the communications are stored, translated and placed in a broader context, the service is purposively gathering information for a specific operation. This falls under the permission regime. Merely collecting possibilities falls under the regime of 'turning buttons'.[64]

Searching HF radio traffic supports the process of targeted interception (pursuant to Article 25) because it makes clear whose communications are transmitted at which frequencies. Essentially, it serves to map out certain sections of the air waves. An example. When DISS wants to intercept the communications of organisation X, it can find out by searching which frequency or frequencies organisation X is using for its communications. Subsequently – with the minister's permission – DISS can exercise the power of Article 25 and actually intercept these communications by targeted interception. So searching serves to enable DISS to carry out targeted interception (at which frequency does organisation X communicate?) or to optimize it (one frequency was already known, but organisation X turns out to be using two other frequencies as well). The difference between Article 25 and Article 26 lies in the stage preceding targeted interception.[65]

It is not permitted to follow a transmission longer than is strictly necessary to establish the identities of the communicating persons or organisations, since then the searching would turn into a non-permissible form of targeted examination of communication content.[66]

When DISS is searching HF radio traffic and comes across communications the service would like to use, it may in principle do so. In that case the use of the communications must be necessary for the proper performance of its tasks. In addition, the requirements of proportionality and subsidiarity must be met. Pursuant to Article 26(4), ISS Act 2002, DISS must submit an application to the minister and must suspend actually using the information until the minister has granted permission. In the meantime, however, DISS may continue intercepting and recording the communications, but may not further examine their content. If the minister refuses permission, then pursuant to Article 26(5), ISS Act 2002, the intercepted and recorded communications must be destroyed immediately.

---

[63] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 30.
[64] *Parliamentary Papers II* 2000/01, 25 877, no. 72, pp. 4-6.
[65] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, pp. 21-22.
[66] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 35.

4.3.2 Searching for the purpose of non-targeted interception

Searching satellite communications is a completely different story. It is not possible for DISS to intercept and record all satellite communications travelling the air waves, it has to make choices. Searching serves the purpose of optimizing its choices. By searching, for example, DISS discovers from which region the communications via a specific satellite channel originate, to which region the communications are sent and the type of communication (voice, fax, internet, etc.).

Searching satellite communications supports the process of non-targeted interception (under Article 27) through the fact that searching enables DISS to examine which are the satellite channels used for transmitting communications that may be relevant to the performance by DISS of its tasks. Searching enables DISS to limit the satellite traffic it will intercept and record to specific channels.[67]

After DISS has chosen a number of satellite channels and has intercepted and recorded the communications transmitted via those channels, it may - with the minister's permission - exercise the power of Article 27(3), ISS Act 2002. From the large volume of satellite communications (the bulk) that has been intercepted and recorded DISS may then select the communications DISS needs to examine for the proper performance of its tasks.

4.3.3 Examining content

The second paragraph of Article 26, ISS Act 2002, provides that no permission as referred to in Article 19 is required for searching. The legislative history of Article 26, ISS Act 2002, shows that this is because the nature of the activity is partly comparable to non-targeted interception and recording of non-cable-bound telecommunications pursuant to Article 27, ISS Act 2002. Its non-targeted nature does not so much follow from the fact that the service scans various frequencies or satellite channels, but rather from the fact that it does not know in advance which communications (type and content) from whom (which person or organisation) it will come across in the process.[68] The legislator observed, moreover, that a permission requirement would have no added value. Searching does not target a specific person or organisation. Neither is it possible to name a specific reason for searching (cf. Article 25(4)(c), ISS Act 2002). This means that the permission requirement would only cover the general purpose of searching, as stated in Article 26(1), ISS Act 2002. [69]

In order to be able to establish the identity of the sender and the relevance of the communications to the performance by DISS of its tasks, DISS must examine the content of the telecommunications. In Article 26(1), ISS Act 2002 the legislature expressly permits DISS to do so. The legislative history

[67] *Parliamentary Papers II*, 2000/01, 25 877, no. 59, p. 12.
[68] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 22.
[69] Idem, p. 23.

shows that examining communication content must be done by random sampling and for a brief duration. Thus, examining communication content is not itself an aim, it is merely a tool.[70] It is not permitted to follow a transmission longer than is strictly necessary to establish the identities of the communicating persons or organisations, since in that case the searching would turn into a non-permissible form of purposive examination of communication content.[71]

In the legislative history the position was taken that the privacy of the telephone is not infringed unless listening in to a telephone conversation is aimed at gaining knowledge of the content itself. If note is taken of the content of a telephone conversation purely as a brief element of an investigation into the identity of the persons or organisations communicating with each other, this was said not to constitute infringement of the privacy of the telephone. Rather, it was considered comparable to the examination of traffic data. According to the legislature, such an examination can be held to infringe the right to privacy as enshrined in Article 10 of the Constitution, but not the privacy of the telephone and telegraph as enshrined in Article 13 of the Constitution.[72] The legislature has also made the comparison between searching and listening-in to telephone conversations by providers of telecommunication networks and services for the purposes of establishing whether there is a proper connection. It would go too far, so it was held, to interpret the privacy of the telephone so broadly that such technical monitoring and repair activities, which inevitably entail overhearing bits of a conversation, would also have to be considered infringement.[73]

It is the opinion of the Committee that the legislature, by taking this position, ignores the fact that searching is in fact directed at communication content. Based on content, searching is used to try and establish the identity of the sender and the communication's relevance to the performance by DISS of its tasks. This is expressly not the case in an investigation of traffic data, during which no note is taken of any communication content at all. The comparison with technical monitoring and repair activities by providers of telecommunications networks and services does not hold either, since in those cases taking note of content is not an intended result of the activities. The activities are not aimed at this.

The fact that searching includes only a brief examination of communication content and is not directed at gaining knowledge of the full content of a communication likewise does not change the fact that the privacy of the telephone and telegraph as enshrined in Article 13 of the Constitution is indeed infringed. It is infringed regardless of the different interpretations given to the object and scope of the fundamental right (see section 3.2). The aforementioned circumstances can only play a role in assessing the severity of the infringement. If one compares searching with a postman who opens an envelope and, after briefly glancing through the purport of the enclosed

[70] *Parliamentary Papers II* 2000/01, 25 877, no. 14, pp. 36-37.
[71] Idem, p. 35.
[72] Idem.
[73] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 23.

letter, reseals it, it is again not justified to conclude that the privacy of correspondence has not been infringed.

This opinion of the Committee leads to the conclusion that the exercise of the power of searching should be preceded by authorisation as referred to in Article 13 of the Constitution. It was described above, however, that the legislative history contains the observation that a permission requirement would have no added value. Searching was said not to be directed at a specific person or organisation. Nor would it be possible to state a specific reason for searching.[74] The legislature therefore considered it hardly worthwhile to require authorisation which would cover the general purpose of searching. The power of searching is, however, included in the ISS Act 2002 as a *special* power. This means that the exercise of the power must satisfy the requirements of necessity, proportionality and subsidiarity.

As was discussed in section 3, metadata does not fall under the current privacy of the telephone and telegraph, but it does form part of privacy. To the extent that metadata can be deemed to be personal data it falls under the protection of Article 10 of the Constitution. The European Court has also placed metadata within the scope of protection of privacy as enshrined in Article 8 ECHR. This means that restraint must be exercised in processing metadata. Metadata relating to the identity of a communicating person or organisation may only be processed if this is necessary for the proper performance by DISS of its tasks (Article 26(3), ISS Act 2002).

Section 7.4 will describe how DISS exercises the power of searching in actual practice.

5. Assessment framework of the ISS Act 2002

The special nature of the aforementioned powers of DISS lies among other things in the fact that they are inherently secret, particularly as far as their actual exercise is concerned. This does not mean, however, that they should not be regulated, quite the contrary. Article 8 ECHR and the case law on the subject developed by the ECtHR prescribe regulation. This has resulted among other things in the requirements of necessity, proportionality and subsidiarity embodied in the ISS Act 2002.

5.1 The criterion of necessity

Article 12(2), ISS Act 2002, provides that data may only be processed for a specific purpose and only to the extent necessary for the proper implementation of the Act or the Security Screening Act. The requirement of necessity applies to all activities carried out by DISS in the performance of its tasks.

[74] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 23.

The requirement of necessity is laid down specifically with respect to the exercise of special powers in Article 18, ISS Act 2002. Special powers may only be exercised to the extent necessary for the proper performance of the tasks of Article 7(2) under (a), (c) and (e). In the Act, these tasks are described as follows:

> "In the interests of national security the Defence Intelligence and Security Service has the following tasks:
> (a) conducting investigations:
> 1°. into the potential and the armed forces of other powers, to further the appropriate composition and effective use of the armed forces:
> 2°. into factors that influence or may influence the maintenance and promotion of international legal order to the extent the armed forces are involved or can be expected to be involved therein;
> […]
> (c) conducting investigations necessary to take measures:
> 1°. to prevent activities aimed at harming the security or preparedness of the armed forces;
> 2°. to promote the proper organisation of mobilising and concentrating the armed forces;
> 3°. to promote the undisturbed preparation and deployment of the armed forces as referred to in subparagraph (a). at 2°.
> […]
> (e) conducting investigations relating to other countries, regarding subjects having military relevance that have been designated by the Prime Minister, Minister of General Affairs, in agreement with the Ministers involved;"

The (a) task of DISS is the task of intelligence gathering by the service. The task laid down in subparagraph (a), at 1°, has its origin in the former ISS Act dating from 1987 and relates mainly to the classic general defence tasks of the armed forces. When the Act was amended in 2002, a new element was added to the (a) task. The task laid down in paragraph (a), at 2°, is a direct consequence of the new mandate of the armed forces after the end of the Cold War, which had the result that the need for intelligence also came to be directed towards maintaining and promoting international legal order. This task mainly concerns investigations for the purposes of carrying out international crisis management operations and peace operations. This means that DISS must be able to gather intelligence about the security situation in countries in which the Netherlands carries out such operations, often in the context of an alliance, or in countries in which according to reasonable expectation the Netherlands will be asked to participate in such an operation.[75]

DISS' (c) task concerns the conduct of investigations for counterintelligence and security

[75] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 12.

purposes. This is about safeguarding the security and preparedness of the armed forces and conducting investigations into potential threats to this security and preparedness, such as espionage, sabotage, subversion and terrorism. Investigations falling under the (c) task focus on actual as well as potential threats to the armed forces and consequently to national security.[76]

DISS' (e) task is the foreign intelligence task. This task concerns investigations of other countries with respect to subjects having predominantly military relevance which have been designated by the Prime Minister in agreement with the minister of Defence and the minister of the Interior and Kingdom Relations. There is an overlap between DISS' activities for the purposes of performing the (e) task and a significant part of its responsibility for the (a) task. For example: a subject initially designated exclusively under the foreign intelligence task may at some point come to be included in the intelligence needs of the ministry of Defence and be given priority under DISS' (a) task. The reverse may happen, too.

There need not always be an actual *threat* to national security for an investigation to be conducted in the context of the (a) task of DISS. The mere *interest* of national security is sufficient ground for DISS to conduct an investigation as part of performing its (a) task. As regards the (e) task, in principle any subject involving the interests of national security can be a subject that is designated and must be investigated by DISS.[77]

The question arises whether a national security interest is also sufficient ground for exercising special powers for the purposes of performing the (a) task and the (e) task. Case law of the ECtHR shows that secret infringing activities of intelligence and security services may be justified even if no *actual* harm is being done to national security. According to the ECtHR there must at the least be a possibility of national security being harmed, in other words *potential* harm to national security. If no harm to national security is to be expected at all, an infringement of privacy cannot be justified.[78]

In its investigations into the implementation of Articles 25 and 27, ISS Act 2002,[79] and into the foreign intelligence task[80], the Committee explained this line of case law and its significance for GISS. In those investigations the Committee established that special powers may only be exercised in the context of investigations of matters which may *potentially* lead to harm being done to national security. Assessing how the harm will eventually materialize is more difficult in the context of the foreign intelligence task than in the context of the security task. This is due

---

[76] See also review report no. 25. The conduct of DISS with respect to two suspended employees, *Parliamentary Papers II* 2009/10, 29 924, no. 59 (appendix), available at www.ctivd.nl, section 3.2.

[77] *Parliamentary Papers II* 1997/98, 25 877, no. 3, pp 10-11.

[78] See i.a. ECtHR 6 September 1978 (*Klass a.o.* v. *Germany*) and ECtHR 26 March 1987 (*Leander* v. *Sweden*).

[79] Review report no. 19. The application by GISS of Article 25 of the ISS Act 2002 (wiretapping) and Article 27 of the ISS Act 2002 (selection of non-targeted interceptions of non-cable-bound telecommunications, *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), available at www.ctivd.nl.

[80] Review report no. 26. The lawfulness of the performance by GISS of the foreign intelligence task, *Parliamentary Papers II* 2010/11, 29 924, no. 67 (appendix), available at www.ctivd.nl.

to the fact that it is often only in the fairly long term that the international developments and political intentions investigated in the context of the foreign intelligence task will have a possible adverse effect on national security.

The Committee takes the same line with respect to the exercise of special powers in the context of the (foreign) intelligence task of DISS. DISS should specify the possible harm to national security when it exercises special powers in the context of the (a) task and the (e) task.

One element of the necessity requirement applying to the exercise of special powers is not only laid down in Article 18, ISS Act 2002, but also in Article 32 of the Act. This Article provides that DISS must immediately cease exercising a special power if the objective for which the power was exercised has been achieved. This means that prior to exercising a special power DISS must have an objective for which it wishes to exercise the special power and that there must be an expectation that the information obtained by exercising the special power will contribute to achieving the objective. After commencing exercising the special power, DISS must examine whether the information obtained does in fact contribute to the objective. If this is not the case, it must cease exercising the special power. When applying for permission to continue exercising a special power DISS must give express attention to the information obtained by exercising the special power and its added value for the investigation.

5.2 The requirements of subsidiarity and proportionality

Article 31(1), ISS Act 2002, provides that a special power may not be exercised unless the intended information cannot be collected or cannot be collected in time by other means without exercising a special power. These other means are the use of public sources or sources of information which DISS has been granted authority to access, such as police registers or the municipal personal records database. If DISS can collect the desired information by using these sources, it is not necessary to exercise a special power. The assessment whether this is the case must be made before making the application for permission to exercise a special power.

According to the legislative history, inability to collect information or to collect it in time by the two aforementioned means includes a situation of serious doubt about the completeness or reliability of the information DISS has been able to obtain by those two means. The conclusion that DISS cannot collect information in time by these means depends (among other things) on the time pressure to eliminate a certain threat. It is self-evident that the pressure of time must be great to justify a decision not to consult the sources of information referred to in Article 31(1), ISS Act 2002.[81]

[81] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 52.

In the ISS Act 2002, the requirement that the infringement resulting from the exercise of a power must be as slight as possible – also known as the requirement of subsidiarity – is laid down in Article 31(2) and in Article 32. Article 31(2) provides that the service may only exercise the power that will cause least harm to the person involved compared to other available powers, having regard to the circumstances of the case, including the seriousness of the threat to the interests to be protected by a service. This rule is also included in Article 32, ISS Act 2002, which provides among other things that a service must cease exercising a special power if the exercise of a less infringing power will suffice.

The package of special powers available to DISS cannot be simply arranged in a hierarchical structure based on the degree to which the rights of the party concerned are infringed. The legislature has, however, differentiated the levels of permission required for the exercise of special powers. A higher level of permission may imply more serious infringement of the rights of the party concerned. This means that targeted interception (Article 25, ISS Act 2002) and selection after non-targeted interception (Article 27, ISS Act 2002) can be considered the most seriously infringing powers, because only the minister of Defence has authority to grant permission to exercise these powers. This follows naturally from the protection of the privacy of the telephone and telegraph by Article 13 of the Constitution. Permission to exercise other powers, such as surveillance or the deployment of agents, may be granted at a lower level through mandating, so that these special powers can be considered to be less infringing.

The infringement severity is mainly determined, however, by the practical and technical specifics of the exercise of a special power and by the duration of, and the information obtained by its exercise. If, for example, a frequency is intercepted for a short time only or if the selection of non-targeted interceptions does not yield a single hit, the actual infringement is less severe than when DISS retrieves a person's telephone traffic records every month for a whole year. This does not change the fact, though, that even if the special power is only used for a short time and the yield is nil, there still is infringement. It will have to be assessed in each individual case how severe the infringement is and whether the requirement of subsidiarity is met. The reasons given for the exercise of a special power and the reasons given for a renewed period of exercising the power must clearly show that such an assessment has been made.[82]

The requirement of proportionality means that the infringement of the rights of third parties must be reasonably proportionate to the objective served by the infringement. In the ISS Act 2002 this requirement is expressed in Article 31, which provides that a special power may not be exercised if its exercise would cause disproportionate harm to the party concerned compared to the intended objective (paragraph 3) and that the exercise of a power must be proportionate to the intended objective (paragraph 4). So the interests of DISS in exercising the special power

[82] See also review report no. 19. The application by GISS of Article 25 of the ISS Act 2002 (wiretapping) and Article 27 of the ISS Act 2002 (selection of non-targeted interceptions of non-cable-bound telecommunications, *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), available at www.ctivd.nl, section 4.2.

must be balanced against the interests of the target of the exercise of the special power. The interests of the person concerned include in any case the right to protection of his privacy, but may also comprise other rights.[83] The proportionality assessment must likewise be clearly expressed in the reasons given for the exercise of a special power and the reasons given for a renewed period of its exercise.

6. The need for Sigint

6.1 Process of stating needs

The first step of the Sigint processing procedure, as practiced at the Sigint department, is that of determining and stating the Sigint needs. These Sigint needs are inferred from the general needs for information in the field of intelligence and security which are determined partly outside DISS and partly within the DISS organisation. For an understanding of the Sigint processing procedure it is important to examine how a need or question finds its way to the Sigint department. The general aspects of these external and internal needs statements will be briefly discussed below.

6.1.1 External statement of needs

The organisations for which DISS collects information include the Dutch armed forces, the ministry of General Affairs and the ministry of Foreign Affairs. These bodies periodically establish their information needs for a fairly long period. The information needs may be adjusted if it is advisable to do so. Short-term needs are usually submitted to DISS on an ad hoc basis, in the form of requests for information.[84] Many of the requests made on a daily basis come from the Commander of the Armed Forces and the Defence Staff, which are responsible for the military decision-making process for planning and carrying out crisis management operations.

National and international partners, such as GISS or foreign services, also submit statements of needs to DISS. The requests coming from these parties are almost exclusively ad hoc requests.

The minister of Defence lays down the annual intelligence and security needs of the defence organisation in a statement of Defence Intelligence and Security Needs (DISN). The DISN specifies what are the needs for each area of attention (regional or thematical). Three categories are used for this purpose. The category determines the required degree of intensity and depth with which DISS is to gather information and can also be seen as an indication of the importance attached by Defence to the area of attention in question. The following categories are used:

[83] Examples are the right of nondisclosure or diplomatic immunity.
[84] Also abbreviated as *RFI*.

I. Areas in which the armed forces are or will be present either permanently or in the context of a crisis management operation, and areas of attention having a direct influence on the mandate of the armed forces;
II. Areas to which the armed forces may be deployed for crisis management operations, areas which have or may have an influence on crisis management operations in view of their geographic location, areas which may pose a risk for the security of Dutch and alliance territory, and countries and/or themes having specific significance for Dutch security policies;
III. Areas that are relevant to Dutch security and defence policies and regarding which the early identification of developments is important (known as the *indicator and warning* function).

The needs of the ministry of General Affairs and the ministry of Foreign Affairs are stated in what is known as the Designation Order. Pursuant to Article 7(2)(e), ISS Act 2002, the Designation Order is adopted by the prime minister in agreement with the minister of Defence and the minister of the Interior and Kingdom Relations. The minister of Foreign Affairs is not mentioned in the Article, but in practice he is involved in adopting the Designation Order.[85]

The Designation Order names the investigation subjects in relation to countries and regions about which political intelligence must be collected. The purpose of designating subjects to be investigated is to gather information that will enable the Dutch government to decide on foreign policy positions and to conduct international negotiations on the basis of information that cannot be obtained or is hard to obtain through other channels, for example diplomatic channels. The subjects are divided between GISS and DISS, with subjects having predominantly military relevance being assigned to DISS. The services may also be jointly responsible for a particular subject.[86]

6.1.2 Internal statement of needs

By and large, the external needs laid down in the DISN and in the Designation Order are decisive for the internal statement of needs. For example, these two documents serve as guidelines for defining the annual priorities and the semi-annual production planning established for each investigation area. This is done at the Intelligence department of DISS.

The Intelligence department is organised in teams. Each team is responsible for the production of intelligence within its own investigation area. An investigation area can be a specific region, for example Africa or the Middle East, but also a specific theme, for example terrorism or the

[85] See also review report no. 26. The lawfulness of the performance by GISS of the foreign intelligence task, *Parliamentary Papers II* 2010/11, 29 924, no. 67 (appendix), available at www.ctivd.nl, section 3.4.
[86] Idem, section 4.3.3.

proliferation of weapons of mass destruction. Teams hold periodic consultations on developments within their area of attention, on contacts with parties submitting statements of needs and with national or international partners, and on the current production of intelligence reports.

The team structure of the Intelligence department extends beyond the department. This means that teams do not only include only analysts of the Intelligence department, but also employees from other DISS units. The purpose of this structure is to ensure that all relevant areas of expertise are involved in preparing intelligence reports. The departments which actually gather information, including the Sigint department, are therefore represented on the teams as well. It is their responsibility to ensure that the teams receive the appropriate information from the sources available to them in good time. To enable them to do so, it is important for them to know what are the needs and what information the teams are looking for.

In the production planning process it is laid down in broad outline what needs there are, what priorities are assigned to them and which concrete intelligence reports are expected on the subjects to which attention will be given within each investigation area. Since mid-2008, action plans are prepared with regard to the expected intelligence reports. An action plan must among other things state what is the focus of the (sub)investigation, which questions or subquestions have to be answered in the investigation process and which sources the analyst intends consulting. The action plans are discussed at team meetings and can thus provide guidance for the departments that will gather the information, including the Sigint department. Together with the priorities established annually and the semi-annual production planning, the action plans serve as guidelines for the gathering of information.

In addition to planned intelligence reports, the teams also work on concrete ad hoc requests received from external bodies that may state intelligence needs and on developments emerging within their area of attention in the course of a planning period. New information will have to be gathered regularly in respect to these matters as well. Here, too, it is important that the departments that do the information gathering, including the Sigint department, know which needs have been stated and what is the concrete information the teams are looking for. Team meetings serve to exchange knowledge and questions between the analysts and those who do the actual information gathering.

6.2 Tasking process

Sigint analysts represent the Sigint department in the various teams managed by the Intelligence department. At the Sigint department there are task groups which are largely counterparts of the teams at the Intelligence department. A Sigint analyst, working in consultation with his superior(s) and the other Sigint analysts within his task group, determines the priorities to be assigned to the various Sigint needs established by the team. The Sigint analyst examines to what extent the

team's information needs can be met by existing Sigint already obtained. If there is insufficient existing Sigint, the Sigint analyst examines in respect of which persons or organisations it is advisable to take measures to obtain new Sigint. In this way a concrete need arises for new Sigint to be obtained for each investigation area (and for each task group).

Priorities are established at department level on the basis of the different needs of the task groups. This is necessary because the interception resources are limited. On the basis of the needs stated, choices must be made for which investigation areas and subtopics it is advisable to take Sigint measures.

The next step is to consider whether it is possible to obtain the desired intelligence in terms of technical and capacity possibilities. It must be examined whether the intelligence can be obtained by the National Sigint Organisation (NSO) or by mobile platforms (cf. section 7.1). For this purpose the Sigint needs must be converted into concrete, workable interception orders. Placing the Sigint needs with partner services is also a possibility that may be considered.

The process of converting Sigint needs into concrete interception orders is called *tasking.* Several consultative meetings are held between the parties involved in order to streamline the tasking process as much as possible. Regular consultations are held between the Sigint analysts of the task groups and the department management office to achieve appropriate prioritization of the Sigint needs of the department as a whole. Regular consultations are held, moreover, between the Sigint department and NSO and between DISS, GISS and NSO for the purpose of allocating the scarce Sigint resources at the disposal of NSO.

In practice, tasking is not a static process and adjustments are sometimes made on a daily basis. The limited available means for obtaining Sigint and the dynamics of communications traffic continuously compel the organisation to clearly state priorities and ensure proper coordination with NSO (and with GISS). It is important, moreover, for NSO to know the context of the interception orders placed by the Sigint department and to be aware of the actual investigations and plans which the Sigint department is carrying out and which affect the activities of NSO in one way or another.

The Committee has not investigated how the coordination with NSO (and GISS) is given shape in actual practice.

6.3 Assessments for the purposes of stating intelligence needs

The preceding sections have shown that a number of steps are completed before it is decided to actually start obtaining Sigint. An external authority states its intelligence needs. These needs are further specified within the department and translated into investigation questions.

The investigation questions are submitted to the departments that actually gather intelligence, one of which is the Sigint department. At the Sigint department it is examined which intelligence is already available within the department. Insofar as intelligence is not available, the department will try to obtain the intelligence. This involves the tasking process, which is used to determine where priorities lie, what capacity is available and whether it is technically possible to obtain the requested intelligence.

On the basis of the needs statement and the technical and capacity possibilities and impossibilities, an application to the minister of Defence is then drawn up for each individual subject for which this is required, for permission for the ultimate acquisition of the requested intelligence by taking Sigint measures (see also sections 7.2 and 8.3). Applications are prepared every three months by the Sigint analyst in charge of the subject concerned. The application must be properly substantiated by reasons, since the exercise of a special power must satisfy a number of statutory requirements (See section 5). The infringement (of privacy) occurring as a result of the exercise of the power must be necessary, it must be proportionate to the intended objective and it must be kept at a minimum. This means that before a service can take measures to obtain new Sigint, it must assess whether these requirements are satisfied. This assessment is currently made at a fairly late stage, namely when the Sigint analyst prepares an application to the minister because he must be able to substantiate the application by proper reasons.

Given the organisation of the process preceding a decision to take Sigint measures, the Committee holds the opinion that the assessment whether the requirements of necessity, proportionality and subsidiarity are satisfied should take place at an earlier stage. The Committee also considers it necessary that these assessments are not made exclusively by the Sigint analyst. It is the team which states that there is a need for Sigint: it does so by establishing priorities and production planning, in the form of concrete investigation questions (action plans) and in the form of ad hoc questions. In the perception of the Sigint analyst, this makes it a given that obtaining Sigint is necessary. A need for Sigint has been stated and the Sigint analyst must ensure that the need is met. He cannot assess whether meeting this specific need is actually necessary for the performance by DISS of its tasks. Subsidiarity is likewise a given to the Sigint analyst. A Sigint analyst has no insight or insufficient insight as to whether the requested intelligence can also be obtained by consulting public sources or by exercising another, less infringing power.

In the given circumstances the Committee considers it necessary that the assessments regarding the necessity and subsidiarity of the intended Sigint measures are made at an earlier stage and are made by the team, in consultation with the Sigint analyst. Unlike the Sigint analyst, the team is able to assess whether a particular investigation or part of an investigation is really necessary for the performance by DISS of its tasks, and insofar as it concerns the (a) task and (e) task, whether there is a potential threat of harm to national security. The team can also determine the objective for which intelligence must be obtained and assess whether obtaining intelligence by taking Sigint measures is necessary to achieve the objective. Perhaps the objective can also

be achieved by consulting public sources or by exercising other, less infringing powers. The Sigint analyst is pre-eminently capable of assessing to what extent taking Sigint measures can contribute to achieving the objective stated by the team. Currently, the team is not involved or not sufficiently involved in making the aforementioned assessments. Internal rules exist requiring that attention be devoted to this point in the action plans for intelligence reports. In practice this hardly happens at all. Neither is there any other evidence that teams assess whether taking Sigint measures is necessary and is the least infringing alternative in a specific situation.

It is the Sigint analyst who can answer the question whether taking Sigint measures is proportionate. To answer this question it must be assessed whether the infringement of the (privacy) rights of the target is proportionate to the objective to be achieved, namely the intelligence that will be obtained. The team has no insight into this matter. It is the Sigint analyst who examines, based on a particular Sigint need, where and in which way he may be able to obtain the requested intelligence, and who decides with respect to which person or organisation it is advisable to take Sigint measures. In this situation, therefore, only the Sigint analyst is able to balance the interests served by taking Sigint measures and the interests of the party that is the target of the measures. It should be noted, though, that the Committee finds in section 8.3 that greater involvement of the team in determining targets of Sigint measures is advisable. This would also shift part of the responsibility for assessing proportionality to the team.

The Committee recommends that DISS introduces a procedure according to which the assessments regarding necessity, proportionality and subsidiarity of taking Sigint measures are made by the team (of which the Sigint analyst is a member). With a view to internal accountability and external monitoring the Committee draws attention to the importance of laying down in writing all assessments that have actually been made and which form the basis for taking Sigint measures. Thus far, this has been done on too limited a scale.

7. Obtaining Sigint

7.1 The agencies that intercept Sigint

The Sigint department of DISS is not itself charged with actually obtaining Sigint from the air. Interceptions of Sigint are done by NSO and by Sigint detachments. In addition, the Sigint department can call upon partner services that also intercept Sigint. These intercepting agencies will be briefly discussed below.

7.1.1 NSO

In organisational terms, NSO forms part of DISS. NSO is a facilities organisation which is responsible for the interception of non-cable-bound telecommunications on behalf of DISS and GISS. This means that NSO does the actual intercepting of HF radio traffic and satellite communications. The communications obtained by NSO from non-targeted interception are at the disposal of both DISS and GISS. In addition, NSO also engages in searching for the purposes of its interception task. NSO has traffic analysis capacity and signal analysis capacity in order to be able to properly perform its interception task.

In addition to the intercepting task, NSO has two other main tasks. NSO does research aimed at innovation and long-term continuity of interception. And NSO is responsible for maintaining expeditionary capacities (Sigint detachments) which can, for example, be used to support crisis management operations.

In management terms, NSO falls under DISS. DISS and GISS are jointly responsible for the control and operational direction of NSO. Details for this cooperative task are laid down in the Covenant on the interception of non-cable-bound telecommunications by the National Sigint Organisation.[87] The present investigation did not include the manner in which NSO and DISS (and GISS) jointly implement the Covenant and the cooperation it implies.

7.1.2 Sigint detachments

DISS may deploy units to intercept local telecommunications traffic abroad. Such traffic cannot be received in the Netherlands. DISS must therefore travel to the signal in order to be able to intercept it. In addition to local telecommunications, such a unit can also intercept HF radio traffic and satellite communications. Units, also known as Sigint detachments, may for example be deployed abroad to provide intelligence support to crisis management operations of the Dutch armed forces.

Sigint detachments are equipped and staffed by NSO but controlled from the Netherlands by the relevant task group at the Sigint department. The task group is responsible for the tasking process for the Sigint detachment. The task group translates Sigint needs into concrete interception orders to the Sigint detachment.

In case of calamities a Sigint detachment may be controlled by a *National Deployed Sigint Section* (NDSS). An NDSS is an advance Sigint post in a deployment area. It serves as link between the relevant task group of the Sigint department in the Netherlands and the units of the armed

[87] *Government Gazette* 2007, no. 129, p. 8.

forces in the deployment area. Relevant Sigint reports for the Commander on the spot are supplied via the NDSS. NDSS sends back important information and concrete Sigint needs from the deployment area to the task group.

In principle, communications intercepted by a Sigint detachment are further processed by the task group in the Netherlands. Subsequently, reports are provided to the units in the deployment area via the NDSS. The Sigint detachment will however try to filter out communications of an urgent nature so that this intelligence is immediately available for use in the deployment area.

A special issue regarding the deployment of Sigint detachments abroad is whether such deployment must take place within the parameters of the ISS Act 2002. DISS takes the position that it is advisable to observe the procedures prescribed by the ISS Act 2002 when abroad, even though this is not a formal requirement. The basic principle is to work in conformity with the Act, also when operating abroad. According to DISS, however, it is not necessary for Sigint detachments to obtain permission for interceptions in deployment areas. In all events the minister will be informed of the activities of Sigint detachments in deployment areas.

The ISS Act 2002 is a national law which does not contain special provisions for conducting investigations and exercising special powers abroad. This means that there is no legal basis for deploying Sigint detachments abroad. It is the opinion of the Committee that the absence of a legal basis for exercising special powers abroad can only be approved if the ISS Act 2002 is applied by analogy. In the opinion of the Committee the procedures prescribed in the ISS Act 2002 for exercising special powers must therefore also be observed when the powers are exercised abroad.[88] This means among other things that any targeted interception of communications by a Sigint detachment requires the prior permission of the minister. The same applies to the selection of communications obtained by Sigint detachments by non-targeted interception.

The Committee can imagine urgent situations requiring immediate action to be able to furnish intelligence support to crisis management operations. If, for example, there is a situation of *troops in contact* in the deployment area, this creates an immediate need for capability to support the incident by means of Sigint. The Committee appreciates that in such exceptional situations there is no realistic possibility of contacting the minister before taking action. In this situation the Committee considers it important, though, that the minister is informed as soon as possible of the special powers that have been exercised without prior permission. In the opinion of the Committee it is, moreover, necessary to prepare detailed written reports of both the exercise of the power and the subsequent coordination with the minister.

The Committee recommends that DISS brings procedure and practice of deploying Sigint detachments into line with the foregoing.

---

[88] See also review report no. 26. The lawfulness of the performance by GISS of the foreign intelligence task, *Parliamentary Papers II* 2010/11, 29 924, no. 67 (appendix), available at www.ctivd.nl, section 3.5.2.

7.1.3 Partner services

DISS may call upon partner services which also obtain Sigint. As a result, DISS has more intelligence at its disposal than if it would have to rely exclusively on its own resources.

Sigint cooperation occurs in bilateral and in multilateral relationships and is usually unrelated to other forms of international cooperation by DISS. Cooperation takes place in several areas, both technical and as regards content.

The cooperation with foreign services is discussed in greater detail in the secret appendix to this review report.

Section 9.3 contains a more detailed discussion of DISS sharing Sigint with partner services.

7.2 Targeted interception

The ISS Act 2002 makes a distinction between targeted interception (Article 25) on the one hand and non-targeted interception which may be followed by selection (Article 27) on the other hand. This distinction also exists in actual practice. Technically, certain communications over the air can be intercepted by targeted interception. This is mainly the case for HF radio traffic. Intercepting this type of communications is therefore governed by Article 25, ISS Act 2002. Other communications over the air are not capable of targeted interception. These communications are sent by bundled transmission from one location on earth to another via a satellite. The interception of such communications is governed by Article 27, ISS Act 2002. This form of interception will be discussed in section 7.3.

7.2.1 Interception and permission

Government organisations often operate national and international telecommunication networks of their own in order to maintain secured telecommunication connections. These telecommunication networks consist of radio transmitters and receivers which transmit communications over the air that are usually secured by cryptography. Radio equipment transmits among other things via HF connections. It is a special feature of HF signals that they are reflected by the ionosphere and the surface of the earth. This enables them to travel distances of thousands of kilometres. HF radio connections are used, for example, by diplomatic institutions and other government organisations, including military organisations, but also e.g. meteorological and radio stations.[89]

[89] *Parliamentary Papers II* 2000/01, 27 591, no. 1, pp. 6-7; *Parliamentary Papers* II 1999/2000, 25 877, no. 9, pp. 20-21.

Targeted interception of communications by NSO usually relates to HF radio connections. HF radio can be used to establish connections over great distances, making worldwide communications possible. As a result of this property, HF radio traffic can usually be intercepted from the Netherlands.

Sigint detachments also carries out targeted interception. Usually, they will intercept local telecommunications traffic. Such connections operate over shorter distances than HF radio connections. Because these communications cannot be intercepted from the Netherlands, the interceptors go to where the signal is.

In order to be able to intercept communications it is important to find out the frequency at which the person or organisation under attention is transmitting. So-called searching (see section 7.4) can contribute to do so. It is a common phenomenon that the frequencies used by a particular person or organisation change regularly and also that more than one frequency is used. Applications to the minister for permission to carry out targeted interception are therefore not required to include the relevant frequency or frequencies. Applications must, however, state particulars of the identity of the person or organisation whose communications will be intercepted and the reason why DISS wishes to intercept their communications (Article 25(4), ISS Act 2002).

It may happen that DISS is aware of a frequency at which communications are transmitted that are relevant to the performance of its tasks, but does not know which person or organisation is transmitting them. In such a case DISS may submit an application which does not state particulars of the person or organisation. Those particulars must subsequently be supplied as soon as possible (Article 25(6), ISS Act 2002).

In practice, therefore, an application for permission for targeted interception will usually state particulars of the person or organisation and the reason why the service wishes to intercept the communications. Applications for permission for targeted interception (and for the exercise of other special powers) are bundled and submitted to the minister on a three-monthly basis. Permission is likewise granted for three months.

7.2.2 Generic identities

The Committee has established that in a number of cases permission was asked and obtained for targeted interception with respect to a particular category of persons and organisations. DISS had designated broadly formulated generic identities covering a particular 'type of persons or organisations. This does not mean that the communications of all persons or organisations falling under the generic identity will actually be obtained from targeted interception, but that it is potentially possible. If a person falling under a generic identity enters the picture and if

the frequencies at which the person or organisation communicates are known, these may be immediately included in the interception programme without waiting for specific permission to do so, since permission for the generic identity has already been obtained.

DISS has put forward various reasons for applying for generic permission for targeted interception. In certain cases a specifically formulated application for permission is found to be too restrictive. Submitting a specific application based on a frequency is hardly feasible because the frequencies used change continuously. A generic identity obviates the problem that an application relates to frequently changing or still unknown persons or organisations. DISS must be able to react quickly to changing circumstances. Mentioning specific names may also be difficult because of the use of aliases and because of different notations.

The Committee has found in the course of its investigation that it has been agreed in the past with the Legal Affairs department of the ministry of Defence that generic permission will be granted only in relation to a defined investigation target, namely a particular region or a particular conflict. The investigation target must be included in the application for permission. It was considered unadvisable to submit endless lists of frequencies and other unappealing information to the minister. Preference was given to a clearly described generic identity, because this was a workable procedure.

DISS has stated that internal checks are carried out with respect to persons and organisations whose communications are included in the interception programme before the service has obtained specific permission to do so. Such interceptions before permission has been obtained do not take place without the approval of the Sigint department's legal expert. Since early 2010, DISS has adopted the practice of expressly naming the persons and organisations in the first following application for permission.

It is the opinion of the Committee that the aforementioned procedure is not consistent with the ISS Act 2002 and does not do sufficient justice to the statutory protection of the (privacy) rights of those whose communications are or may be intercepted. The application for permission is intended to gain targeted access to the communications of individual persons or organisations. At the least, the application must show against whom the power may be exercised and why. Article 25, ISS Act 2002, does in fact require this. The generic identities designated in the applications for permission are so broad that in the opinion of the Committee it is impossible to foresee exactly which persons and organisations fall or may fall under this identity.[90] This is not changed by the internal check done by the department's legal expert. In addition, the Committee points out the vulnerability of the role of the legal expert who bears (too) great responsibility in this matter.

The Committee does appreciate that in a situation where exactly the same reasons apply to

[90] This issue will be discussed in greater detail in the secret appendix to this review report.

the interception of the communications of certain persons or organisations, the service may bundle the applications for permission into one application.[91] In this case it is necessary that it is absolutely clear which persons or organisations fall within the bundled group. In the opinion of the Committee the submission of a bundle of applications does not harm the protection of the (privacy) rights which the procedure laid down in the ISS Act 2002 envisages to safeguard. Moreover, it meets the wish to keep the applications for permission clear and manageable.

Article 25(6), ISS Act 2002, allows for the possibility of supplementing the particulars concerning the identity of a person or organisation at a later stage. In an earlier review report the Committee accepted that where permission has been granted for the interception of the communications of an organisation and where the application has been sufficiently limited according to the category of members liable for interception, individual members of an organisation may also be ranged under the permission. Members that are subsequently identified may also fall within the permission granted, if they qualify.[92] The Committee considers the same procedure acceptable with respect to a person falling within a bundled group of persons and whose name is subsequently identified. In that case DISS must state in the first following application for renewal why the person is considered to belong to the organisation or group of persons in question. The Committee has found that since 2010 the service follows the practice of including the names of persons whose communications have been added to the interception programme after generic permission was granted. No reasons are stated, however, why the person in question is considered to belong to the organisation or group. The Committee considers this necessary. The Committee recommends, moreover, that DISS adopts an internal written procedure formalising its actual practice.

7.2.3 Stating reasons

Article 25 not only requires an application for permission for targeted interception to show with sufficient precision with respect to whom the power will or may come to be exercised, but also what is the reason for exercising the power in respect of these parties. Each application must be substantiated by reasons, from which it must clearly emerge how the requirements of necessity, proportionality and subsidiarity are met. The Committee has established that many applications for permission are not sufficiently substantiated by reasons.

It is true that DISS does, in its applications for permission, state the reason for the wider investigation for the purposes of which the power is to be used. In doing so it also gives attention to the subject (for example a particular region designated in the DISN or the Designation Order)

---

[91] This issue will be discussed in greater detail in the secret appendix to this review report.

[92] Review report no. 19. The application by GISS of Article 25 of the ISS Act 2002 (wiretapping) and Article 27 of the ISS Act 2002 (selection of non-targeted interceptions of non-cable-bound telecommunications, *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), available at www.ctivd.nl, section 6.2.1.

and the subject elements in which DISS is interested. The Committee holds the opinion that in nearly all cases these explanations give a clear picture of the investigation and provide grounds for the use of special powers in its context. The Committee points to the requirement, when special powers are exercised in the context of the (a) task and the (e) task, of also stating what is the potential threat to national security (see section 5.1).

The Committee has established, however, that applications state only very summary reasons focusing specifically on the person or organisation. In the case of generic identities designated by DISS, moreover, the reasons are often insignificant and formulated in too general terms. The Committee has also found that applications for permission frequently use purely standard reasons.

It is the opinion of the Committee that reasons must be stated with respect to each individual or organisation or for each bundled group why targeted interception of his or its communications is considered necessary. The application must also state what is the objective of the targeted interception in the context of the investigation and what is the basis for expecting that the intelligence obtained from interceptions will contribute to achieving the objective.[93] So a link must be established between the wider investigation being carried out and the necessity of intercepting the communications of the specific person or organisation. This will be different for each person, organisation or bundled group.

An application for renewal must subsequently devote express attention to the intelligence obtained from the interceptions and its added value for the investigation, not in a general sense but specifically with respect to the person or organisation. It is the opinion of the Committee that commonplace remarks that the exercise of the special power has contributed to meeting the intelligence need or has resulted in (unspecified) reports or has confirmed the existing standard picture do not suffice.

In addition to necessity, an application for permission must also state how the requirements of proportionality and subsidiarity are met. With respect to these requirements, so the Committee has found, the service also uses standardized texts which are intended to cover the proportionality and subsidiarity issues of the exercise of special powers for an entire investigation at once. Moreover, the general passages included in the applications do not make it clear or do not make it sufficiently clear what assessments have been made in this respect. Usually, the application only states the conclusion that the required intelligence cannot be adequately obtained by exercising another (special) power or by cooperating with foreign services.

The Committee holds the opinion that this procedure does not satisfy the requirements laid down in the ISS Act 2002 or in the assessment framework formulated in Articles 31 and 32 of the Act.

[93] The Committee considers reasons such as "is associated with terrorism" or "communication traffic of these institutions is a valuable source of information for the investigation" to be meaningless and insufficiently specific.

The legislature has enacted that prior to and during the exercise of a specific special power it must be assessed on the basis of the requirements of proportionality and subsidiarity whether it is (still) lawful to exercise the power. It is not clear or not sufficiently clear from the applications for permission or for renewal of permission that these assessments have actually been made. As was discussed in section 6.3 above, the process preceding a decision to take the measure of targeted interception likewise does not demonstrate sufficiently that these assessment are being made.

Since the Committee has insufficient knowledge of the reasons underlying interception, it is unable to assess the lawfulness of interceptions pursuant to Article 25(1), ISS Act 2002.

In section 6.3 above, the Committee recommended that DISS introduces a procedure according to which the assessments regarding necessity, proportionality and subsidiarity of taking Sigint measures are made by the team (of which the Sigint analyst is a member) and laid down in writing. By extension, the Committee recommends that DISS mentions in its applications for permission submitted to the minister which assessments have actually been made regarding necessity, proportionality and subsidiarity, specified per person or organisation against whom or which the power will be exercised.

7.3 Non-targeted interception (and subsequent selection)

NSO intercepts communications transmitted via communications satellites for use by DISS (and GISS). A satellite operates as if it were a mirror for radio signals. When a radio signal is sent to the satellite by a transmitter, the satellite receives the signal and then sends it back towards earth. A satellite can simultaneously cover a large area on earth. This area is called the *footprint* of the satellite. Communications with the satellite are controlled by ground stations.

What happens with interception is that the interceptor picks up beam connections that are sent between ground stations from one location on earth to another via a satellite. These 'links', as they are called, contain considerable quantities of communications and they can be picked up at great distances from the destination station. They comprise amongst other things data, telephone and internet traffic.

The ISS Act 2002 only confers power of non-targeted interception of non-cable-bound telecommunications. Where these communications are transmitted via cable links, they are strictly forbidden ground for DISS as far as non-targeted interception is concerned. In the opinion of the Committee the distinction between cable-bound and non-cable-bound communications is rather dated. The use of cables for international telecommunications traffic has increased as a result of the large capacity of modern fibre optic technology. Telecommunications traffic between different continents often passes through cables laid on the seabed. This is how a large part of transatlantic telephone communications is transmitted.

DISS has indeed taken the position that non-targeted interception of cable-bound telecommunications should be added to the powers conferred on it by law. The ISS Act 2002 provides sufficient safeguards against infringement by the exercise of special powers of the (privacy) rights of third parties. It should not make any difference whether the powers are exercised with respect to communications via a satellite or via a cable. The Committee has not researched the (legal) implications of widening the power of non-targeted interception to include cable-bound communications. The Committee considers it important, though, that these implications be researched.

Interception of satellite communications is considered to be non-targeted because it is not clear in advance who are the persons or organisations whose communications are being intercepted. Communications passing through a certain satellite channel are as it were copied from the air and stored in large files. This 'bulk' of communications can comprise thousands of communication sessions. It is not visible in advance from whom the communication sessions originate and what is their subject. This does not emerge until selections are made based on previously approved selection criteria. This selection process will be discussed in section 8.3.

Because it is not clear, in the case of non-targeted interception, which communications are being obtained and the communications content is not yet examined at this stage, DISS does not require permission for non-targeted interception. It does require permission for the further selection of the communications, though. So in theory, DISS may obtain all satellite communications from all over the world using non-targeted interception. In practice, however, there are technical and capacity limitations as a result of which DISS (NSO, in actual fact) intercepts only part of these communications. Cooperation with partner services ensures that the organisation's own limitations are supplemented.

The choice of the satellite channels that will be subjected to non-targeted interception is determined by the tasking process described in section 6.2. The supporting searching process is essential to making this choice. Section 7.4 will deal with the practice of searching.

7.4 Searching

There are thousands of HF radio transmitters on the air worldwide which transmit communications having their origin or destination abroad. In addition, there is the satellite data traffic which is complex, massive and continuously moving. Only a small part of this traffic is relevant to the performance by DISS of its tasks. In actual practice, the exercise of the powers of targeted interception (Article 25, ISS Act 2002) and selection after non-targeted interception (Article 27, ISS Act 2002) is made possible by searching. Usually, therefore, searching precedes the exercise of these powers; it is one of the factors enabling the services to exercise those powers. Searching must also be seen, however, as a continuous process of continuously exploring the air waves.

DISS describes searching under Article 26, ISS Act 2002, as surveying the radio spectrum and satellite traffic in order to obtain a better understanding of which telecommunications are found in which segments of the ether and by which technical parameters some telecommunications stands out from other telecommunications. Furthermore, it is possible to establish whether the signals can be intercepted, selected and processed with the available technical means. Subsequently, it can be broadly determined whether the telecommunications is relevant to the performance by DISS of its task. DISS can also examine whether previous explorations of the ether are still accurate.

NSO performs searching of HF radio links and of satellite communications. These searching processes are fairly technical in nature. The Sigint department also engages in searching for the purposes of non-targeted interception. Furthermore, the Sigint department searches to support the selection process. This form of searching is more content-oriented. Each of these types of searching will be discussed in greater detail below.

7.4.1 Searching for the purposes of targeted interception

NSO carries out search activities of HF radio links on a continuous and structural basis with a twofold objective: to collect search data for the purposes of performing interceptions and to determine the technical feasibility of intercepting. Searching for the purposes of targeted interception can be compared to turning the radio knob so that one keeps receiving different broadcasts. At the same time one listens to the broadcast content. Automation of searching HF radio links is difficult.

The searching process starts with identifying metadata of the transmissions and storing them in a database. These metadata consists, for example, of the frequency, time and date of receiving the transmission, bearing data (direction finder: where does the signal come from), its nature (military or non-military), the connection protocols used and other technical data. The metadata is compared with the standard picture to find out whether anything special is going on. The metadata then forms the basis for determining the technical feasibility of targeted interception and the necessity of further analysis.

Metadata relating to the identity of the communicating person or organisation may only be processed if it is necessary for the proper performance by DISS of its tasks (Article 26(3), ISS Act 2002). The Committee has not found indications that metadata has been processed wrongfully.

If it is considered necessary, the transmissions received are further analysed. This further analysis involves purposeful inspection of the content of transmissions, exclusively for the purposes of establishing the nature of the communications and the identity of the sender. These data are recorded as well.

Data that are stored may be used for targeted interception. When the Sigint department requires information originating from a particular organisation or a particular type of organisations which uses/use HF radio links, it can go through the database to see at which frequencies the communications to be intercepted are transmitted. If this is not known yet, it can search for the relevant source or sources.

If DISS is searching and comes across communications that are immediately relevant for DISS, it can submit an application for permission to the minister within two days. Until permission is granted DISS may intercept and record the communications, but it may not yet inspect the content. Such a situation hardly ever occurs in practice.

DISS is not permitted to follow a transmission longer than is strictly necessary to establish the sender's identity and the relevance for the performance by DISS of its tasks. The Committee has not found any indications that this has happened or is happening.

7.4.2 Searching for the purposes of non-targeted interception

The important point of searching for the purposes of non-targeted interception is to find out which satellite channels are used for communications with the greatest relevance for the performance by DISS of its tasks. The fact is that technical and capacity limitations compel DISS to make choices as to which satellite channels it will include in the non-targeted interception programme. Searching helps to make these choices. Searching is also aimed at safeguarding the continuity of non-targeted interception. Changes occur in the technical characteristics of the satellite channels used for a particular type of communications. It is advisable to keep track of such changes. In addition, it is important to know where DISS can find which communications so that it can respond to new needs.

Searching for the purposes of non-targeted interception is for the most part done by NSO. Searching starts with the interception of a quantity of communications transmitted over a particular satellite channel. The subsequent searching process comprises roughly two steps: a basic technical search and a more thorough search which involves content as well.

A satellite channel comprises a multitude of communications. When the communications are intercepted, all sorts of technical characteristics become available. These technical characteristics are recorded in a database. They relate e.g. to frequency, bandwidth, compression system, location of the ground stations between which a satellite link is set up, whether it is an analogue or a digital signal, etcetera. Based on these technical data it can be established whether additional interception is technically possible and advisable. At this stage it is still unknown who are the users of the communications transmitted via the satellite channel in question and whether these communications are relevant. Often, however, it can be established where the communications

come from, to which region they were sent and what type of communications (voice, fax, etc.) is being transmitted via the channel.

If it is technically possible and considered advisable, the data traffic can then be further analysed in order to establish the nature of the communications in greater detail. This is mainly done on the basis of metadata, i.e. data not concerning communication content but concerning the link and the transportation of the data. However, the analyst will also take a look at communication content. The information found in the process is stored in a database for future use. In addition to the data discovered in the more basic technical search, this information consists of data on the links used, the identity of the users, the locations from and to which the communications were sent and a brief profile of the communication content.

Metadata relating to the identity of the communicating persons or organisations may only be processed if it is necessary for the proper performance by DISS of its tasks (Article 26(3), ISS Act 2002). The Committee has not found any indications that metadata has been processed wrongfully.

Separating metadata from communication content can be difficult. In some cases it is technically difficult. In other cases it is not clear what is metadata and what is content, for example where metadata is transmitted as part of the communication content or when a particular characteristic of the content of a communication can be discerned from the communication exterior without examining its content. Technical developments are blurring these boundaries. The Committee holds the opinion that it is not possible in all cases to draw a clear dividing line between metadata and communication content. This will have to be assessed on a case by case basis.[94] Insofar as examining metadata coincides with examining content data, all the information together must be assumed to be content data.[95]

In many cases the intercepted communication sessions are in another language or encrypted in one form or another. In those cases NSO cannot examine the content of the communications. They must first be decrypted or translated. NSO does not itself have this capability, but may call upon the decryption and translation capacity of the Sigint department.

The Commission has found in its investigation that there is a difference of opinion between NSO and the Sigint department on the question whether NSO may examine communication content for the purposes of the searching processes it carries out. NSO takes the position that it is necessary to examine communication content in order to gear the interception of satellite communications as much as possible to the needs of the Sigint department and enable it to

[94] See also review report no. 19 The application by GISS of Article 25 of the ISS Act 2002 (wiretapping) and Article 27 of the ISS Act 2002 (selection of non-targeted interceptions of non-cable-bound telecommunications, *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), available at www.ctivd.nl, section 2.3.

[95] See also *Parliamentary Papers II* 2000/01, 27 460, no. 1, p. 27.

guarantee the quality and continuity of its non-targeted interceptions. The Sigint department endorses this position, but holds that this does not mean that NSO may, when searching, look for communication sessions of persons and organisations in whom/which DISS is interested in the context of ongoing investigations.[96] According to the Sigint department, this would be going too far and this power is reserved to the department itself. In practice both NSO and the Sigint department carry out such searching activities.

The power to search includes authority to look briefly at communication content in order to determine whether a particular satellite channel is (still) of interest and should (still) be intercepted. In this context the legislature has stated expressly that it is not permitted to intercept a transmission *longer* than is strictly necessary, since searching would then turn into a non-permitted form of targeted examination of communication content.[97] The Committee holds the opinion that it follows naturally that looking at communication content *more frequently* than is strictly necessary is not permitted either. This would entail unnecessary infringement of the (privacy) rights of third parties. The Committee recommends that NSO and the Sigint department make an arrangement which makes it clear which service will exercise this power.

The databases in which search data are stored are managed by NSO, and the Sigint department has access to them. The data recorded in the databases enables the Sigint department to control and adjust the searching activities of NSO, also with changing information needs. The details of how the searching will be carried out are discussed at the aforementioned tasking consultations between NSO and the Sigint department. Furthermore, search orders are placed with NSO. These state, for example, the communications of which satellite must be searched and in which region the Sigint department is interested.

When conducting its investigation, the Committee noticed that search orders are usually formulated rather broadly. The Committee has been unable to establish to what extent the search orders are further specified at the tasking consultations or in the daily contacts between the Sigint department and NSO. The Committee has found that it is sometimes difficult for NSO to characterise which searching activities have (the greatest) importance for the Sigint department.

In line with the recommendation to make a clear division of tasks in the area of searching, the Committee recommends that DISS will, where possible, further specify the searching orders placed with NSO and lay down the specifications in writing.

---

[96] As opposed to searching for the purposes of targeted interception. Then, NSO is in fact asked to search for frequencies used by persons and organisations in which DISS is interested.

[97] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 35.

7.4.3 Searching geared to the selection process

The Committee has established that DISS has added another form of searching to the aforementioned search processes mainly carried out by NSO. This is searching geared to the selection process.This form of searching is done by searching the communications bulk obtained from non-targeted interception for technical data, such as telephone numbers and e-mail addresses, for additional information about persons and organisations that are investigation targets, and for new persons and organisations that may possibly become investigation targets. These searches are conducted in relation to ongoing investigations of DISS and in relation to new areas of investigation which DISS is expected to start investigating in the (near) future.

In this context, searching is seen as the power to explore or catalogue intercepted and recorded communications. In this form of searching, communication content is not examined for the purpose of using the communications in content analyses and reports, but for the purposes of augmenting knowledge of the nature of the communications and of coming up with selection criteria for use in the selection process pursuant to Article 27, ISS Act 2002. The point is not, therefore, to use the intercepted and recorded communications, but to gather data in order to optimize the selection process.This searching process must be distinguished from searching for the purposes of non-targeted interception discussed in section 7.4.2. above. The point of the last-mentioned process is to optimize interceptions by evaluating communications via satellite channels.The selection process itself is discussed in section 8.3.

DISS takes the position that there is no essential difference between this form of searching for the purpose of the selection process and searching for the purpose of non-targeted interception. According to the service, the only difference is the moment at which the two forms of searching take place in the Sigint process. Searching for the purpose of non-targeted interception is done at the beginning of the Sigint process to find out whether a satellite link comprises communications that are of interest to DISS so that it is worthwhile to include or maintain the link in the interception programme.The other form of searching is not carried out until later in the process.This form of searching also leads to identification of senders of communications that are relevant to the performance by DISS of its tasks.The service will not carry out any content-related activities until it has applied for the minister' permission to select the communications.

The Committee recognizes that the searching processes carried out by NSO and the Sigint department have points in common and that it is not always possible to make sharp distinctions between the processes or process procedures. Nevertheless, the Committee holds the opinion that by taking the above position DISS disregards the distinction that can be made between the objectives at which the searching is directed and the grounds for infringing privacy by examining communication content.The Committee has established in this context that the actual practice of exercising the power to search has drifted a long way from the statutory power to search.

The Committee has also established that there is only a partial internal description of the procedure followed by DISS with regard to searching for the purpose of the selection process and that no procedure has been formalised in writing. In the course of its investigation, and also based on interviews held with the persons involved, the Committee has described the procedure followed in actual practice at DISS. It holds the opinion that the practice as described should be formalised in a written procedure and recommends that DISS does so as soon as possible.

The Committee has established that there are various different matters that may provide the reason and the objective for carrying out a search activity for selection purposes. It has in any case distinguished the following common practices:

1. Searching the communications bulk to determine whether the desired intelligence can be generated using the selection criteria for which permission has been obtained;
2. Searching the communications bulk to identify or characterise potential targets;
3. Searching the communications bulk for data from which future selection criteria can be derived for the purposes of an expected new investigation area.

The first searching practice for selection purposes means that data concerning persons and organisations already included in the selection programme – the minister has granted permission for the selection – are taken as a basis for a search for technical characteristics belonging to the persons and organisations in question. DISS may suspect, for example, that a particular technical characteristic is used by an existing target. By searching, DISS can find out whether this is in fact the case. It may also happen that one number of a target is known to DISS, but that the target is using other numbers as well. Searching the communications bulk enables DISS to identify the other numbers as well, which can then be used in the selection process.Another possibility is the situation that it is not known which members of an organisation with respect to which selection is permitted play an active role in that organisation nor which technical characteristics are used by these members. Searching may enable DISS to discover this information.The objective of this searching practice is therefore to optimize the criteria to be used for selection.

The first searching practice for selection purposes has quite a few aspects in common with the other forms of searching aimed at interception as described above. In all cases the objective of searching is to discover where to find the communications that DISS is looking for and for which it has obtained permission and to discover how those communications can best be obtained.

In contrast to the other forms of searching, this searching practice involves a more extensive examination of communication content, not merely as a brief element of an investigation into the question where to find the communications that are relevant for DISS. The point is indeed to obtain as much useful data concerning a target (person or organisation) as possible so that the communications selected with respect to this target are of the highest possible quality. The infringement entailed thereby is obviated, however, by the fact that pursuant to Article 27(3)DISS

has obtained the minister's permission to select the communications relating to the target. The first searching practice for selection purposes can, moreover, result in a more focused selection. Searching makes it possible to better assess in advance which selection criteria will yield the data required by DISS and which will not. This in turn makes it possible to reduce the volume of communications selected in vain and whose examination by the services turns out to be unnecessary in retrospect, and to increase the volume of selected communications necessary for the performance by the service of its tasks. Especially in the case of a power which sometimes involves looking for the proverbial needle in a haystack, it is important to locate the desired communications (for which permission has been obtained) as precisely as possible.

The second searching practice for selection purposes is aimed at identifying or finding out more about potential targets. These are persons and organisations with respect to whose communications no permission for selection has been granted yet. These persons or organisations enter the picture, for example, because they are in contact with existing targets. It also happens that only a technical characteristic of a potential target is known, following which a search is done to see whether this technical characteristic belongs to a person or organisation that may be interesting in the context of the relevant ongoing investigation. The objective of this searching practice is therefore to discover whether the potential target that has entered the picture actually qualifies in some way or other for selection of his communications, in relation to the ongoing investigation.

The second searching practice for selection purposes differs from the first practice and from the other forms of searching through the fact that it does not serve to support the exercise of the special power but is on the contrary aimed at starting a new exercise of the power. The searching is not done to try and discover where to find the communications that DISS is looking for and for which it has obtained permission, and how these communications can best be obtained. It rather serves to assess which further interesting communications can be found and whether these communications qualify for a new selection process.

To illustrate the difference between the first and the second searching practice for selection purposes, the Committee calls to mind the situation described above in which DISS has a technical characteristic – a telephone number, for example – and does not know to whom this number belongs. If it is thought that the number may belong to a target already included in the selection programme with the minister's permission, then the Committee holds the opinion that DISS is free to do a search to find out whether this is in fact the case. If the answer is affirmative, this may be recorded. A simple affirmative (or negative, as the case may be) answer may be shared with the Sigint analyst who will process the information content. In this case the privacy infringement is obviated by the minister's permission. The situation is different where DISS does not know to whom the number belongs or thinks that the number is used by a potential new target. If DISS does a search to discover these facts, however desirable this may be for the intelligence process, the privacy infringement is not covered by any permission from the

minister. Neither is the infringement covered by Article 26, ISS Act 2002, which does not provide for this form of searching.

The third searching practice for selection purposes concerns searching for data from which future selection criteria can be derived for use in an expected new investigation area. This form of searching involves searching the communications bulk for possible data (technical characteristics) of persons and/or organisations that tie in with the subject of the investigation that is expected to be started in the forseeable future. Such data that may at some point form the basis for determining selection criteria are also collected by other methods. For example by consulting public sources, previously selected communications, and information from partner services. When the investigation into the subject is actually taken in hand, analysts can make a quick start based on the data that have been collected. This searching practice likewise does not serve to support the exercise of the special power but is on the contrary aimed at a new use of the power. The privacy infringement resulting from the searching is not covered by any permission.

In addition, Article 27(9), ISS Act 2002, provides that any data contained in the communications bulk that has not been selected may be retained for a maximum period of one year for the purposes of further selection. This is made subject to the condition that such further selection must take place for a reason or in relation to a subject for which permission had been granted at the time the data was obtained from non-targeted interception. So further selection is only permitted in the context of a concrete ongoing investigation of DISS. A second condition is that further selection is urgently required.

Both conditions are by definition not satisfied in the case of an expected new investigation subject. Consequently, the selection of data from previously intercepted communications for use in an expected new investigation area is not permitted. Considered from this perspective it is difficult to defend that searching the communications bulk for the purposes of an expected new investigation area is permitted. This type of searching is aimed at generating data from which selection criteria can be derived, while it is clear from the beginning that selection of these communications is not permitted.

DISS has tried to obviate the infringement caused by searching for selection purposes by incorporating certain safeguards in the process. These safeguards are intended to prevent that communications examined in the searching process are used in the intelligence process. For example: a technical separation has been introduced between the files in which the communications bulk is stored and the files in which the communications selected with permission are stored. Analysts concerned with analysing content and reporting on the intelligence obtained thereby have access to the 'selections files'. Only persons responsible for searching have access to the 'bulk files'.

The same separation is maintained with respect to the searching results. Data generated by searching activities may only be shared in broad outline with task group analysts. Factual data

from the communications may not be shared with the analysts. For the purposes of supervising the process, a procedure has been in place since the end of 2009 that search results may only be provided to analysts in writing. The rules concerning the restricted sharing of search results and written records of such sharing have not been formalized (yet) at the Sigint department.

In this way DISS tries to guarantee that any communication content that has been examined in the searching process cannot be further processed. Only data selected with the permission of the minister is included in reports on content. DISS believes that the separation procedure provides sufficient safeguards against infringement of the (privacy) rights of third parties. The separation is not airtight, though, since linguists are involved in both processes. This will be discussed in greater detail in section 8.2.

The Committee considers the first searching practice permissible. Searching the communications bulk to determine whether the required intelligence can be generated using the selection criteria for which permission has been obtained serves to support the exercise of the special power of selection. The infringement resulting from the searching process is obviated by the minister's permission to apply selection with respect to the person or organisation mentioned. Furthermore, searching can result in a more targeted selection. The Committee observes that records may be made only of searching results relating to the current targets of the service. This data may be shared with the analysts.

The Committee holds the opinion that the safeguards introduced by DISS to prevent any unlawful exercise of the power provide insufficient protection. Apart from the technical measures introduced in the system, the separation between the activities of the persons responsible for searching and those of the analysts responsible for analysing and reporting on content and also the restrictions imposed in practice on providing data content are based exclusively on informal arrangements and depend on the goodwill of the employees concerned.

The Committee recommends that DISS introduces an operational procedure that guarantees the separation between searching and reporting on content, and formalises it in an internal document.

The Committee holds the opinion that the infringement of the (privacy) rights of third parties resulting from the second and third searching practices for selection purposes has no basis in the ISS Act 2002. It is the opinion of the Committee that the power of searching as laid down in Article 26, ISS Act 2002 and further explained in the legislative history, has the objective of supporting the exercise of the powers of Articles 25 and 27, ISS Act 2002. In other words, searching may be done exclusively for the benefit of targeted interception and for the benefit of non-targeted interception followed by selection. The Committee holds the opinion that the second and third searching practices for selection purposes do not contribute to support or optimize the selection process but are aimed at a new use of selection after non-targeted interception. Article 26, ISS Act 2002, provides insufficient basis for these forms of searching.

The Committee has established that the statutory provisions and actual practice are at odds on this point. It suggests that the legislature considers whether it is necessary to confer the powers in question on DISS (and GISS) with due regard to the protection of privacy.

8. Processing Sigint

Communications obtained from targeted or non-targeted interceptions are subsequently processed by the Sigint department. The following paragraphs deal with deciphering, the linguistic process and the selection of communications based on approved selection criteria and key words.

8.1 Decryption

Transmission of communications is made possible by fixed technical and procedural arrangements between sender and receiver, known as communications protocols. In addition, all sorts of techniques are used to improve communication efficiency and reliability. DISS has knowledge of the protocols and techniques used so that it can process the intercepted signals into intelligible information, such as printed text or spoken language. The information thus obtained may still be encrypted.

Encryption means the encoding of information to make it illegible to third parties. DISS tries to break the encryption of communications by crypto analysis, a process that can be very time-consuming. DISS has the necessary equipment and specialist employees to do this work. Furthermore, DISS cooperates in this field with both national and international partner services.

The law permits the use of technical facilities to break encryption. The power of decryption is included in the law as an element of the powers of targeted interception (Article 25(1), searching (Article 26(1) and non-targeted interception (Article 27(1). So it is not necessary to obtain separate permission with respect to encryption. Pursuant to legislative history, encryption includes all conceivable means of making information inaccessible to third parties. This includes encryption.[98]

Furthermore, the ISS Act 2002 provides that any person who has knowledge of undoing the encryption of communications obtained from targeted interception must give every necessary assistance in undoing the encryption upon the written request of the head of the service (Article 25(7). A similar obligation to assist is included with respect to the encryption of data stored or incorporated in an automated work (Article 24(3)), but not in Articles 26 and 27, ISS Act 2002, probably by mistake.

[98] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 40.

The Committee has found in the course of its investigation that DISS exercised special powers to collect information for decryption purposes and for the purpose of related (technical) research. In previous review reports[99] the Committee established that the ISS Act 2002 does not allow the exercise of special powers *in support of* the performance by the services of their tasks. Article 18, ISS Act 2002, provides that special powers may only be exercised to the extent necessary *for the proper performance of the tasks* referred to in Article 7(2), subparagraphs (a), (c) and (e), of the Act and not in support of such performance. The Committee considers that decryption does not itself fall under the (a), (c) and (e) tasks of DISS, but is a supplementary power serving to support the aforementioned special powers. It may be argued, therefore, that the special powers exercised to collect information for the purpose of decryption and for the purpose of related (technical) research were exercised *in support of* the proper performance of tasks, which the ISS Act 2002 does not permit. The legislative history is rather vague on this point, however, and only mentions the example of checking the reliability of a human source as a form of support.[100] The Committee has established that the above special powers are on the verge of what is and what is not permitted by law. The Committee therefore urges DISS to exercise restraint in exercising special powers and to pay special attention to substantiating decisions to do so by sound reasons.

8.2 Translation and linguistics

Communications obtained from targeted or non-targeted interception are usually conducted or expressed in other languages. Before they can be analysed, the communications must be processed by an interpreter or a linguist. Linguists play an important role in making a (first) selection between relevant and less relevant information for the performance of tasks. They must therefore be well-informed about the investigations for which the communications have been intercepted. Linguists perform their activities in close contact with the Sigint analysts. There is a certain overlap in their work. They also support and cooperate with each other in further analysing the information obtained. Within a certain task area the analysts' task is even performed entirely by linguists because DISS lacks analysis capacity to perform this task.

The Committee has found in the course of its investigation that the support of linguists is also used for searching purposes, since NSO or GISS also come across communications in other languages when they are searching. In many cases they will then need the support of linguists in the searching process to enable them to establish the sender's identity and the relevance of the communications for the performance of their tasks.

---

[99] Review report no. 6. Investigation by GISS into radical animal rights activism and left-wing extremism, *Parliamentary Papers II* 2005/06, 29 924, no. 9 (appendix), available at www.ctivd.nl, pp. 10-11; Review report no. 25. The conduct of DISS with respect to two suspended, *Parliamentary Papers II* 2009/10, 29 924, no. 59 (appendix), available at www.ctivd.nl, section 9.4.

[100] *Parliamentary Papers II* 2000/2001, 25 877, no. 15, p. 5.

The Committee notes that in this situation the separation made by DISS between the searching process and the intelligence process, mentioned section 7.4, cannot be maintained. Linguists are involved in both processes. When they support the searching process they become aware of communication content and if the occasion arises they are asked not to use the knowledge thus acquired in the intelligence process. The separation set up by DISS is not guaranteed except by the responsibility assumed by the linguists themselves in this regard.

8.3 Selection

In section 7.3 the Committee discussed the non-targeted interception of satellite communications. Interception of satellite communications is considered to be non-targeted because it is not clear in advance who are the persons or organisations whose communications are intercepted. Communications transmitted through a certain satellite channel are as it were copied from the air and stored in large files. This communications bulk may contain thousands of communication sessions. It is not visible in advance who are the senders of the communication sessions and what is the subject of the communications. This does not emerge until after communications are selected based on previously approved selection criteria.

8.3.1 The selection process

Selection of communications is carried out using selection criteria or key words. Selection criteria are, for example, data concerning the identity of a person or organisation (Article 27(3)(a), ISS Act 2002) or a number or other technical characteristic (Article 27(3)(b), ISS Act 2002). The criterion can be a telephone number, for example, or an e-mail address. Selection based on key words is done on the basis of a list of more general key words that are related to a particular subject of investigation (Article 27(3)(c), ISS Act 2002).

Selection criteria and lists of key words are passed through the communications bulk like a kind of filter. All communication sessions that match the selection criteria and key word lists are selected and transferred to another file. For the purposes of this review report the Committee uses the terms 'selection file' and 'bulk file'. The selection file contains all the selected communication sessions and is accessible to linguists and Sigint analysts so that they can further process the information, if so desired. The bulk file contains among other things the total volume of satellite communications obtained from non-targeted interception by NSO and Sigint detachments. In principle, the bulk file is not accessible to officers involved in the substantive intelligence process, but it is accessible to technicians and persons responsible for searching the bulk file (see also section 7.4).

In order to obtain the communications it is looking for, it is important for DISS to generate selection criteria and key words with the greatest possible specificity. The broader the selection

criteria and key words, the greater the volume of selected communications that are irrelevant to the task performance. This is not only undesirable from the perspective of privacy protection. Viewing and assessing all the selected communications is also a particularly intensive and time-consuming process. On the other hand it is also true that the more specific the selection criteria and key words, the greater the chances that relevant or even essential communications will be missed. It requires great expertise to prepare a good 'filter' for the selection process, which will yield high-quality intelligence. The analysts of the Sigint department take care of this process.

Usually, the selection criteria and key words that are used become more specific as an investigation continues and progresses. Working with previously selected communications, a Sigint analyst can adjust the selection criteria and key words to achieve the best possible results. This adjusting process requires time; this also depends on the (type of) investigation being conducted, the number of measures taken and the communications found after selection. At the beginning of an investigation it is therefore to a certain extent a matter of 'trying out' and hoping that relevant communications will turn up. This is inherent to the selection process and thus an important disadvantage of using the Sigint measure.

It should be noted, though, that the selection result depends to a high degree on what is initially obtained 'by chance' from non-targeted interception. Searching in support of non-targeted interception may make a substantial contribution to securing the most relevant communications for the performance by DISS of its tasks (see section 7.4.2).

8.3.2 Permission procedure

The permission of the minister of Defence is required for the selection of communications using selection criteria (which, briefly stated, is a name or number). The law provides that the same permission rules must be applied as those laid down in Article 25, ISS Act 2002, because the legislature assumed that it concerns 'targeted' selection of data. This means that the selection is directed at a specific person or organisation. The application for permission must in any case state the data concerning the identity or the number or technical characteristic to be used as selection criterion and also the reason why selection is desired. Permission is granted for a maximum period of three months and may be renewed every three months.[101]

If after the maximum three-month period permission is not renewed or if no application for renewal is submitted, the selection criterion in question must be removed immediately so that the selection ceases. This process has been automated at the Sigint department. The guarantee that selection will take place exclusively with the minister's permission is therefore incorporated in the system.

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

Different rules apply to selection based on key words: permission may be granted for a maximum period of one year and may be renewed every year. The minister's permission is not granted for individual key words but for the subject to which the key words are related. Preparing the list of key words is done by the Sigint analysts at DISS. Lists of key words may be adjusted daily, as needed. The legislature has given the following explanation regarding lists of key words:

> "As a rule, a list of key words relating to a subject will consist of (combinations of) specific technical terms and designations in various languages. The list is prepared in such a way that optimal use is made of the selection system to find the desired information. A list of key words for use in the context of an investigation into the proliferation of certain dual-use goods to a specific country or region, for example, may consist of names of certain chemical substances and chemical compounds in combination with the country or region. A slightly simplified example is that of searching for communications containing the word sodium and at the same time within two positions also the word chlorid or fluorid. A list of key words to be used in an investigation into the export of a rocket system to certain countries or regions could consist of various names used to designate the specific rocket system, and, if appropriate, project names or designations of the various components forming part of the system in question."[102]

According to the legislature, this type of search is not a targeted search for data relating for example to a specific individual and directly involving his privacy. It merely involves a selection of data which are in a general sense relevant to investigations on which DISS is working. However, as soon as such a search results in specific persons entering the picture, whom DISS then wishes to subject to targeted selection, DISS will require permission of the minister to do so.[103]

The Committee has established that the lists of key words used by the Sigint department include names of persons and organisations. DISS stated to the Committee that the names mentioned in the lists are exclusively names of persons and organisations with respect to whom or which the minister has approved selection criteria. Adding these names to the lists of key words can yield better selection results through the fact that the names are linked to related key words. DISS stated that the names are only included in the lists of key words for the duration of the minister's permission. This is checked by random sampling by the legal expert of the Sigint department. The Committee has not found internal rules or a procedure for this practice.

The Committee holds the opinion that DISS can freely include names of persons and organisations in the lists of key words if and as long as valid permission of the minister is in place for selection on the basis of selection criteria with respect to those persons and organisations. The Committee considers it necessary to introduce additional safeguards to prevent unlawful use. It considers monitoring by random sampling by the department lawyer to be insufficient.

---

[102] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 33.
[103] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 45.

The Committee recommends that DISS formalises internal rules regulating the procedure for including names of persons and organisations in lists of key words. The Committee also recommends introducing additional safeguards against unlawful use of this power.

Section 8.3.6 deals with the obligation laid down in Article 27(7) to report selection based on key words.

8.3.3 Generic identities[104]

The Committee has established that in a number of cases permission was requested and granted for selection of a particular category of persons and organisations. DISS had named broadly formulated generic identities covering a particular 'type' of persons or organisations. When a person or organisation falling within a generic identity entered the picture, selection criteria with respect to that person or organisation could be immediately included in the selection programme without obtaining specific permission, since permission for the generic identity had already been obtained.

DISS has put forward various reasons for applying for generic permission for selection. In certain cases a specifically formulated application for permission is found to be too restrictive. A generic identity obviates the problem of covering frequently changing or still unknown persons or organisations. DISS must be able to respond quickly to changing circumstances. Mentioning specific names may moreover be difficult because of the use of aliases and because of different notations.

The Committee has found in the course of its investigation that it was agreed in the past with the Legal Affairs department of the ministry of Defence that generic permission would only be granted in relation to a defined investigation subject, namely a particular region or a particular conflict. The investigation subject must be stated in the application for permission. It was considered unadvisable to submit endless lists of frequencies and other unappealing information to the minister. Preference was given to a clearly described generic identity because it was a workable procedure.

DISS has stated that internal checks are carried out regarding persons and organisations with respect to whom criteria were included in the selection programme before specific permission had been obtained. No such early selection will take place without the approval of the Sigint department's legal expert. The Committee points out the vulnerability of the role of this legal expert who bears (too) great a responsibility in this matter. Since early 2010 DISS has adopted

[104] In section 7.2.2 the Committee mentioned that permission had been obtained for targeted interception of communications with respect to generic identities. In its investigation into the exercise by DISS of the power of selection the Committee came across the same procedures. This has resulted in some repetition in the text of this section and of section 7.2.2.

the practice of expressly stating the names of the persons and organisations that were included in the selection programme before specific permission had been obtained in the first following application for permission. The Committee has not found internal rules or an internal procedure in which the above practice has been laid down.

The Committee holds the opinion that the above procedure is not consistent with the ISS Act 2002. It was the decision of the legislature to make the same rules applicable to selection of data on the basis of selection criteria linked to a person or organisation as those applying to targeted interception. The law requires that the application for permission must at the least show with respect to whom the power can be exercised and why. The generic identities named in the applications for permission are so broad that in the opinion of the Committee it is impossible to foresee exactly which persons and organisations fall or may come to fall under this generic identity.[105] This is not changed by the internal checking by the department's legal expert.

Unlike its opinion on naming generic identities for the purpose of targeted interception, the Committee has some sympathy for the practice of naming generic identities for selection purposes. The legislature proceeded on the assumption that selection is aimed at a specific person or organisation. But this is not always the case. When DISS starts an investigation or addresses a new investigation question, it is often far from clear to DISS which persons or organisations may yield the desired intelligence. So a certain degree of 'trying out' will have to take place for DISS to be able to acquire an intelligence position in the Sigint area within a relatively short time. This is inherent to the Sigint measure. In the Committee's opinion the statutory rules and the necessities of practice diverge on this point.

The Committee notes that DISS also uses other methods to try and identify 'targets' and collect selection criteria, for example consulting open sources and using information from partner services. The Committee holds that improved use can be made of the knowledge being built up by or already present in the team of the Intelligence department charged with the investigation in question when preparing and subsequently adjusting the selection criteria. The team can make a contribution to the characterisation and assessment of potential sources of information. It is also advisable for the team to be more involved with making the required the assessments concerning necessity, subsidiarity and proportionality in determining selection targets.

The Committee holds the opinion that after a certain time the selection should be sharply narrowed down, making less and less use of generic identities and increasingly using the identities of specific persons and organisations that have come into the investigation picture. Each application for permission will have to state whether and why permission for the generic identity is still necessary, which persons and organisations have meanwhile be included in the selection programme and for what reasons. The Committee can imagine that there is a connection between the degree to which the criteria are narrowed down and the importance of the investigation. In

[105] This issue will be discussed in greater detail in the secret appendix to this review report.

the case of a military mission abroad (category I area) which is about to take place, DISS must very quickly acquire a good Sigint position regarding the mission area. In that case DISS may start with broad selection criteria which it can sharply narrow down as the investigation begins to take shape. This is different, for example, in an investigation into the political intentions and military possibilities of a specific country (category II area). In this case the service has more time and scope to gather intelligence by other means (open sources, partner services). In this situation it is not necessary to start the investigation using broad selection criteria.

The Committee notes that Article 27, ISS Act 2002, does not allow the possibility of subsequently supplementing data concerning the identity of an organisation, with the result that it would not be possible to include newly-identified members in the permission granted with respect to an organisation. Article 25, ISS Act 2002, on the other hand, does allow this possibility (see also section 7.2.2). Since it was the intention of the legislature that selection using selection criteria should be governed by the same rules as those applying to the application of Article 25, ISS Act 2002,[106] the Committee holds that it is strongly arguable that the identity of an organisation may subsequently be supplemented for selection purposes as well. The Committee suggests considering to amend the ISS Act 2002 on this point.

8.3.4 Stating reasons[107]

Article 27, ISS Act 2002, not only requires that an application for permission for selection shows with sufficient precision with respect to whom the power will or may be exercised, but also what is the reason for the selection. Each application must be substantiated by reasons, from which it must clearly emerge how the requirements of necessity, proportionality and subsidiarity are met. The Committee has established that many applications for permission are insufficiently substantiated by reasons.

It is true that in the applications for permission DISS states the reason for conducting the wider investigation for the purposes of which the power is to be used. It gives attention to the investigation subject (for example a particular region designated in the Statement of Intelligence and Security Needs or the Designation Order) and the subject elements in which DISS is interested. The Committee holds the opinion that in nearly all cases these explanations give a clear picture of the investigation and provide grounds for the use of special powers in that context. The Committee draws attention to the fact that when special powers are exercised for the purpose of performing the (a) task and the (e) task, it is necessary to state what is the potential threat to national security (see section 5.1).

---

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

[107] In section 7.2.3 the Committee described that the reasons stated for applications for permission for targeted interception do not come up to the mark. In its investigation of the exercise by DISS of the power of selection the Committee came across the same imperfections. This has led to some repetition in the text of this section and of section 7.2.3.

The Committee has established, however, that applications state only very summary reasons focusing specifically on the person or organisation. In the case of generic identities named by DISS, moreover, the reasons given are often trivial and formulated in too general terms. The Committee has also found that applications for permission frequently state purely standard reasons.

In section 8.3.3 the Committee stated that in certain circumstances it has sympathy for the practice of applying for generic permission in the early stages of an investigation. The Committee holds the opinion that the application must state whether and why permission for the generic identity is (still) necessary. The Committee holds that it does not suffice to merely state that the named identities may possibly communicate about a subject in which DISS is interested.

It is the opinion of the Committee that for each person or organisation who or which subsequently enters the investigation picture the service must state reasons why selection of his or its communications is considered necessary. It must also state expressly what is the objective of the selection in the context of the investigation and on what the service bases the expectation that the intelligence obtained from the selection will contribute to achieving the objective.[108] So it must make a link between the wider investigation that is being carried out and the necessity of selecting the communications of the specific person or organisation. This link will be different for each person or organisation.

Subsequently, an application for renewal must devote express attention to the intelligence obtained from the selection and its added value for the investigation, not in a general sense but specifically with respect to the person or organisation. It is the opinion of the Committee that commonplace remarks that the exercise of the special power has contributed to meeting the need, or has resulted in (unspecified) reports or has confirmed the existing standard picture do not suffice.

In addition to necessity, an application for permission must also state how the requirements of proportionality and subsidiarity are met. With respect to these requirements, so the Committee has found, the service also uses standardized texts which are aimed at covering the proportionality and subsidiarity issues of the exercise of special powers for an entire investigation at once. Moreover, it is not clear or not sufficiently clear from the general passages included in the applications what assessments have been made. Usually, the application merely concludes that the required intelligence cannot be adequately obtained by exercising another (special) power or by cooperating with foreign services.

The Committee holds the opinion that this procedure does not satisfy the requirements laid down in the ISS Act 2002 or in the assessment framework formulated in Articles 31 and 32 of the Act. The legislature has enacted that prior to and during the exercise of a specific special

[108] The Committee considers reasons such as "is associated with terrorism" or "communication traffic of these institutions is a valuable source of information for the investigation" to be meaningless and insufficiently specific.

power it must be assessed on the basis of the requirements of proportionality and subsidiarity whether it is (still) lawful to exercise the power. It is not clear or not sufficiently clear from the applications for permission or renewal of permission that these assessments have actually been made. As was discussed in section 6.3 above, the process preceding a decision to use the power of selection likewise does not demonstrate sufficiently that these assessments are made.

Since the Committee has insufficient knowledge of the reasons underlying selection, it is unable to assess the lawfulness of the exercise of the power of selection pursuant to Article 27(3)(a) and (b), ISS Act 2002.

In section 6.3 the Committee recommended that DISS introduces a procedure requiring the assessments regarding necessity, proportionality and subsidiarity of the use of Sigint measures to be made by the team (of which the Sigint analyst is a member) and laid down in writing. By extension, the Committee recommends that DISS includes in its applications for permission submitted to the minister which assessments have actually been made regarding necessity, proportionality and subsidiarity, specified per person or organisation against whom or which the power will be exercised.

8.3.5 Removing certain identities from the specific search criteria

Selection of communications is only lawful if the requirements of necessity, proportionality and subsidiarity (Articles 18, 31 and 32, ISS Act 2002) are met. The intelligence obtained by exercising the power of selection is an important factor in determining whether it is justified to renew the permission to exercise the power. It must be assessed each time whether the intelligence obtained is proportionate to the infringement of (privacy) rights. If this is not the case, the selection of the communications of the person or organisation in question must be terminated. At the Sigint department this is known as removing identities from the specific search criteria.

The Committee has found in its investigation that identities were not removed very often in the past. Criteria sometimes continued to be included in the selection programme without producing any results. Recently, this has changed at the Sigint department. Analysts are asked to review on a three-monthly basis which identities can be removed from the search criteria. The legal expert of the Sigint department monitors the process. Since early 2010, moreover, lists of removed identities are annexed to the applications for permission submitted to the minister, so that the minister, too, can see that criteria are not maintained in the selection programme longer than is necessary. The Committee has not found evidence that this practice has been laid down in internal rules.

The Committee considers the development described above to be of essential importance to the lawful exercise of the power of selection. It recommends that DISS adopts internal rules formalising the practice. The Committee further holds the opinion that each application for

renewal of permission should devote express attention to the result of the selection and its added value for the investigation. This should be specified per person or organisation.

8.3.6 Duty to inform

Article 27(7), ISS Act 2002, provides that one or both Chambers of the States-General must be confidentially informed whenever permission is granted to exercise the power of selection based on key words, stating the subject and the reason for the selection.

The Committee has found in the course of its investigation that on request the Sigint department informs the Legal Affairs department of DISS about the lists of key words. If so desired, the subjects of the key words can then be discussed with the Committee. Furthermore, the Committee is free to inspect the lists of key words for the purposes of its investigation activities. It did in fact do so in the present investigation. There is, however, no question of any proactive sharing of information by DISS. In fact, so far the Committee has not requested DISS to do so.

The present investigation further shows that the subjects of the lists of key words are not discussed on a structural basis with the Parliamentary Standing Committee on Defence or the Committee on the Intelligence and Security Services (ISS Committee). The Committee does not know whether the subjects have come up for discussion in these committees in the past, nor whether it is considered advisable for the committees to be informed about the subjects of the lists of key words on a structural basis.

The Committee has established that most of the applications for permission submitted to the minister nonetheless state that the ISS Committee and the Committee are confidentially informed of any permission granted to exercise the power of selection based on key words relating to an investigation subject. The Committee considers these statements to be incorrect and holds the opinion that they give the minister a wrong impression.

9. Reporting and distributing Sigint

9.1 Reporting

After the intercepted communications have been processed and analysed for the purposes of the performance by DISS of its tasks, the reporting stage begins. Signals intelligence reports are prepared in which the relevant Sigint relating to a particular subject is included. Signals intelligence reports may contain both Sigint obtained by the department itself and Sigint received from partner services.

Within the organisation, the signals intelligence reports are provided to the Intelligence department. There, the Sigint, together with other intelligence acquired, can be further incorporated into a final report on a particular subject. These final reports are products for which in principle all the available sources have been used. The Sigint that has been obtained is therefore only an element in the larger whole. This implies a certain degree of dynamics. For example, the Sigint that has been obtained can be reinforced by other sources, making the picture more complete. But the Sigint aspect can also be given a subordinate role in the final report. The Intelligence department analyst determines the content of the final report in consultation with the team.

As a rule, the Sigint department analysts will get feedback on the Sigint they have supplied. This is usually done orally in corridor chats and sometimes in writing. In addition, Sigint analysts can read in the final report how the Sigint supplied by them has been incorporated. Based on this information a Sigint analyst can adjust his interception and selection needs.

In section 7.2.3 and in section 8.3.5 the Committee held that the results obtained by exercising the power of interception or selection are an important factor in determining whether it is justified to renew permission to exercise these powers. It must therefore be considered on the basis of the results whether the statement of needs should be adjusted. This requires new assessments of the necessity, proportionality and subsidiarity of exercising the power to use Sigint.

The Committee considers it important that Sigint needs are adjusted by the team (of which the Sigint analyst is a member). In the opinion of the Committee, insufficient attention is currently being given to this issue.

9.2 National distribution

The final reports prepared by the analysts of the Intelligence department are subsequently distributed to external parties. The products are distributed to the same parties mentioned in section 6.1 as the parties that state intelligence needs. These include the Dutch armed forces, the ministry of General Affairs, the ministry of Foreign Affairs, national and international partner services. Articles 36–42, ISS Act 2002, on the distribution of data to external parties apply to this distribution of Sigint.

The teams of the Intelligence department maintain contacts with the national parties that have stated intelligence needs, about their intelligence needs and the intelligence reports subsequently provided to meet these needs. The Committee has found in the course of its investigation that the task groups of the Sigint department also maintain contacts to a greater or lesser degree with national parties that have stated needs. With some of these parties they also share so-called half-finished products containing Sigint only. This avoids the longer process via the Intelligence

department, in which the Sigint is incorporated in a final report, and gives the Sigint department itself control of when and how Sigint is shared with external parties.[109]

On account of international rules and guidelines on how to handle Sigint to which DISS has committed itself, it is necessary in certain cases that authority to maintain contacts with and provide intelligence to external parties is vested in the Sigint department or tasks groups of this department.

9.3 Distribution to partner services

The Sigint department conducts its own customer relationship management with international partner services. Consequently, Sigint is exclusively distributed to international partner services by the Sigint department. In this context a distinction must be made between providing evaluated Sigint (reports) and other forms of distributing Sigint.

Evaluated Sigint or Sigint reports that are provided to partner services contain Sigint that has already been processed by DISS. When distributing this data, DISS must observe the legal framework for providing data that follows from the ISS Act 2002. The Committee has elaborated this legal framework in a previous report.[110] DISS is authorised to provide data to foreign services either under Article 36(1))d), ISS Act 2002, for the purposes of the proper performance of its own tasks or under Article 59(2), ISS Act 2002, in which case the interest of the foreign service in being provided with data is the guiding principle. The legislature has set further criteria for the provision of data under Article 59(2), ISS Act 2002. The same Article provides that data may be provided insofar as (a) the interests to be served by the counterpart services are not incompatible with the interests to be served by DISS, and (b) providing the data is not incompatible with the proper performance by DISS of its tasks. Furthermore it is relevant to mention the general standards parameters that apply to the processing of data (Articles 12-16, ISS Act 2002) and which include the requirements of necessity and proper and due care. The Committee further draws attention to the additional requirements laid down in the ISS Act 2002 and the legislative history of the Act with respect to providing personal data and to compliance with the third-party clause, as laid down in Article 37, ISS Act 2002.[111]

The Committee takes the position that the other forms of exploiting Sigint[112] do not so much

[109] For completeness' sake the Committee notes that after this review report was drafted, the minister indicated that DISS had recently decided that contacts with national parties stating needs would no longer be maintained by the task groups of the Sigint department. Half-finished products will henceforth be issued by DISS-wide teams.

[110] See also review report no. 22A. The cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, section 7.

[111] The Committee will discuss these issues in greater detail in the review report on the current investigation on the cooperation by DISS with foreign intelligence and/or security services.

[112] This subject is discussed in greater detail in the secret appendix to this review report.

concern provision of data but rather giving technical support as referred to in Article 59(4), ISS Act 2002.

The ISS Act 2002 sets two conditions for giving technical support within the meaning of Article 59(4) of the Act. Support is only permitted insofar as the interests to be served by the foreign services are not incompatible with the interests to be served by DISS (Article 59(4)(a), ISS Act 2002) and insofar as giving support is not incompatible with the proper performance by DISS of its tasks. According to the legislative history the basis for assessing whether incompatible interests may perhaps exist must include Dutch foreign policy, including Dutch human rights policy.[113] Moreover, DISS must perform its tasks in subordination to the law. This means that the interests to be served by DISS must be deemed to include the standards, and definitely also the fundamental and human rights standards, laid down in the Constitution and in the international conventions ratified by the Netherlands.[114] An example mentioned in legislative history of a situation in which the proper performance of its statutory tasks by DISS is incompatible with giving support to a foreign service is the frustration of own ongoing operations of DISS. The Committee further observes that the type of support that is requested is relevant, too. It must, among other things, fit within the legal parameters to be observed by DISS. If a certain form of support is incompatible with those parameters, it would be contrary to the proper performance by DISS of its statutory tasks if it were to give the support notwithstanding.[115]

Before giving support, DISS must assess whether the above conditions are satisfied. In its investigation the Committee has not found any indication that DISS assesses whether this is the case before giving support. In the opinion of the Committee it is necessary that this is done. The Committee considers that for this purpose it will suffice if DISS makes a general assessment whether this far-reaching form of cooperation with the foreign services in question is lawful.

Pursuant to Article 59, paragraphs (5) and (6), ISS Act 2002, support may only be given with the permission of the minister involved. The Sigint department has arranged a standard practice with a number of partner services that it will provide certain types of support. These arrangements are made in the context of broader agreements with foreign services ((Memoranda of Understanding) which have been approved by the minister. The Committee holds the opinion that a broad, prior permission from the minister per individual foreign service to which support will be given, constitutes sufficient compliance with Article 59, paragraphs (5) and (6), ISS Act 2002.

Furthermore, when DISS exercises special powers in support of a foreign service, it must comply with the statutory requirements applying to the exercise of these powers. This means that in this case, too, the requirements of necessity (for the performance of its own task), proportionality and

[113] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 74.
[114] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 65.
[115] Idem, p. 64.

subsidiarity must be satisfied.[116] In the course of its investigation the Committee has not found any evidence, however, that DISS submits applications to the minister, substantiated by reasons, for permission to exercise special powers specifically for the benefit of partner services.

The Committee recommends that DISS, before giving support to a foreign service, assesses whether the conditions are satisfied that the support may not be incompatible with the interests to be served by DISS and may not conflict with the proper performance of its tasks. The Committee further recommends that DISS follows the applicable procedures when exercising special powers, also if they are exercised for the purposes of giving support to a partner service. The Committee further recommends bringing the internal (permission) procedures in line with these recommendations.

10. Conclusions and recommendations

10.1 It is the opinion of the Committee that the legislature, by taking the position that searching does not infringe confidentiality of the telephone, ignores the fact that searching is in fact directed at communication content. In the opinion of the Committee this is not changed by the fact that searching includes only a brief examination of communication content and is not directed at gaining knowledge of the full content of the communication. (section 4.3.3)

10.2 Given the organisation of the process preceding a decision to take Sigint measures, the Committee holds the opinion that it should be assessed at an earlier stage whether the requirements of necessity, proportionality and subsidiarity are satisfied. The Committee also considers it necessary that these assessments are not made exclusively by the Sigint analyst.
The Committee recommends that DISS introduces a procedure according to which the assessments regarding necessity, proportionality and subsidiarity of taking Sigint measures are made by the team (of which the Sigint analyst is a member). With a view to internal accountability and external monitoring the Committee draws attention to the importance of laying down in writing all assessments that have actually been made and which form the basis for taking Sigint measures. Thus far, this has been done on too limited a scale. (section 6.3)

10.3 It is the opinion of the Committee that the absence of a legal basis for exercising special powers abroad can only be approved if the ISS Act 2002 is applied by analogy. In the opinion of the Committee the procedures for exercising special powers prescribed in the ISS Act 2002 must therefore also be observed when they are exercised abroad. This

[116] See also review report no. 22A. the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, section 8.1.

means among other things that any targeted interception of communications by a Sigint detachment requires the prior permission of the minister.The same applies to the selection of communications obtained by Sigint detachments by non-targeted interception.
The Committee can imagine urgent situations requiring immediate action to furnish intelligence support to crisis management operations. The Committee appreciates that in such exceptional situations there is no realistic possibility of contacting the minister before taking action. In this situation the Committee considers it important, though, that the minister is informed as soon as possible of the special powers that have been exercised without prior permission. In the opinion of the Committee it is, moreover, necessary to prepare detailed written reports of both the exercise of the power and the subsequent coordination with the minister.
The Committee recommends that DISS brings procedure and practice of deploying Sigint detachments into line with the foregoing. (section 7.1.2)

10.4 The Committee has established that in a number of cases permission was asked and obtained for targeted interception with respect to a particular category of persons and organisations. DISS had designated broadly formulated generic identities covering a particular 'type' of persons or organisations. It is the opinion of the Committee that this procedure is not consistent with the ISS Act 2002 and does not do sufficient justice to the statutory protection of the (privacy) rights of those whose communications are or may be intercepted. The generic identities designated in the applications for permission are so broad that in the opinion of the Committee it is impossible to foresee exactly which persons and organisations fall or may fall under this identity. This is not changed by the internal check done by the department's legal expert with respect to persons and organisations whose communications have been included in the interception programme before specific permission had been obtained. (section 7.2.2)

10.5 The Committee does appreciate that in a situation where exactly the same reasons apply to the interception of the communications of certain persons or organisations, the service may bundle the applications for permission into one application. In this case it is necessary that it is absolutely clear which persons or organisations fall within the bundled group. In the opinion of the Committee the submission of a bundle of applications does not harm the protection of the (privacy) rights which the procedure laid down in the ISS Act 2002 envisages to safeguard. Moreover, it meets the wish to keep the applications for permission clear and manageable. (section 7.2.2)

10.6 Under certain circumstances the Committee considers it acceptable that a person who is identified as falling within a bundled group after permission for the bundled group was granted, is ranged under the permission granted for the bundled group. In that case DISS must state in the first following application for renewal why the person is considered to belong to the group of persons in question.The Committee has found that since 2010 the

service follows the practice of including the names of persons whose communications have been added to the interception programme after generic permission was granted. No reasons are stated, however, why the person in question is considered to belong to the organisation or group. The Committee considers this necessary. The Committee recommends, moreover, that DISS adopts an internal written procedure formalising its actual practice. (section 7.2.2)

10.7 The Committee has established that applications for permission for targeted interception are in many cases insufficiently substantiated by reasons.
It is the opinion of the Committee that it must be assessed with respect to each individual or organisation or for each bundled group whether targeted interception of his or its communications satisfies the requirements of necessity, proportionality and subsidiarity. It is not clear or not sufficiently clear from the applications for permission or for renewal of permission that these assessments have actually been made. Since the Committee has insufficient knowledge of the reasons underlying interception, it is unable to assess the lawfulness of interception pursuant to Article 25(1), ISS Act.
The Committee recommends that DISS includes the assessments actually made by the team (of which the Sigint analyst is a member) regarding necessity, proportionality and subsidiarity in the applications for permission submitted to the minister, specifically for each person or organisation with respect to whom or which the power will be exercised. (section 7.2.3)

10.8 With respect to searching for the purposes of targeted interception the Committee has not found indications that metadata has been processed wrongfully. (section 7.4.1)

10.9 It is not permitted to follow a transmission longer than is strictly necessary to establish the sender's identity and the relevance for the performance by DISS of its tasks. The Committee has not found any indications that this has happened or is happening. (section 7.4.1)

10.10 With respect to searching for the purposes of non-targeted interception the Committee has not found any indications that metadata has been processed wrongfully. (section 7.4.2)

10.11 The Committee holds the opinion that it is not possible in all cases to draw a clear dividing line between metadata and communication content. This will have to be assessed on a case by case basis. Insofar as examining metadata coincides with examining content data, all the data together must be assumed to be content data. (section 7.4.2)

10.12 The Commission has found in its investigation that there is a difference of opinion between NSO and the Sigint department on the question whether NSO may examine communication content for the purposes of the searching processes it carries out.

In actual practice both NSO and the Sigint department carry out such searching activities. The Committee holds the opinion that examining communication content more frequently than is strictly necessary is not permitted. This would entail unnecessary infringement of the (privacy) rights of third parties. The Committee recommends that NSO and the Sigint department make an arrangement which makes it clear which service will exercise this power. (section 7.4.2)

10.13 When conducting its investigation the Committee noticed that search orders placed with NSO are usually formulated rather broadly. The Committee has found that it is sometimes difficult for NSO to deduce which searching activities are (most) important for the Sigint department. The Committee recommends that DISS will, where possible, further specify the searching orders placed with NSO and lay down the specifications in writing. (section 7.4.2)

10.14 The Committee has established that DISS also exercises the power of searching for the purpose of the selection process. DISS has taken the position that there is no essential difference between this form of searching and searching for the purpose of non-targeted interception. According to the service, the only difference is the moment at which the two forms of searching take place in the Sigint process. The Committee, however, holds the opinion that by taking this position DISS disregards the distinction that can be made between the objectives at which the searching is directed and the grounds for infringing privacy by examining communication content. The Committee has established in this context that the actual practice of exercising the power to search has drifted a long way from the statutory power to search.

The Committee has also established that there is only a partial internal description of the operating procedure at DISS with regard to searching for the purpose of the selection process and that it has not been formalised. In the course of its investigation, and also based on interviews held with the persons involved, the Committee has described actual practice at DISS. It holds the opinion that the practice as described should be laid down in a written operating procedure and recommends that DISS does so as soon as possible.

The Committee has established that there are various different matters that may provide the reason and the objective for carrying out a search activity for selection purposes. It has in any case distinguished the following common practices:

1. Searching the communications bulk to determine whether the desired intelligence can be generated using the selection criteria for which permission has been obtained;
2. Searching the communications bulk to identify or characterise potential targets;
3. Searching the communications bulk for data from which future selection criteria can be derived for the purposes of an expected new investigation area. (section 7.4.3)

10.15 The Committee considers the first searching practice permissible. Searching the communications bulk to determine whether the required intelligence can be generated using the selection criteria for which permission has been obtained serves to support the exercise of the special power of selection. The infringement resulting from the searching process is obviated by the minister's permission to apply selection with respect to the person or organisation mentioned. Furthermore, searching can result in a more targeted selection.
The Committee holds the opinion that the safeguards introduced by DISS to prevent any unlawful exercise of the power provide insufficient protection. Apart from the technical measures introduced in the system, the separation between the activities of the persons responsible for searching and the analysts responsible for analysing and reporting on content and also the restrictions imposed in practice on providing data content are based exclusively on informal arrangements and depend on the goodwill of the employees concerned.
The Committee recommends that DISS introduces an operational procedure that guarantees the separation between searching and reporting on content, and formalises it in an internal document. (section 7.4.3)

10.16 The Committee holds the opinion that the infringement of the (privacy) rights of third parties resulting from the second and third searching practices for selection purposes has no basis in the ISS Act 2002. It is the opinion of the Committee that the power of searching as laid down in Article 26, ISS Act 2002, and further explained in the legislative history, has the objective of supporting the exercise of the powers of Articles 25 and 27, ISS Act 2002. In other words, searching is done exclusively for the benefit of targeted interception and for the benefit of non-targeted interception followed by selection. The Committee holds the opinion that the second and third searching practices for selection purposes do not contribute to support or optimize the selection process but are aimed at a new use of selection after non-targeted interception. Article 26, ISS Act 2002, provides insufficient basis for these forms of searching.
The Committee has established that the statutory provisions and actual practice are at odds on this point. It suggests that the legislature considers whether it is necessary to confer the powers in question on DISS (and GISS) with due regard to the protection of privacy. (section 7.4.3)

10.17 The Committee has found in the course of its investigation that DISS exercised special powers to collect information for decryption purposes and for the purpose of related (technical) research. The Committee has established that the above special powers are on the verge of what is permitted by law. The Committee therefore urges DISS to exercise restraint in exercising special powers and to pay special attention to substantiating decisions to do so by sound reasons. (section 8.1)

10.18 The Committee has established that the lists of key words used by the Sigint department include names of persons and organisations. The Committee holds the opinion that DISS can freely include names of persons and organisations in the lists of key words if and as long as valid permission of the minister is in place for selection on the basis of selection criteria with respect to those persons and organisations. The Committee considers it necessary to introduce additional safeguards to prevent unlawful use. It considers monitoring by random sampling by the department lawyer to be insufficient.

The Committee recommends that DISS formalises internal rules regulating the procedure for including names of persons and organisations in lists of key words. The Committee also recommends introducing additional safeguards against unlawful use of this power. (section 8.3.2)

10.19 The Committee has established that in a number of cases permission was requested and granted for selection of a particular category of persons and organisations. DISS named broadly formulated generic identities covering a particular 'type' of persons or organisations. It is the opinion of the Committee that this procedure is not consistent with the ISS Act 2002. It was the decision of the legislature to make the same rules applicable to selection of data on the basis of selection criteria linked to a person or organisation as those applying to targeted interception. The law requires that at the least the application for permission shows with respect to whom the power can be exercised and why. The generic identities named in the applications for permission are so broad that in the opinion of the Committee it is impossible to foresee exactly which persons and organisations fall or may come to fall under this identity. This is not changed by the internal checks by the department's legal expert. (section 8.3.3)

10.20 Unlike its opinion on naming generic identities for the purposes of targeted interception, the Committee has some sympathy for the practice of naming generic identities for selection purposes. The legislature proceeded on the assumption that selection is aimed at a specific person or organisation. This is not always the case, however. When DISS starts an investigation or addresses a new investigation question, it is often far from clear to DISS which persons or organisations may yield the desired intelligence. . So a certain degree of 'trying out' will have to take place for DISS to be able to acquire an intelligence position in the Sigint area within a relatively short time. This is inherent to the Sigint measure. In the Committee's opinion the statutory rules and the necessities of practice diverge on this point.

The Committee holds the opinion that after a certain time the selection should be sharply narrowed down, making less and less use of generic identities and increasingly using the identities of specific persons and organisations that have come into the investigation picture. Each application for permission will have to state whether and why permission for the generic identity is still necessary, which persons and organisations have meanwhile been included in the selection programme and for what reasons. (section 8.3.3)

10.21 The Committee notes that Article 27, ISS Act 2002, does not allow the possibility of subsequently supplementing data concerning the identity of an organisation, with the result that it would not be possible to range newly-identified members under an organisation.The Committee suggests considering to amend the ISS Act 2002 on this point. (section 8.3.3)

10.22 The Committee has established that applications for permission for selection after non-targeted interception are in many cases insufficiently substantiated by reasons.
It is the opinion of the Committee that it must be assessed with respect to each individual or organisation why selection of his or its communications satisfies the requirements of necessity, proportionality and subsidiarity. It is not clear or not sufficiently clear from the applications for permission or for renewal of permission that these assessments have actually been made. Since the Committee has insufficient knowledge of the reasons underlying selection, it is unable to assess the lawfulness of selection pursuant to Article 27(3), subparagraphs (a) and (b), ISS Act.
The Committee recommends that DISS includes in its applications for permission submitted to the minister which assessments have actually been made regarding necessity, proportionality and subsidiarity, specified per person or organisation against whom or which the power will be exercised (section 8.3.4)

10.23 The Committee has found in its investigation that identities were not removed very often in the past. Recently, this has changed at the Sigint department.The Committee considers this to be of essential importance to the lawful exercise of the power of selection. It recommends that DISS adopts internal rules formalising this practice. The Committee further holds the opinion that each application for renewal of permission should devote express attention to the result of the selection and its added value for the investigation. This should be specified per person or organisation. (section 8.3.5)

10.24 The Committee has established that most of the applications for permission submitted to the minister wrongly state that the ISS Committee and the Review Committee are confidentially informed of any permission granted to exercise the power of selection based on key words related to an investigation subject. The Committee considers these statements to be incorrect and holds the opinion that they give the minister a wrong impression. (section 8.3.6)

10.25 The Committee considers it important that Sigint needs are adjusted by the team (of which the Sigint analyst is a member). In the opinion of the Committee insufficient attention is currently being given to this issue. (section 9.1)

10.26 The Committee takes the position that certain forms of distributing Sigint services consist of giving (technical) support as referred to in Article 59(4), ISS Act.

In its investigation the Committee has not found any evidence that DISS, before giving support, assesses whether the conditions for support are satisfied. The Committee considers that for this purpose it will suffice if DISS makes a general assessment whether this far-reaching form of cooperation with the foreign services in question is lawful.
The Committee recommends that DISS, before giving support to a foreign service, assesses whether the conditions are satisfied that the support may not be incompatible with the interests to be served by DISS and may not be in conflict with the proper performance of its tasks. (section 9.3)

10.27 The Committee holds the opinion that a broad, prior permission from the minister per individual foreign service to which support will be provided, constitutes sufficient compliance with Article 59, paragraphs (5) and (6), ISS Act. (section 9.3)

10.28 When DISS exercises special powers in support of a foreign service, it must comply with the statutory requirements applying to the exercise of these powers. This means that in this case, too, the requirements of necessity, proportionality and subsidiarity must be satisfied.[117] In the course of its investigation the Committee has not found any evidence, however, that DISS submits applications to the minister, substantiated by reasons, for permission to exercise special powers specifically for the benefit of partner services.
The Committee recommends that DISS follows the applicable procedures when exercising special powers, also if they are exercised for the purposes of giving support to a partner service. The Committee further recommends bringing the internal (permission) procedures in line with this recommendation. (section 9.3)

[117] See also review report no. 22A. the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, section 8.1.

11. Final observation

In this review report the Committee has established several times that the statutory rules regarding the powers of DISS in the field of Sigint do not correspond or are even at odds with (advisable) practice at DISS. This problem occurs *inter alia* in the implementation of the power to search (Article 26, ISS Act 2002), with respect to the non-cable-bound restriction of non-targeted interception (Article 27(1), ISS Act 2002) and with respect to the extent to which the selection process is directed (Article 27(3), ISS Act 2002).

The Committee suggests to consider whether it is necessary, with due regard to the protection of privacy, to give DISS (and GISS) wider powers that are more in line with the existing (advisable) practice. It is the responsibility of the legislature to give careful consideration to this matter.

The Committee points out that it is essential for those involved in this process that the procedures of the service(s) as followed in practice are clearly described and laid down in writing. The Committee recommends urgently that this will be done as soon as possible.

Thus adopted at the meeting of the Committee held on 23 August 2011.

APPENDIX IV

Review report 29: the official messages issued by GISS in the period October 2005 - May 2010

Review Report CTIVD no. 29

of the review report on the official messages issued by GISS in the period October 2005-May 2010

Table of contents

Review Report CTIVD no. 29

of the review report on the official messages issued by GISS in the period October 2005-May 2010

Summary

The Committee's investigation was directed at the official messages which GISS issued in the period from October 2005-May 2010. Based on the explanatory memorandum to the ISS Act 2002 the Committee has used the following definition of 'official message': the provision of information to a recipient who is authorized to take measures as a result of this information against the person or organisation mentioned in the message. In its investigation the Committee assessed, as it did in its first investigation of the official messages of GISS, whether the official messages issued by GISS satisfy the statutory requirements regarding the processing and external provision of (personal) data. In addition, the present investigation paid attention to the use made of the official messages in the follow-up procedures.

In view of the large number of official messages assessed by the Committee and the long period covered by the investigation, the Committee has only a limited number of critical remarks.

The official messages issued to the Public Prosecution Service, the Immigration and Naturalization Service (INS) and the category of 'other recipients' such as mayors and chiefs of police, generally satisfy the statutory requirements. The remarks of the Committee regarding these categories of official messages concern isolated defects, not structural ones. With respect to one official message issued to the INS the Committee holds the opinion that the indicated reliability regarding part of the information provided is not supported by the underlying file. In this respect, the official message is unlawful. In a number of cases, moreover, the Committee holds the opinion that GISS should have exercised greater care in formulating the text of the official message. Furthermore, the Committee has commented with respect to official messages issued to the Public Prosecution Service and the INS that the GISS should as far as possible seek to provide concrete, factual information, bearing in mind, of course, the need to keep secret its sources, its current level of knowledge and/or the operational methods of the service.

The official messages issued by GISS to the ministry of Economic Affairs, Agriculture and Innovation (EAA&I) in the context of applications for export permits are of a different nature than the aforementioned categories. These official messages are classified state secret, and they are to a certain extent standardized in nature. During the first part of the review period GISS did not consider this type of information provision to constitute official messages. Partly for this

reason GISS initially did not observe the statutory requirements very strictly. The Committee has established, however, that GISS has improved its procedure in recent years, with the result that they are now acting in compliance with the statutory requirements.

The fact that the official messages issued to the ministry of EAA&I are classified is not consistent with the basic principle of the ISS Act 2002 that an official message may be inspected without any objections by the person or organisation to which it relates. The Committee holds the opinion, however, that the classification of this category of official messages is justified, because the information provided will by definition reveal the knowledge level of GISS regarding companies in so-called countries of concern. It is important, though, that GISS is aware of the drawbacks associated with the classification of official messages, both for the ministry of EAA&I, which bases its decision wholly or partly on secret information, and for the exporter concerned who is not in a position to question the statements of GISS. In consultation with the ministry of EAA&I GISS must therefore try and find ways to promote that the ministry can take its decisions on the basis of an adequate information position. One possibility is to grant the ministry inspection of the documents underlying the official messages where necessary.

The Committee has included two categories of information provision in its investigation which previously were not classed as official messages. These are the category of provision of information to political party chairpersons concerning holders of or candidates for political office and the category of provision of information to the person charged with forming a new government or the prime minister on candidates for government posts. GISS may provide information on holders of or candidates for political office in response to a request for information from the party chairperson. GISS then provides the party chairperson with information obtained by an administrative check concerning the person in question in the databases of GISS. Prior to providing information on candidates for government posts GISS always does an administrative check at the request of the person charged with forming a new government or the prime minister. The Committee holds the opinion that these forms of information provision fall under the term 'official message' as defined by the Committee.

The messages concerning holders of or candidates for political office issued to political party chairpersons and the official messages concerning candidates for government posts issued to the person charged with forming a new government or the prime minister have certain structural shortcomings as regards both policy and implementation.

A particular shortcoming in official messages issued to party chairpersons is the absence of an indication of reliability or source reference, while in some cases personal data were provided orally instead of in writing. In addition, GISS wrongly considers doing an administrative check in its own databases in response to a request for information from a party chairperson to be a form of data provision. The Committee points out to GISS that the legal basis for such administrative checks is not the article of law pertaining to the provision of data, but the article of law pertaining

to data processing in general. This means that doing an administrative check in response to a request from a party chairperson must be necessary for the performance by GISS of its tasks, in the interest of national security. The Committee has found that there were three cases in which there was insufficient legal basis for the administrative checks done by GISS.

As regards the official messages to the person charged with forming a new government or the prime minister the Committee has found that GISS, contrary to the statutory provisions on the external provision of personal data, has opted for a policy of providing the information orally. As a result, and because of the absence of a report on the oral provision of information in 2007, it was impossible for the Committee to find out on which candidate for a government post information was provided in this period.

The Committee points out that it is precisely the political sensitivity of the provision of information concerning holders of or candidates for political office and candidates for government posts that is an urgent reason for thoroughly laying down all steps in writing.

List of abbreviations

belonging to the review report on the official messages issued by GISS in the period October 2005 up to and including May 2010

CT Infobox	Counterterrorism Infobox
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EAA&I	(ministry of) Economic Affairs, Agriculture and Innovation
GALA	General Administrative Law Act
GISS	General Intelligence and Security Service
INS	Immigration and Naturalisation Service
ISS Act 1987	Intelligence and Security Services Act 1987 (old)
ISS Act 2002	Intelligence and Security Services Act 2002
Sv	Code of Criminal Procedure
WMD	weapons of mass destruction

Review Report CTIVD no. 29

of the review report on the official messages issued by GISS in the period October 2005-May 2010

1. Introduction

Every year the General Intelligence and Security Service (GISS) issues a great number of official messages to bodies which are authorised to act on the information contained in the official message by taking measures. Essentially, therefore, the investigations carried out by GISS serve the purpose of giving the responsible bodies early warning against possible threats to the interests mentioned in the mandate of GISS.[1]

The Intelligence and Security Services Act 2002 (ISS Act 2002) does not contain a definition of the term 'official message'. The explanatory memorandum to the bill introducing the ISS Act 2002 contains a discussion of the term:

> "If it is to be expected on the basis of the information to be provided that the competent authority will take measures against the person concerned which will prejudice his legitimate interests, the information must be provided in a written (unclassified) official message. […] The basic principle is, that in the case of providing information to parties outside the circle of intelligence and security service, the information must be provided to the authority which is authorised to take measures for the preventive protection of the interests concerned or to take repressive action against impairment of the interests."[2]

Based on these passages the Review Committee for the Intelligence and Security Services (further referred to as: the Committee) arrives at the following definition of the term 'official message': the provision of information to a recipient who is authorised to act on the information by taking measures against the person or organisation mentioned in the message.

In 2006 the Committee issued a report on the official messages issued by GISS in the period from January 2004 - October 2005. The results of the Committee's investigation were mainly positive. The Committee's final conclusion was in fact that the official messages issued by GISS in that review period were in accordance with the law and had been prepared in an appropriate manner and with proper and due care.[3]

---

[1] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.

[2] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.

[3] Review report of the Committee no. 9a on the official messages issued by the AIVD in the period from January 2004 October 2005. *Parliamentary Papers II* 2005/2006, 29 924, no. 9 (annex), final observation. Also available at www.ctivd.nl.

Because of the increased use and importance of official messages in judicial proceedings, the Committee announced in the report that it would monitor the official messages of GISS on a regular basis. Such monitoring means that the Committee regularly examines the official messages that have been issued together with the corresponding files in the light of a number of statutory requirements (see section 3). As a result of the first findings of this monitoring the Committee decided to do a new in-depth investigation, so that it could conduct a more thorough investigation of the issues that had arisen upon a first reading of the official messages and underlying files. The present review report is the result of this investigation. The investigation paid particular attention to the use made of the official messages in the follow-up procedure.

By letter of 5 April 2007 this follow-up investigation of official messages was announced to the minister of the Interior and Kingdom Relations and the presidents of the two Chambers of the Dutch parliament. Initially, the investigation was aimed at the official messages issued in the period from October 2005 up to and including January 2007. After the investigation had been at a standstill for some time, mainly due to several time-consuming investigations instituted at the request of the minister of the Interior and Kingdom Relations[4] and the minister of Defence[5] and partly because the Committee's secretariat was short of staff, the Committee decided to extend the investigation to include the period from February 2007 up to and including May 2010. Consequently, this review report covers the official messages issued by GISS in the period from October 2005 up to and including May 2010.

The Committee drafted the review report on 10 August 2011 and sent it to the minister of the Interior and Kingdom Relations, requesting a reaction before 15 September 2011. On 27 September 2011 the Committee received a letter containing the minister's reaction to the draft report. The Committee adopted the review report on 28 September 2011.

2. Organisation of the investigation

The Committee included all provisions of information falling under the above definition of the term official message in its investigation. Two categories of information provision which were previously were not classed as official messages, were now included in the present investigation. These are the category of provision of information to political party chairpersons on holders of or candidates for political office and the category of provision of information to the person charged with forming a new government or the prime minister on candidates for government posts.

---

[4] Review Report of the Committee no. 17 on the assessment processes at GISS with respect to Mohammed B., *Parliamentary Papers II* 2007/08, 29 854, no. 22 (annex). Also available at www.ctivd.nl.

[5] Review report of the Committee no. 25 on the conduct of DISS with respect to two suspended employees, *Parliamentary Papers II* 2010/11, 29 924, no. 59 (annex). Also available at www.ctivd.nl.

In the course of its investigation the Committee examined the files of 566 official messages, checking whether they complied with the statutory requirements pertaining to data processing, and more specifically the requirements pertaining to the external provision of (personal) data. Three requirements played a key role in the investigation:

1. the official message must have its basis in Article 36, 38 or 39 of the ISS Act 2002;
2. the official message must be substantiated by the underlying information;
3. the official message must contain an indication of the reliability of the information or a reference to its source.

Insofar as there was reason for doing so, the Committee also investigated the lawfulness of how the data incorporated in the messages had been processed. Such processing may take the form, for example, of an administrative check by GISS in its own databases or the use of special powers.[6]

Another point for attention in the process of examining the files was the transparency of the files, since that is important element of internal accountability for the information provision and its external monitoring. A transparent and complete file is moreover an important basis enabling GISS to prepare an official message with due care.

In addition to examining the files, the Committee conducted interviews with lawyers employed at GISS. Some official messages were also discussed with employees and heads of the teams that drafted the official messages. The Committee spoke with an employee of the ministry of Economic Affairs, Agriculture and Innovation (EA&I) about the official messages issued to this ministry. The Committee also talked with two national public prosecutors for counterterrorism (further referred to as 'national public prosecutors') about the official messages issued to the Public Prosecution Service and with the head of a Regional Intelligence Service. Furthermore, the Committee also interviewed an employee of the Immigration and Naturalisation Service (INS), who works at GISS as the Service's liaison officer (further referred to as: the INS liaison).

When the first review report on the official messages of GISS was presented to the States General, the minister promised that GISS would adopt the Committee's recommendations in full. In the review report on the follow-up by GISS to the recommendations, the Committee established that GISS had taken action on all recommendations regarding the official messages, in particular those concerning the adjustment of internal rules.[7] In the present review report these recommendations will only be discussed insofar as the internal rules or their implementation give the Committee cause for further comments.

---

[6] During the review period the Committee also regularly (and separately) monitored the lawfulness of the use of the special powers under Articles 25 and 27 ISS Act 2002. See for an explanation of the structural monitoring activities of the Committee the Committee's annual report 2010-2011, available at www.ctivd.nl.

[7] Review report of the Committee no. 18a 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. *Parliamentary Papers II* 2007/08, 29 924, no. 25 (annex). Also available at www.ctivd.nl.

The review report has the following structure. Section 3 sets out the legal framework for issuing official messages. Sections 4 through 9 then discuss the different categories of recipients of official messages and the findings of the Committee. The relevant case law is reviewed in the process. Section 10 contains the conclusions and recommendations of the Committee.

This review report has no secret annex.

3. Legal framework for issuing official messages

3.1 Data processing generally

The law sets three requirements for data processing generally – the external provision of data is one of the types falling in this category – which are laid down in Article 12 ISS Act 2002 (paragraphs 2, 3 and 4). In the first place data may only be processed for a specific purpose and only insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. Secondly, data processing must take place in accordance with the law and with proper and due care. The last general requirement is that the data must be provided together with an indication of the degree of reliability or a reference to the document or source from which the information is derived.

These three general requirements will be further elaborated below and discussed specifically with regard to official messages.

3.1.1 For a specific purpose and insofar as necessary

The origin of the requirement that data may only be processed for a specific purpose and only insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act lies partly in a comparable provision in the ISS Act 1987,[8] the legislation that was the basis for the activities of the predecessor of GISS, the National Security Service.[9] In the ISS Act 2002 the requirement that data may only processed for a specific purpose was added to the requirement of necessity under the influence of the bill containing the Personal Data Protection Act, which included a provision that personal data may only be collected for specific, expressly defined and legitimate purposes.[10] [11]

[8] Article 16(1) ISS Act 1987.
[9] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 19.
[10] *Parliamentary Papers II* 1997/98, 25 892, no. 1, p. 3 (Article 7).
[11] *Parliamentary Papers II* 1997/98, 25 877, no. 8, p. 41.

Partly in reaction to two judgments of the Administrative Jurisdiction Division of the Council of State in which it was ruled among other things that the existing rules for inspection of personal data recorded by the National Security Service did not satisfy the requirements of the European Convention on Human Rights (ECHR),[12] rules were inserted into the ISS Act 2002 about the inspection of data processed by or for the use of the services (Articles 45-57 ISS Act 2002).[13] Furthermore, it was decided in response to a recommendation in the final report of the Parliamentary Committee of Inquiry into Investigation Methods (Van Traa Committee)[14] to create an explicit legal basis in the ISS Act 2002 for the provision of data to the Public Prosecution Service for the purposes of the investigation and prosecution of offences (Article 38 ISS Act 2002).[15] At the same time a legal basis was included for the provision of data, for urgent and serious reasons, to persons or bodies designated by or pursuant to a general administrative measure and charged with a public task (Article 39 ISS Act 2002). These statutory provisions pertain to activities of GISS which do not serve the interest of national security, though they do serve a public interest. Consequently, these activities fall outside the statutory description of tasks of GISS under to Article 6(2) ISS Act 2002.

In the light of this extension of the statutory activities of GISS compared to those of the National Security Service, the scope of the necessity requirement was also adjusted so that it does not only apply to data processing for the purpose of performing the statutory tasks – in the interest of national security – but also to the other forms of data processing provided for by or pursuant to the ISS Act 2002 or the Security Screening Act.[16] The wording chosen for Article 12(2):"necessary for the proper implementation of this Act or the Security Screening Act" comprises all statutory activities of GISS. However, the necessity requirement operates differently in the case of data processing for the purpose of the own task of GISS than in the case of data processing for the purpose of activities outside the own task of GISS.

When GISS issues an official message for the purpose of performing its tasks (Article 36 ISS Act 2002), providing the data to the body authorised to take measures against a person or organisation must be necessary in the interest of national security. In addition, providing the data must also serve a specific purpose. It emerges from the legislative history that this requirement relates to how the service actually performs its tasks.[17] Providing data pursuant to Article 36 ISS Act 2002 must therefore fit in with the way in which GISS actually performs its tasks.

Providing the Public Prosecution Service with data that may be important for the investigation or

---

[12] Administrative Jurisdiction Division of the Council of State 9 June 1994, AB 1995/238 (Van Baggum).

[13] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 3.

[14] *Parliamentary Papers II* 1995/96, 24 072, no. 11, p. 441.

[15] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 58.

[16] The Explanatory Memorandum to the bill containing the ISS Act 2002 shows that the general provisions on data processing by the services pertain to data processing for the purpose of the performance by the service of its tasks and to other forms of processing provided for by or pursuant to the ISS Act 2002 or the Security Screening Act (*Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 18).

[17] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 19.

prosecution of offences (Article 38 ISS Act 2002) and providing persons and bodies charged with a public task with data for an urgent and serious reason (Article 39 ISS Act 2002) are activities that fall outside the statutory tasks of GISS. In such cases data is provided for the purpose of the recipient's task. For those forms of data provision, the combination with the requirement of necessity leads to the requirement that providing the data must be necessary for the purpose of the task of the recipient body, with a view to the measures to be taken by that body. GISS obviously has only limited insight into the information position of the recipient body, so that the service cannot be expected to assess to what extent the data to be provided is essential for the recipient for it to be able to take measures. To the extent that the service does have an insight into the importance of the information, it must include this aspect in its assessment. In this context the liaisons of the recipient bodies play a role. Both the Public Prosecution Service and the Immigration and Naturalisation Service (INS) employ persons whose tasks include the task of monitoring cooperation with GISS. Two national public prosecutors and two INS officers act as liaisons.

The legislative history of the ISS Act 2002 shows that when GISS assesses whether it is necessary to issue an official message, it must include the nature and seriousness of the facts in its assessment and also the weighty interests involved and the possible consequences for the person concerned, in particular if fundamental rights may be at issue.[18] This means that whenever it is assessed whether it is necessary to issue an official message, an element of proportionality enters the picture as well, since the seriousness of the facts and the weighty interests to be served by the information provision must be balanced against the possible consequences for the person concerned.

3.1.2 In accordance with the law and with proper and due care

With regard to official messages, the requirement that data processing must take place in accordance with the law and with proper and due care means in the first place that the official messages must satisfy the requirements set for such messages pursuant to section 3.3 of the ISS Act 2002.

In the context of official messages, the requirement of proper and due care concerns the procedure followed to make the message. Making an official message with proper and due care requires first of all that the text of the message is based on information in the possession of GISS. An official message is only lawful when its text is substantiated by the underlying information. The thorough preparation of a file containing all the documents on which the text of the message is based is one of the safeguards on this point. As the Committee observed in its first review report on the official messages of GISS, the transparency of data processing will benefit by the addition

[18] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.

of a supplementary memorandum to each file, which contains references to the documents on which the official message is based.[19]

In addition to the substantiation of the information provided, the accuracy of the text of an official message is also important:

> "It is self-evident that it is a compelling duty of the services to guarantee the exactness and accuracy of the information provided."[20]

The fact that GISS must carefully choose the wording of an official message follows from the requirement that data processing must take place with proper and due care. An official message must contain an accurate, factual presentation of the underlying information and must, moreover, be as clear as possible, so that it is not capable of different interpretations. At the same time it must be borne in mind that GISS must also take account of its statutory duty to ensure that sources qualifying for secrecy are in fact kept secret and its duty to ensure the safety of the persons cooperating in the collection of information (Article 15 ISS Act 2002). In some cases it may be necessary for the service to make the text of the message slightly less specific so that it cannot be deduced from the text that the information derives from a specific technical or human source.

One aspect which, in the opinion of the Committee, is related to the provision of information with proper and due care is, that the internal procedure for making official messages should provide for the necessary control mechanisms to ensure the accuracy and exactness of the information. For this purpose the law imposes a specific statutory duty on the head of the service to ensure that the necessary arrangements are in place to promote the accuracy and completeness of the data that is processed (Article 16(a) ISS Act 2002).

Article 38(3) ISS Act 2002 provides with regard to official messages to the Public Prosecution Service that the appropriate officer of this Service is authorized to inspect all information underlying the official message which he needs to be able to assess the accuracy of the message. This provision is another safeguard that data processing takes place with proper and due care.

3.1.3 Indication of reliability or source reference

For the recipient of an official message, who may possibly proceed to take measures against the party concerned, it is relevant to know what is the quality of the data provided by GISS. Article 12(4) ISS Act 2002 therefore provides that the data processed by the service in the context of

---

[19] Review report of the Committee no. 9a on the official messages issued by GISS in the period from January 2004 – October 2005. *Parliamentary Papers II* 2005/06, 29 924, no. 9 (annex), section 3.3. Also available at www.ctivd.nl.

[20] *Parliamentary Papers II* 1997/98, 25877, no. 3, p. 55.

the performance of its task must be accompanied by an indication of reliability or a reference to its source. The simplest way of satisfying this requirement is to include a source reference in the official message. It will be clear, however, that where secret methods have been used to collect the data, it is impossible to refer to the source without disclosing information on the operational methods of the service or without acting in violation of the obligation of secrecy and the obligation to ensure the safety of the persons who cooperated in collecting the data (Article 15 ISS Act 2002). In such cases the service must choose the option of indicating the reliability of the data in the text of the official message. This indication of reliability may take different forms. Two of the indications used by GISS are: "GISS has reliable information" and "GISS has information [...]. The reliability of this information could not be established." For the recipient body this indication of reliability is essential to being able to assess on the merits whether or not to take measures.

The statutory obligation to indicate the reliability of information means that GISS, before issuing an official message, must assess the reliability of the information in its possession. This assessment should be made using procedures which, in conformity with Article 16(a) ISS Act 2002, promote the accuracy and the completeness of the data that have been processed. An example of such a procedure is the use of data from different sources if it possible to do so. Often, moreover, GISS will already have acquired the necessary knowledge in this area in the course of the investigation from which the information originates, thus making it possible for the employees concerned to form a sound opinion of the reliability of the information. When the information originates from a human source, it is important for GISS to critically evaluate its cooperation with the source on a periodic basis. Pursuant to Article 21 ISS Act 2002, agents are subjected to periodic evaluation anyway in connection with the three-monthly renewal of the agent's deployment. In addition, the internal rules require that a brief memorandum on the source is drawn up to be included in the file underlying the official message, which states what is the basis of the reliability assessment (further referred to as: reliability memorandum). In point of fact the reliability memorandum forms (part of) the substantiation of the indication of reliability.

3.2 Processing of personal data

Article 13(1) of the ISS Act 2002 contains an exhaustive list of the categories of persons whose personal data GISS may process. In addition to data relating to persons who are investigation targets in the context of the tasks of GISS, GISS may also process personal data of persons about whom data has been collected by other intelligence or security services, or whose data is necessary to support the proper performance by the service of its tasks, or who are or have been employed by the service.

Data relating to a person's religion or belief, race, health or sexuality may only be processed supplementary to the processing of other data and exclusively if this is required for the purpose of processing such other data (article 13(3) and (4), ISS Act 2002).

3.3 External provision of data

For the purposes of GISS' tasks, in the interests of national security, various powers have been conferred on GISS that it can use to collect (personal) data in secret and privacy-infringing ways. It follows that the data collected by GISS may only be disclosed externally in the interests of national security or because of another weighty interest such as the investigation and prosecution of offences. For this reason the ISS Act 2002 has a closed system of data provision, which means that data may only be disclosed externally if a specific statutory basis exists for doing so. Consequently, GISS may only issue an official message pursuant to Article 36, 38 or 39 of the ISS Act 2002 and in accordance with the requirements set for issuing official messages in the ISS Act 2002.

As was already briefly discussed in section 3.1.1, the law provides that information may be provided for two reasons. In the first place, an official message may be issued in the context of proper task performance, that is to say for the purpose of the tasks of GISS, in the interests of national security. The basis for the provision of information in the context of the performance by GISS of its task is Article 36 ISS Act 2002. These are cases in which the responsible body must be informed well in time so that it can take measures against a person or organisation who or which is the subject of the official message. Such a measure can e.g. be the refusal of an export permit application for exports that would contribute to the proliferation of weapons of mass destruction (WMD) or an order declaring a person forming a threat to national security to be an undesirable alien. Other examples of such measures are the sanction of freezing financial assets or refusing permission to hold a demonstration.

Secondly, GISS may provide information in the context of the task of the recipient. There is a specific legal basis (Article 38 ISS Act 2002) for the provision of data that is important for the investigation and prosecution of offences. Such data is provided to the member of the Public Prosecution Service designated for this purpose, namely the National Public Prosecutor. Although this Article and the Explanatory Memorandum to the Bill containing the ISS Act 2002 show that the provision relates to a discretionary power of the minister of the Interior and Kingdom Relations to provide data to the Public Prosecution Service, it will be clear that the discretionary margin decreases as the gravity of the offence increases.[21] The Committee further points out that one must not lose sight of the reason for allowing the service this discretionary margin in assessing whether or not to provide data to the Public Prosecution Service; one of the factors to be taken into account is the extent to which providing data could adversely affect an investigation of GISS or the performance by GISS of its tasks, generally.

Finally, Article 39 ISS Act 2002 constitutes a legal basis for the provision of data that is relevant to other public tasks than investigating or prosecuting offences. Since the principle of the closed system of information provision calls for restraint in providing data for the purposes of

[21] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 58.

interests other than those of national security, Article 39 ISS Act 2002 sets two conditions for such data provision: (1) data may be provided only to persons or bodies designated by general administrative measure and involved in performing a public task and (2) there must be an urgent and serious reason for providing the data.

Pursuant to Article 39 ISS Act 2002, the following persons and bodies have been designated by general administrative measure: the ministers, the Dutch Central Bank (De Nederlandsche Bank N.V.), the Dutch Authority for the Financial Markets (Stichting Autoriteit Financiële Markten) and the mayors insofar as the data to be provided relates to their responsibility for public order and insofar it relates to their advisory task regarding nominations for a royal honour (Designation Order pursuant to Article 39 ISS Act 2002).[22] It rarely happens that official messages are issued pursuant to Article 39 ISS Act 2002. This is in keeping with the expectation, expressed when the bill containing the ISS Act 2002 was discussed in parliament, that the services would in practice make sparing use of the power laid down in Article 39.[23]

3.4 External provision of personal data

Articles 40, 41 and 42, ISS Act 2002, set a number of additional requirements for the provision of personal data. The reason for additional requirements is that it is appropriate to exercise special due care because the provision of personal data very emphatically affects the privacy of the person concerned.[24]

The main rule is that personal data is provided in writing where the recipient is competent to act on the data by taking measures against the person concerned (Article 40(1) ISS Act 2002). Personal data may only be provided orally in case of urgency. Written confirmation should follow as soon as possible in such cases (Article 40(2) ISS Act 2002).

By way of additional safeguard for the accuracy and reliability of the personal data to be provided Article 41(1) ISS Act 2002 provides that the service may not provide personal data whose accuracy cannot reasonably be established or which was processed more than ten years ago, while no new data has been processed regarding the person in question since that time. Derogation of this provision is possible in the case of the provision of personal data to the Public Prosecution Service, to counterpart services of GISS and in other special cases to be determined by the minister of the Interior and Kingdom Relations (Article 41(2) ISS Act 2002). When data is provided in derogation of the provision of Article 41(1), the degree of reliability and the age of the data must be stated (Article 41(3) ISS Act 2002).

---

[22] Order of 22 September 2004 designating persons and bodies pursuant to Article 39(1) of the Intelligence and Security Services Act 2002 (Designation Order pursuant to Article 39 ISS Act 2002), Stb. 2004, 506, amended by order of 21 November 2006 amending general administrative measures in connection with the introduction of the Financial Supervision Act, *Stb.* 2006, 663.

[23] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 35.

[24] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 59.

Article 42 ISS Act 2002, finally, provides that records must be kept of the provision of personal data. In its previous review report on official messages issued by GISS the Committee already came to the conclusion that this obligation to keep records is complied with through the retrievable storage of the official messages at GISS.[25] This makes it possible for both the service and the Committee to retrieve what personal data was provided to which recipient.

4. Official messages to the Public Prosecution Service

4.1 Use of official messages to the Public Prosecution Service

The role that information from the intelligence and security services can play in criminal process was discussed as early as in February 1992 in connection with the former National Security Service in a letter sent by the minister of Justice to the Second Chamber of Parliament.[26] This letter first deals with the difference between collecting intelligence and investigating crimes. It is explained that intelligence is collected in the interest of national security regardless of the existence of an offence or suspected offence.

The ISS Act 2002 emphasizes the distinction by providing that officers of the services do not have powers to investigate offences (Article 9(1) ISS Act 2002). The distinction between intelligence collection and crime investigation does not imply, however, that information in the possession of National Security Service should not be useful for criminal law enforcement. The distinction can, however, give rise to a different assessment of the information for evidential purposes. Ultimately, this assessment is made by the criminal court.[27]

In conclusion, the aforementioned letter to the Second Chamber mentions the following uses of information from the National Security Service:

a) the information can constitute reason to start a criminal investigation;
b) the communicated facts and circumstances can result in a legitimate suspicion within the meaning of Article 27 of the Dutch Code of Criminal Procedure;
c) the information can constitute legal proof within the meaning of the Code of Criminal Procedure.[28]

Decisions have been given on this issue in Case Eik, first by the Court of Appeal of The Hague

[25] Review report of the Committee no. 9a on the official messages issued by GISS in the period from January 2004 - October 2005, *Parliamentary Papers II* 2005/06, 29 924, no. 13 (annex), section 4.8. Also available at: www.ctivd.nl.
[26] When the ISS Act 2002 was discussed in parliament, the minister stated that broadly considered this letter was still an accurate and useful presentation of how data from the intelligence and security service can be used in criminal investigations. *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 12.
[27] *Parliamentary Papers II* 1991/92, 22 463, no. 4, p. 2.
[28] *Parliamentary Papers II* 1991/92, 22 463, no. 4.

and subsequently by the Supreme Court. On 21 June 2004 the Court of Appeal of The Hague ruled that the Public Prosecution Service and the criminal court may in principle assume that GISS performed its task lawfully and duly placed its official messages at the disposal of judicial authorities. Not only can information from GISS form the basis for starting a criminal investigation, it can also be the basis for arresting the suspect.[29] The Supreme Court confirmed this trend in its judgment of 5 September 2006, adding that in principle there are no objections to using material gathered by intelligence and security services in criminal proceedings. The criminal courts, so the Supreme Court states, are deemed to assess carefully on a case-by-case basis whether the material can form part of the evidentiary material, having regard to the sometimes limited review possibilities.[30] The Committee notes that the new rules on hearing identity-protected witnesses are intended to enhance the evidential value of official messages (see section 4.2).

The Supreme Court mentions a number of situations in which information from GISS may in any case not be taken into account in weighing the evidence.[31] For example: it is not permitted to deliberately not use investigative powers with a view to bringing about that criminal-law safeguards will not apply so that information from GISS can be used or continued to be used. Furthermore, the acts of GISS may not restrict the fundamental rights of the suspect to such extent that there is no longer question of a fair trial as referred to in Article 6 of the ECHR. Finally, the court must examine whether the limited possibilities of reviewing the information from GISS do not restrict the rights of the defence to such extent that using the information in evidence results in violation of the fair trial requirement of Article 6 ECHR.

The use of information from GISS in the criminal process was once again the subject of extensive discussions in the Second Chamber in the context of the bill containing the Witness Identity Protection Act.[32] It was emphasized that the extent to which the reliability of the information stated in an official message can be verified will affect the use of information from GISS as evidence.[33] The Second Chamber also discussed the issue of GISS' continuing to provide information after a criminal investigation has been started. In this situation a distinction must be made between the provision, at the request of the Public Prosecution Service, of intelligence already collected by GISS, and the collection of intelligence at the request of the Public Prosecution Service followed by the provision of this intelligence.[34] The former information provision is permitted, the latter conflicts with Article 9(1) ISS Act 2002. The Supreme Court quoted this explanation in a case involving the continued exchange of information between GISS and the Public Prosecution Service after a criminal investigation had been started. The defence complained that the investigations had become intermingled. The Supreme Court ruled that there is no rule of law precluding parallel investigations with GISS continuing to provide information, so long as there

[29] Court of Appeal The Hague 21 June 2004, *NJ* 2004, 432 / *LJN*: AP3601 and AP2058 (case Eik), para. 4.3.10.
[30] Supreme Court 5 September 2006, *LJN*: AV4144 (case Eik), para. 4.6.
[31] Supreme Court 5 September 2006, *LJN*: AV4144 (case Eik), paras. 4.7.2 and 4.8.
[32] *Parliamentary Papers II* 2003/04, 29 743, no. 3.
[33] *Parliamentary Papers II* 2003/04, 29 743, no. 3, p. 5.
[34] *Parliamentary Papers II* 2004/05, 29 743, no. 7, p. 23.

is cause to continue the intelligence investigation for the purposes of the performance by GISS of its task. In the case in question the Supreme Court held that it was not an incomprehensible decision of the Court of Appeal that evidently the available information was cause for GISS to continue its intelligence investigation.[35]

4.2 The Witness Identity Protection Act

In 2002 the District Court of Rotterdam, in a judgment that was subsequently set aside by the Court of Appeal of The Hague[36], held that information from GISS may serve as initial information at the start of criminal proceedings, but that a person may not be considered a suspect within the meaning of Article 27 of the Dutch Code of Criminal Procedure (also referred to as "Sv") exclusively on the basis of an official message from GISS.[37] Shortly after this judgment it was decided to prepare for an amendment to the Code of Criminal Procedure. The proposal formed part of a package of changes in the law to combat terrorism.

On 1 November 2006 the Act amending the Code of Criminal Procedure (witness identity protection) (further referred to as the Witness Identity Protection Act) entered into force.[38] The purpose of this change in the law is to increase the usefulness of official messages of GISS in the criminal process. Where formerly an official message could only be used in evidence in combination with other evidence, it now constitutes full documentary evidence (Article 344 Sv). It is subsequently for the court to further examine its reliability so that it can establish its evidential value. For this purpose the court may e.g. hold that it needs to hear an employee of GISS. At a public hearing, however, this employee will usually have to invoke his obligation of secrecy (Article 85 ISS Act 2002). The examining magistrate of the District Court of Rotterdam has exclusive jurisdiction to hear identity-protected witnesses under the witness identity protection regime (Article 178a(3) in conjunction with Articles 226m-226s Sv), in which case the minister of the Interior and Kingdom Relations can release the GISS employee concerned from his obligation of secrecy (Article 86(2) ISS Act 2002). In principle, the defence and the public prosecutor handling the case do not have the right to be present at the hearing, but they may submit questions (Article 226p, paragraphs (1) and (4) Sv). The identity-protected witness himself assesses whether the interest of national security precludes furnishing the report of the witness hearing to the parties in the proceedings and including it in the documents of the case (Articles 226p(3) and 226s(1) Sv). If the witness does not assent to the report being furnished, it is destroyed and the examining magistrate makes a note of the fact in a new report. It is the responsibility of the examining magistrate to include an opinion on the reliability of

[35] Supreme Court 13 November 2007, *LJN*: BA2553 (animal rights activist), paras. 3.4.1-3.5.3, also: Court of Appeal The Hague 2 October 2008, LJN: BF3987 (case Piranha).

[36] Court of Appeal The Hague 21 June 2004, *NJ* 2004, 432 / *LJN*: AP3601 and AP2058 (case Eik).

[37] District Court of Rotterdam 18 December 2002, *LJN*: AF2141 (case Eik).

[38] Act amending the Code of Criminal Procedure (witness identity protection), 28 September 2006, *Stb.* 2006, 460. Entry into force: 1 November 2006 (*Stb.* 2006, 461).

the statement made by the identity-protected witness in the report (Article 226q Sv). Since the amendment of Article 187d Sv, the examining magistrate himself can now also prevent, when he prepares the report, that answers to questions concerning specific data come to the notice of the public prosecutor, the suspects and his counsel if there are good reasons to believe that this would harm the interest of national security (Article 187d(1)(c) Sv). Based on the report of the witness hearing and the examining magistrate's opinion on the reliability of the witness' statement, the trial judge then establishes the persuasive power of the official message.

Since the entry into force in 2006 of the Witness Identity Protection Act no use has been made yet of the opportunity to hear GISS employees as identity-protected witnesses.[39] In the criminal cases in which the evidential value of official messages came up for examination, the means provided by the Witness Identity Protection Act for further examining the evidential value of official messages were not applied.[40] So far, the rules on hearing witnesses under the partial anonymity regime (Article 190(2) SV) have been used when GISS employees were heard. Partial anonymity means that the examining magistrate can direct that questions about particular facts shall not be asked, if there are good reasons to believe that the witness will suffer nuisance in connection with his having given evidence or will be impeded thereby in the performance of his duties. In the fairly recent case concerning the leaking of information to daily newspaper De Telegraaf, the examining magistrate inspected the documents underlying the official message in question pursuant to the authority of Article 187d Sv.[41]

The minister of Justice has undertaken to report to the States-General on the effectiveness and the effects of the Act in actual practice. The Research and Documentation Centre is currently carrying out an assessment. The assessment is expected to be completed in the third quarter of 2011.[42]

4.3 Procedure for making official messages to the Public Prosecution Service

The National Public Prosecutor has been designated as the recipient of official messages issued to the Public Prosecution Service. This officer passes on the official messages to the appropriate public prosecutor's office. This can be a district public prosecutor's office, the National Public Prosecutors' Office or the National Public Prosecutor's Office for Financial, Economic and Environmental Offences. In 2006 a second National Public Prosecutor was appointed.

---

[39] See in this connection also the cabinet report on counterterrorism measures in the Netherlands in the first decade of the 21st century (*Antiterrorismemaatregelen in Nederland in het eerste decennium van de 21ste eeuw*), published in January 2011, annex H, p. 88.

[40] For example District Court Rotterdam 1 December 2006, *LJN*: AZ3589 (Samir A. a.o.), Court of Appeal The Hague Den Haag 2 October 2008, *LJN*: BF3987 (case Piranha, Samir A. a.o.).

[41] District Court Haarlem 14 July 2010, *LJN*: BN1191 and *LJN*: BN1195 (Telegraaf leak)

[42] *Parliamentary Papers I* 2010/11, 32 500 VI, no. L, p. 4.

When information has emerged from an investigation by GISS which qualifies for being provided to the Public Prosecution Service, the team concerned usually consults with the National Public Prosecutor. This officer then informs GISS whether in his opinion the information is useful for the Public Prosecution Service. If it is, the team prepares a draft text and collects the underlying documents. Subsequently, the text of the official message together with the underlying documents is discussed and agreed with the legal department of GISS. In situations where GISS has identified an acute threat, it may happen that no prior coordination with the National Public Prosecutor takes place.

The legal department is responsible for ensuring agreement on the text of the official message between the National Public Prosecutor and the team. The National Public Prosecutor examines among other things whether the wordings used in the official message are sufficiently factual and unambiguous. It is not the intention that the text already contains criminal characterizations of facts, since it is the task of the court to assess whether criminal characterizations apply on the basis of the available factual information. If necessary, the parties concerned can consult about making changes in the text of the official message. As soon as agreement has been reached on the text of the official message, the team will complete and put the file in order. The internal rules at GISS prescribe that the author of the official message must prepare an overview to accompany the file.

After the team head and the legal department have approved the official message and the accompanying file, the message is presented to the National Public Prosecutor together with the file. The check done by the National Public Prosecutor at this stage concerns the accuracy of the official message (Article 38(3) ISS Act 2002). Accuracy means that the text is substantiated by the underlying documents. In addition, the National Public Prosecutor pays attention to the accuracy of the indication of reliability. It is emphatically not for the National Public Prosecutor to assess the truth of the information; that task is reserved for the criminal court. Neither does the National Public Prosecutor review whether the underlying information has been gathered lawfully. The judgments of the District Court of Haarlem in the case concerning the leaking of state-secret information to daily newspaper De Telegraaf show that the National Public Prosecutor must check whether the message is correct by reference to the underlying documents before the official message is issued, unless it is demonstrated that there was no time to do so on account of the circumstances.[43]

After the National Public Prosecutor has checked whether the official message is correct, it is presented together with the file to the head of the unit to which the team in question belongs. The National Public Prosecutor is notified of any adjustments in the text of the official message. Finally, the official message is signed and adopted by the head or deputy head of GISS.

[43] District Court Haarlem 14 July 2010, *LJN*: BN1191 and *LJN*: BN1195 (Telegraaf leak). At the time of adopting the present review report the case was still pending before the appeal court.

4.4 Findings of the Committee

4.4.1 The number of official messages in the review period

The Committee has established that GISS issued 132 official messages to the Public Prosecution Service in the review period. These official messages thus account for 23% of the total number of official messages issued in this period. The annual number of official messages issued to the Public Prosecution Service varies, but averages approximately 30 official message per year.

4.4.2 Legal basis

The legal basis for issuing official messages relating to offences to the Public Prosecution Service is Article 38 ISS Act 2002. In the opinion of the Committee, all but one of the official messages issued by GISS to the Public Prosecution Service are rightly founded on this basis.

In 2006 GISS issued an official message which in the Committee's opinion should not have been issued to the Public Prosecution Service on the basis of Article 38. The official message was issued in connection with the results of a security screening by GISS of a civil servant who had applied for a position of confidentiality. In the course of the security screening, facts became known about the civil servant which were not fitting for a person holding a position of confidentiality, but which were also not fitting for the position the civil servant already held at the time. The civil servant was confronted with the facts and decided to withdraw his application for the position of confidentiality, as a result of which GISS did not complete the security screening. Because GISS believed that the activities of the civil servant were incompatible with the position the civil servant was holding at the time, and that those activities might impair the integrity of the organisation in which the civil servant was employed, GISS decided to issue an official message. The official message was issued to the National Public Prosecutor, stating that the reason was that it could not be excluded that the civil servant had not declared the possible secondary income from the activities to the Tax Authorities, which in the opinion of GISS had given rise to a suspicion of tax evasion.

The Committee holds the opinion that GISS wrongly issued this official message to the Public Prosecution Service. The fact is that GISS did not know whether the activities had actually generated income, nor was there evidence of any other offences. Moreover, the National Public Prosecutor had already notified GISS that it would not prosecute the person concerned. The Committee endorses the opinion of GISS that the activities of the civil servant were incompatible with his position. Since impairment of the integrity of public administration may in some cases also constitute a danger to the continued existence of the democratic legal order, or to national security or other serious state interests, GISS could have sent the official message to the employer

pursuant to Article 36 ISS Act 2002.[44] In the opinion of the Committee, however, GISS should not have issued the official message to the Public Prosecution Service.

4.4.3 Necessity

As was already explained in section 3.1.1, providing information to the Public Prosecution Service with a view to measures to be taken must be necessary for the purposes of the task of the Public Prosecution Service: the investigation and prosecution of offences. In the course of its investigation the Committee came across two cases in which GISS provided data to the Public Prosecution Service which the Service already possessed. GISS was in fact aware of this. It concerns official messages issued in 2007 and 2010. In both cases the Committee found that by issuing the messages GISS sought to influence the follow-up steps to be taken by the Public Prosecution Service.

The first case concerned information from the police which had been reported to GISS via the Regional Intelligence Service. Because GISS considered the threat to be serious, it subsequently provided the information to the National Public Prosecutor to induce the Public Prosecution Service to take action. GISS thus acted contrary to its own internal rules which direct that regular police information is not included in official messages except in exceptional cases. GISS must then state expressly in the official message that the information had been provided to GISS pursuant to Article 62 ISS Act 2002, which in this case it did not do.

In the other case GISS intended to exert influence on the choice of the service that was to carry out the investigation. GISS considered it important for the investigation in question to be conducted by the National Police Internal Investigations Department, while at that moment it was also possible that the Public Prosecution Service would choose to keep the investigation within its own organisation and have it carried out by a unit of the National Public Prosecutor's Office for Financial, Economic and Environmental Offences. By issuing the official message GISS wished to stress the seriousness of the case and thus influence the choice of the service that was to carry out the investigation. The Committee observes on this point that it finds it understandable that GISS, which at the time of issuing an official message has often already invested many months – if not years – in the case, wishes to ensure that the body to which it provides the information handles the case in a certain way. However, issuing an official message containing information that is already known to the recipient is not the appropriate procedure for achieving this. When GISS has specific wishes or advice concerning the steps which the Public Prosecution Service should undertake in a certain investigation, it can consult with the Service – through the National Public Prosecutor. The Committee holds the opinion that in such cases providing information is not necessary for the purpose of the investigation and prosecution of offences since the Public Prosecution Service already has the information.

[44] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 33 and Parliamentary Papers II 2005/06 VII, no. 47.

The Committee has established that situations may exist in which GISS chooses to provide information to the Public Prosecution Service while it has already been made clear to GISS through the National Public Prosecutor that the Service does not consider it expedient or sees no possibility to act on the information. Taking into consideration its above observations, the Committee advocates that in such a situation GISS first tries to reach agreement through the existing hierarchical channels.

4.4.4 Content

The Committee has found that the content of the official messages issued by GISS to the Public Prosecution Service in the review period is substantiated by the underlying files. In a number of cases, however, GISS did not draft the text of the message with sufficient care.

In 2008 GISS issued an official message which in the opinion of the Committee contains a confusing passage. In this official message GISS stated among other things that there was concrete evidence that the person concerned was involved with certain activities. This was based amongst other things on the suspected presence of the person concerned at certain meetings. The Committee holds the opinion that qualifying as concrete evidence the information in question, which related to events which were suspected to have taken place, creates confusion. This wording does not make clear to the recipient how strong the evidence is.

In a comparable case, in an official message issued in 2005, GISS informed the Public Prosecution Service that the person concerned belonged to a certain group. Investigation by the Committee showed that this assertion could not be fully substantiated by the available information. In view of the scanty information on the contacts between the person concerned and members of the relevant group, it is the opinion of the Committee that GISS should have chosen a wording that was more in keeping with the actual findings.

An official message issued by GISS in 2008 reported that the person concerned, who was being associated with terrorist activities, seemed to be in contact with another person *in this context.* After studying the file, the Committee found that GISS only had information that the two persons were registered at the same address. Upon enquiry at GISS it turned out that the service wished to indicate that the person concerned was in contact with the other person and that in this context the other person also required (or might require) the attention of the Public Prosecution Service. It is the opinion of the Committee that in this case, too, GISS should have formulated the text of the message with greater care.

In some other official messages the structure of the text leads to a lack of clarity. One official message issued in 2006 states that the information in the message was obtained from more than one source. A list of information follows. It is not clear to the reader whether each item of the

information originates from one or from several sources. Another example is an official message issued in 2009, which states in the first sentence that the information is reliable. Further on in the official message only the word information is used, so that it is not clear whether this is information that is justly qualified as "reliable information".

Of the two other cases in which the Committee hold the opinion that GISS did not exercise sufficient care, one message stated an incorrect house number and the other message an incorrect address. In both cases GISS had the correct information. The Committee points out that including incorrect address details may have serious consequences, for example if the Public Prosecution Services decides to carry out a police raid at the (incorrect) address stated by GISS.

4.4.5 Deciding to provide information to the Public Prosecution Service

As a result of two detailed official messages which GISS issued to the Public Prosecution Service in 2009, the legal experts of GISS discussed the fact that the Public Prosecution Service is increasingly asking GISS for detailed official messages. Subsequently, the policy line in this field was laid down in an internal memorandum. Pursuant to this memorandum GISS may only comply with a request for a detailed official message if there are urgent reasons in the context of the tasks of GISS to bring about that the criminal investigation gets a speedy start. GISS will not be allowed to comply with such a request from the Public Prosecution Service if this would harm the interests of GISS, such as protecting its operational methods.

The Committee holds the opinion that this reasoning is at odds with the intention of the legislature. In the Explanatory Memorandum to the bill containing the ISS Act 2002 it is explained that the underlying reason for the margin of appreciation allowed GISS in deciding whether or not to provide information to the Public Prosecution Service is, that the proper performance by the service of its task would be impeded if they would have to notify the Public Prosecution Service each time it identified an offence. It follows that GISS, in deciding whether or not to provide information to the Public Prosecution Service, must assess to what extent this will harm the performance of its own task, taking account of the possibility that the Public Prosecution Service will decide to investigate and prosecute. If GISS only provides detailed information when national security urgently calls for a matter to be investigated and prosecuted, then GISS exercises greater restraint than was envisaged by the legislature. The Committee points out that the interests of investigation and prosecution must carry great weight. Whenever it is possible for GISS to reveal (detailed) information, it should only decide not to do so if providing the information would harm the interests of the service.

4.4.6 Indication of reliability or source reference

In its investigation the Committee established that as a rule GISS consistently includes an indication of reliability in the official messages to the Public Prosecution Service.

Two related official messages issued in 2006 are an exception to this rule. These messages merely mention information without characterising its reliability. The Committee has found that GISS wished to leave it to the Public Prosecution Service to characterise the information, in order not to interfere with the investigation that had already been started. The Committee points out that characterising the reliability of information must be distinguished from characterising the information itself. The former is a statutory duty for GISS, while it may refrain from the latter if it is appropriate to do so in view of the obligation of secrecy or the demarcation of the tasks of the service.

Another case in which GISS did not include an indication of reliability is an official message issued in 2008. This proved to be a deliberate choice of GISS. The information that was the reason for issuing the message, which was considered reliable, originated from a foreign counterpart service and GISS was not permitted to distribute the information on account of international agreements on further distribution. There were, however, also reports in the media that supported the information. In addition, GISS possessed certain information which it had obtained from its own investigations. By leaving out the indication of reliability, GISS in fact left it undecided on which information it had ultimately based the official message. The Committee finds that if GISS adhered to the agreement with the counterpart service, it did not provide the information originating from that service. This has the result that part of the official message is based on a media report only. This should have been clear from the text of the official message. With respect to information from publicly accessible sources the best choice is generally to mention the source, since this improves the transparency of the message.

In its first review report on the official messages of GISS the Committee explained that it is not necessary that information is confirmed by material from other sources for GISS to establish that information is reliable. This means that GISS can assess information from one single human source as reliable. In its investigation the Committee came across some examples of official messages to the Public Prosecution Service in which information from one single human source formed the basis of part of the message. The files of these official messages include memorandums on the reliability of the sources in question. The Committee holds the opinion that in these cases GISS exercised due care in establishing the reliability of the information.

4.4.7 Exculpatory information

Information qualified as reliable by GISS which contradicts the conclusion drawn in the official

message, is called exculpatory information. GISS includes this information either in the official message or in the underlying file. If, however, GISS has information which it does not qualify as reliable but which contradicts the conclusion drawn in the official message, then GISS does not consider this to be exculpatory information. In such cases GISS will not mention the information in the official message nor include it in the underlying file.

In 2006 the Public Prosecution Service enquired at GISS, through the National Public Prosecutor, whether the service had exculpatory information concerning a person with respect to whom GISS had previously issued an official message. In reply to this request GISS issued an official message in which it explained how the accuracy and completeness of official messages are safeguarded by internal procedures. The Committee has established that this explanation leaves room for misunderstandings as far as the subject of exculpatory information is concerned. GISS stated in the official message that:

> "[…] in the case that we have contradictory information, the service will decide either to give expression to this in the wording of the official message or not to issue an official message because the information is insufficiently reliable and consequently unsuitable for being mentioned in an official message."

This explanation creates the impression that information which GISS does not consider reliable but which contradicts the conclusion drawn in the official message, will nevertheless be included in the official message or may even have the result that no official message is issued. As was described above, this is not the procedure followed at GISS. The fact is that GISS, when drafting the official message, finds that such information must not be considered as exculpatory information. This assessment and the subsequent decision not to include the information in the official message fall within the statutory task of GISS.

The Committee wishes to point out, though, that because this information is not included in the underlying file, it will not be found by the National Public Prosecutor who checks the content of the official messages issued to the Public Prosecution Service. It will also not be possible for the Committee to review the assessment in retrospect. As a result, the assessments made by GISS regarding the reliability of this information are unverifiable. In the opinion of the Committee it is advisable to arrange the files underlying official messages in such a way that they show whether exculpatory information is available and how GISS assessed its reliability.

4.4.8 Lawfulness of the underlying data processing

In 2009 GISS issued two official messages to the Public Prosecution Service relating to the export practices of a specific company. A CD-ROM containing tapped telephone conversations was enclosed as an annex with each of the two messages. As a result of the official messages of

GISS a criminal investigation was started in the course of which the criminal investigation team used telephone taps. The intelligence investigation of GISS, which also included the use of special powers, was continued as well. The latter investigation resulted among other things in a third official message to the Public Prosecution Service, in 2010. As a general observation it can be said that special powers may be used while a criminal investigation is going on at the same time as long as there is a lawful basis for such use (see section 4.1). In this situation, however, GISS must make sure that the needs of the Public Prosecution Service do not become the guiding factor in its intelligence investigation. On the other hand it is important that both GISS and the Public Prosecution Service obtain as complete a picture of the subject matter as possible. This requires coordination, with each party keeping its own task in mind while gaining an understanding of the other party's needs, so that the appropriate information can be provided. The Committee studied the reasons stated for the continued use of special powers in the investigation in question. It holds the opinion that this continued use was lawful from the intelligence perspective. It emerged from interviews held with employees of the service and with the National Public Prosecutor that regular consultations took place between the relevant GISS team and the criminal investigation team, under the leadership of the National Public Prosecutor. The Committee has found that due care was exercised in keeping the two parallel procedures strictly separate.

In addition, the Committee has seen cause to put further questions to GISS about the use of special powers in an investigation of GISS aimed at characterising a potential imminent threat to the democratic legal order. GISS had provided information to the National Public Prosecutor to be used by the criminal intelligence unit of the National Investigation Service, which was conducting an investigation of the group in question at the same time. The Committee examined whether the use of the special powers satisfied the statutory requirements of necessity, proportionality and subsidiarity. The Committee holds the opinion that in view of the relevant facts and circumstances the powers were used lawfully, although the reasons stated in writing for the use of the special powers showed some defects.

4.4.9 Documentation

One of the safeguards for the careful making of an official message is the existence of a complete underlying file. The Committee has established that generally the official messages that have been issued to the Public Prosecution Service are supported by thorough documentation.

In one case GISS added an earlier official message on the relevant persons to the file of a subsequent official message to substantiate certain information. The Committee points out that the use of official messages in substantiation of other official messages entails the risk of losing sight of the age of the information that actually underlies the subsequent official message. It is the opinion of the Committee that in such cases GISS should add (copies of) the relevant documents from the file of the earlier official message to the new message file.

5. Official messages to the Immigration and Naturalisation Service (INS)

5.1 The use of official messages issued to the Immigration and Naturalisation Service

Pursuant to its statutory mandate, GISS has power to investigate whether threats exist to national security, including threats coming from aliens staying in the Netherlands. A decision of the INS to cancel or refuse a residence permit and/or an order declaring a person an undesirable alien, one of the criteria for which is whether the alien constitutes a threat to national security,[45] may therefore be based on an official message from GISS.

The European Court for Human Rights (ECtHR) has accepted in its case law that the states that are signatories to the ECHR do not further define the term 'national security' in their national legislations. The states are left a margin of appreciation when interpreting the term. This margin of appreciation is delimited by what can still be deemed to fall under the natural meaning of the term. The ECtHR has ruled, for example, that considering a person a threat to national security on the grounds of his involvement with drugs trafficking went beyond the natural meaning of the term 'national security'.[46]

If an official message from GISS shows objectively, impartially and clearly which facts and circumstances underlie the conclusion of the message and if this conclusion is not incomprehensible without further explanation, there is no reason for INS to inspect the documents underlying the official message.[47] So an official message can be considered an expert opinion, which means that INS may in principle assume that the information is accurate, unless there are concrete indications that there is reason to doubt the accuracy or completeness of the information.[48] It is the responsibility of the alien to allege any such indications.[49]

It is logical that the more concrete and detailed the facts and circumstances are described in the official message, the more readily INS will be able to conclude that the official message is clear and transparent and decide not to further investigate its content.[50] For the sake of clarity it must be noted in the context of the foregoing that INS remains responsible for stating the reasons for its decisions under aliens law.

---

[45] Cancellation of fixed-term residence permit: Article 32(1)(b) of the Aliens Act 2000; cancellation of permanent residence permit: Article 35(1)(d) of the Aliens Act 2000; order declaring a person an undesirable alien: Article 67(1)(c) of the Aliens Act 2000.

[46] ECtHR 24 April 2008 (*C.G. e.a./Bulgaria*), A 1365/07, para. 43.

[47] Administrative Jurisdiction Division of the Council of State 4 July 2006, *LJN*: AY3839, para. 2.1.4.

[48] Administrative Jurisdiction Division of the Council of State 12 October 2001, *LJN*: AD5964, para. 2.3.4 and District Court The Hague 12 June 2006, *LJN*: AY4303, para. 5.2.

[49] Administrative Jurisdiction Division of the Council of State 4 July 2006, *LJN*: AY3839, para. 2.1.4.

[50] District Court The Hague 28 May 2010, *LJN*: BM7552, para. 7.

For some years now GISS has also been issuing official messages to INS which do not include the conclusion "threat to national security". It follows from case law that these official messages must also be considered expert opinions.[51] By means of an official message INS can be informed, for example, of an alien's anti-integrative behaviour, where this falls within the scope of the mandate of GISS. Examples are persons who make statements directed against the democratic legal order or who incite to actions that are contrary to statutory and other rules.[52] This information from GISS can be used to constitute (part of) the basis for a decision refusing an application for being granted Dutch nationality or for withdrawing Dutch nationality.[53] It also happens that GISS provides information of a factual nature to INS, when there are reasons to suspect that a person has furnished incorrect data or has withheld information in the context of the grant or renewal of a residence permit. This type of data provision may only take place to the extent that providing the data is in the interest of national security. Derogation from this rule is only permitted if there is another urgent and serious reason to provide the data. In the latter case the data is provided to the minister for Immigration and Asylum pursuant to Article 39 ISS Act 2002.

In administrative procedures the court has the possibility of ascertaining that the conclusions in the official message are supported by the underlying file.[54] If the file underlying the official message includes documents that are classified state-secret, the minister of the Interior and Kingdom Relation will inform the court that only the court is authorised to inspect the underlying file.[55] This means that neither the alien concerned nor the government member concerned is granted inspection of the underlying documents at that stage. To satisfy the requirements of fair trial, Article 87(1) ISS Act 2002 provides that the court may only (partially) base its judgment on those documents with the consent of the parties. The possibility for the court to inspect the underlying file is important with a view to the case law of the ECtHR, from which it ensues that a party whose treaty rights are infringed by a measure taken for the purposes of national security, must have the possibility of having the measure reviewed by an independent and impartial body that is authorised to examine all the relevant facts and issues of law.[56]

The fact that the alien himself will generally not be allowed to inspect the documents underlying the official message on account of their state-secret nature, may restrict his right to a defended action. This restriction does not by definition mean, however, that there can be no fair trial.[57] In order to stand the test of the ECtHR, however, the official message itself, which the alien

---

[51] Administrative Jurisdiction Division of the Council of State 29 September 2010, 201000881/1/V6, paras. 2.6.1 and 2.6.2 (Taraghini).

[52] Guide to the Netherlands Nationality Act, explanatory note to Article 8(1)(d) of this Act, section 3.3.

[53] This is effected pursuant to Article 8(1)(d) of the Netherlands Nationality Act (civil integration counter-indication) and/or Article 9(1)( )a of the same Act (serious suspicion of threat to public order, public morality or the security of the Kingdom).

[54] If the minister of the Interior and Kingdom Relations refuses to allow the court inspection of the underlying documents of the official message, the court may draw such conclusions as it deems fit from this fact (Article 8:31 of the Dutch General Administrative Law Act).

[55] Article 8:45 in conjunction with Article 8:29 of the General Administrative Law act read with Article 87(1) ISS Act 2002.

[56] ECtHR 20 June 2002 (*Al Nashif/Bulgaria*), A 50963/99, para. 123.

[57] ECtHR 20 July 2010 (*A./Netherlands*), A 4900/06, para. 160; ABRvS 7 October 2008, *LJN*: BG1209, para. 2.4.

may inspect, must contain sufficient concrete and specific information and thus give the alien sufficient reference points to be able to contest the information. In *A. e.a./United Kingdom* the ECtHR mentions as an example of a concrete reference point the allegation that the person concerned had attended a terrorist training camp at a stated location between stated dates.[58]

5.2 Procedure for making official messages to the Immigration and Naturalisation Service

In its first review report on the official messages issued by GISS the Committee considered it advisable, in view of the increased number of official messages to INS, that GISS would make sound arrangements with INS about a procedure for communicating with INS about official messages. It suggested that INS adopt a procedure providing for the designation of an officer who would act as permanent liaison with regard to official messages. This recommendation has had the result that since 2007 the INS liaison, who had previously been appointed as contact for operational matters, has been assigned a structural role in the procedure for making the official messages issued by GISS to INS. Recently, a second INS liaison was appointed.

The exchange of information between GISS and INS is regulated in greater detail in a covenant between the two services. The covenant provides – briefly stated – that the services may provide each other with data that can be relevant to the performance of their tasks. The covenant, which dates from 2003, adds little to the statutory provisions. Newer forms of cooperation, such as the provision of information in the context of the decision-making process under the Netherlands Nationality Act and the requests for information from INS to GISS, have not been incorporated in the covenant. At the time of drafting the covenant, moreover, the position of INS liaison at GISS did not yet exist. As early as in 2007, in its review report on the exchange of information between GISS and INS, the Committee already pointed out that the covenant needed to be revised. The reason why the revision has been postponed so far is that the services were awaiting an amendment of the ISS Act 2002 (the so-called post-Madrid measures), because this amendment was expected to result in a fundamental change in the basis for the cooperation between GISS and INS. Recently, however, the bill amending the ISS Act 2002 was withdrawn. The Committee therefore recommends that GISS, in consultation with INS, formalises the current practice of exchanging information between GISS and INS in a written procedure as soon as possible.

From the perspective of internal procedure the official messages which GISS issues to INS must be distinguished into two categories. The first category comprises official messages issued in reaction to an advice from the Counter-Terrorism (CT) Infobox, a cooperative group in the field of counter-terrorism and radicalism comprising *inter alia* GISS, DISS, INS, the Public Prosecution

[58] ECtHR 19 February 2009 (*A. a.o./United Kingdom*), A 3455/05, para. 220.

Service and the National Police Services Agency.[59] These are official messages concerning persons who are associated with terrorism and/or radicalism and who are for this reason included in the CT Infobox list. The employees of INS seconded to the CT Infobox have access to the information in the possession of GISS about persons on the list and can examine which information may be relevant for INS. This makes it possible to make an analysis based on the combined information of the two services and the information provision can be tailored to either the aliens law procedure or the naturalisation procedure.

The second category comprises the official messages not issued on the basis of an advice from the CT Infobox. These are official messages issued on the initiative of GISS or official messages issued in response to a request for information from INS. Apart from the INS employees seconded to the CT Infobox, INS has no insight into the information available at GISS. In the case of official messages not issued on the advice of the CT Infobox it is therefore the responsibility of GISS to notice that certain information is relevant for INS.

The procedure followed by INS to request GISS for information about an alien is known as a "*silent procedure*". When INS has not received a reaction from GISS within ten working days, the alien's procedure is continued without the information from GISS. The guiding principle is that such requests for information are addressed to GISS when there are signs that the service might have information relating to the alien in question. An example of such a signal is the fact that GISS has already issued an official message concerning the person in question before. Another example is that the statement made by the person concerned shows that there are links with areas of attention of GISS such as terrorism, radicalism or extremism.[60] If INS has started an investigation pursuant to Article 1F of the Convention relating to the Status of Refugees, there may also be reason to request additional information from GISS.[61]

The Committee points out that when GISS does an administrative check in its own databases at the request of INS to see whether any relevant information is available, this constitutes data processing within the meaning of the ISS Act 2002 (Article 1f ISS Act 2002). This means that such a check may only be carried out insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act (Article 12(2) ISS Act 2002). Since neither the ISS Act 2002 nor the Security Screening Act contains a provision making it possible for GISS to process data for the purposes of the task of INS, the check must serve the interest of national security. If the check yields relevant data and it is decided to provide these data to INS, this must be done in the form of an official message. The legal basis for issuing official messages to INS is Article 36 ISS Act 2002. This means that the provision of data, too, must be necessary in the interest of national security.

---

[59] See for more information on the CT infobox CTIVD review report no. 12 on the Counter-Terrorism Infobox Infobox, *Parliamentary Papers II* 2006/07, 29 924, no. 16 (annex). Also available (in Dutch) at www.ctivd.nl.

[60] See the annual reports of GISS.

[61] This Article provides that persons who have committed crimes or been guilty of acts contrary to the purposes and principles of the UN are not eligible for refugee status.

A policy document of GISS dated 28 October 2010 concerning administrative searches and checks shows that when GISS receives a request for a check, it assesses first of all whether such a check is consistent with the rules on the provision of data laid down in Articles 36-39 ISS Act 2002. This assessment takes account of the principles of necessity, proportionality and subsidiarity. The data is provided by means of an official message. The Committee observes with regard to this policy that the basis for the assessment that must be made before GISS proceeds to do an administrative check does not lie in the statutory provisions on data provision (Articles 36-39 ISS Act 2002), but in the general provision on data processing (Article 12 ISS Act 2002). Pursuant to Article 12 the administrative check must be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. As was explained above, an administrative check in response to a request from INS must be necessary for the purposes of the performance by GISS of its tasks, in the interest of national security. Providing data is a subsequent step which is separate from the decision to do an administrative check. The Committee recommends that GISS correctly sets out in the applicable policy document the legal basis for doing an administrative check at the request of INS as well as the related statutory requirements.

The Committee has found that in practice the requests from INS always lead to an administrative check by the front office of GISS, which is where these requests are received. The front office conducts the check to examine whether the request can be passed on to a specific team. The team will then further deal with the request. However, this first check is also a form of data processing which should satisfy the requirement of necessity in the interest of national security. In view of this fact the Committee holds that GISS must first assess the request against this requirement before it tries to link it to a team. The assessment can be made using the form supplied by INS which among other things states the reason for the request for information.

If GISS has the intention to provide information to INS, the draft official message will be submitted to the INS liaison, so that he can assess whether the information is useful for INS and whether the text has been drafted in such a way that the message can be used in the decision-making procedure of INS. This applies to both official messages on GISS' own initiative or in response to a request from INS, and official messages in reaction to an advice from the CT Infobox. Drafts of official messages of the latter category, however, are not submitted to the INS liaison until a later stage, because the primary assessment whether the information is useful is made by the INS employees seconded to the CT infobox. The main point of the assessment by the INS liaison is to ascertain that the message content is sufficiently concrete and clear so that the conclusion of the message is not incomprehensible without further explanation. This assessment is made bearing in mind the case law of the Administrative Jurisdiction Division of the Council of State.

As regards the roles played by the team and the legal department and the approval of the official message, the procedure for making official messages to INS is identical to the procedure described in section 4.2 above. Unlike the National Public Prosecutor, however, the INS liaison does not check the accuracy of the official message against the underlying file.

5.3 Findings of the Committee

5.3.1 The number of official messages in the review period

In the review period GISS issued 46 official messages to INS. These official messages therefore account for approximately 8% of the total number of official messages. At the beginning of the review period the number of official messages issued to INS per year was significantly lower than at the end. The Committee has established that a decline set in after a peak in 2004 caused by the introduction of the CT Infobox. Since the end of 2007 the number of official messages issued to INS again rose slightly due to the fact that GISS now also issues official messages about anti-integrative behaviour.

5.3.2 Legal basis

The legal basis for the provision of data to INS is Article 36 ISS Act 2002. This Article gives rules for the external provision of data for the purpose of the proper performance by GISS of its task. Where an official message is issued in connection with the withdrawal of a residence permit or an order declaring a person who in the opinion of GISS poses a threat to national security an undesirable alien, the link with the task of GISS is obvious. Preventing the naturalisation of persons who on the basis of their radical ideas reject or call on others to reject the Dutch democratic legal order or who sympathise with violent international jihad likewise falls within the scope of the task of GISS. The Committee holds the opinion that the official messages issued by GISS to INS in the review period could rightly be based on Article 36 ISS Act 2002.

In 2009 GISS issued two official messages to INS which were aimed at enabling INS to ward off the plea of Article 3 ECHR (prohibition of torture or inhuman treatment) by the alien in question in proceedings under aliens law. In those two cases the service provided information showing that the alien in question was staying or had stayed in the country of origin of his own free will. This enabled INS to oppose the allegation that the alien feared deportation on account of the risk of torture and/or inhuman or degrading treatment.

The Committee holds the opinion that these official messages, too, could rightly be based on Article 36 ISS Act 2002. When GISS has provided data to INS which contributed to the decision to deport the alien, GISS may also contribute to the deportation decision being upheld in the proceedings under aliens law by providing relevant further information. In such a case it is of course important that either the data in question had already been collected previously, or that for the purpose of the task of GISS there is reason to perform investigative acts yielding such further information.

5.3.3 Content

The Committee's investigation has shown that all but one of the official messages issued by GISS to INS in the review period (see section 5.3.4) are substantiated by the underlying information. The messages are, moreover, carefully formulated, so that they are in line with the underlying information.

The Committee has found that GISS does not use a consistent definition of the term "threat to national security". GISS considers on a case-by-case basis whether this conclusion applies. Each of the official messages examined by the Committee concerned activities having such a clear connection with national security, that in the opinion of the Committee they justified the conclusion. The activities consisted of actively supporting and/or participating in violent international jihad or participating in a terrorist organisation.

It emerged in section 5.1 that official messages to INS must contain sufficiently concrete and specific information to give the alien elements for his defence. In addition, GISS must take account of the fact that INS will not be permitted to simply base its decisions on the official message without inspecting the underlying documents if the text of the message does not show on which facts and circumstances its conclusion is based. In 2009 and 2010 GISS issued three official messages supplementary to official messages it had issued earlier. They concerned three separate cases in which INS had requested GISS to provide further factual information. In line with the judgment of the ECtHR in *A. e.a.* v. *United Kingdom*[62] the supplementary official messages stated, as far as was possible for reasons of source protection and keeping secret the current level of knowledge and/or the operational methods of the service, with which persons contacts were maintained and when these contacts took place. A judgment of the District Court of The Hague of 26 January 2010 shows that such an approach may lead to the decision-process being upheld.[63] However, the Committee draws the attention of GISS to the fact that it is important for the alien about whom the service issues an official message that he receives sufficient factual information at the earliest possible stage. When the protection of sources, the secrecy of the current level of knowledge and/or the operational methods of the service or the third party rule[64] do not constitute a reason to withhold concrete details, then in the opinion of the Committee GISS should therefore seek to provide INS with as much concrete information as possible.

---

[62] ECtHR 19 February 2009 (*A. a.o.* v. *United Kingdom*), A 3455/05, para. 220.

[63] District Court of The Hague 26 January 2010, *LJN*: BL0575.

[64] Foreign services often provide information subject to the condition that it may only be passed on if the foreign service in question has granted permission to do so. See for a more detailed discussion of this subject review report no. 22a of the Comm ttee on the cooperation of GISS with foreign intelligence and/or security services, *Parliamentary Papers II* 2009/10, 29 924, no. 39 (annex). Also available at www.ctivd.nl.

5.3.4 Indication of reliability or source reference

The Committee has established that the official messages issued by GISS to INS contain an indication of reliability.

In one case the Committee has established that with respect to part of the information provided the indication of reliability in the official message was not substantiated by the underlying file. In this official message, issued 2006, it was stated that the information "was obtained from a reliable source". The underlying information, which had been provided by the Regional Intelligence Service, did not include an indication of the source or its reliability. It emerged from the Committee's investigation that the reliability of the information from the Regional Intelligence Service had not been established. The Committee points out that the indication of reliability, like the rest of the text of the official message, must find support in the information in the possession of GISS. When it is not fully supported thereby, as in this particular case, the official message cannot be said to have been drafted with proper and due care. In this respect the official message is unlawful. The Committee therefore recommends that GISS records this in the relevant file pursuant to Article 43(2) ISS Act 2002 and informs INS that the reliability of the sources on which the first part of the official message is based has not been established.

As a result of the above case the Committee investigated more closely how the Regional Intelligence Services provide information to GISS pursuant to Article 60 ISS Act 2002 and whether in doing so they comply with Article 12(4) ISS Act 2002 as well. The notification forms used by the Regional Intelligence Services usually have a separate line for evaluating the reliability of the source. The Committee has found that this item is often not filled out. Where it is filled out, the reliability indication is ambiguous, since the Services use different coding systems and qualifications. This way of processing information is contrary to Article 12(4) ISS Act 2002. The Committee recommends introducing clear and unambiguous indications of the reliability of information passed on by Regional Intelligence Services to GISS.

6. Official messages to the ministry of Economic Affairs, Agriculture and Innovation

6.1 Use of official messages to the ministry of Economic Affairs, Agriculture and Innovation ("EAA&I")

The ministry of EAA&I is responsible for the export controls of strategic goods, including so-called dual-use goods. These goods are suitable for both civil and military use. Dual-use goods are often considered to be strategic goods because of the fact that they can be used to manufacture WMD.

The most important instrument for controlling the export of strategic goods is the licensing system. Formally, decisions on applications for export licences are taken by the Central Import and Export Office which falls under the customs and therefore under the ministry of Finance. When granting or refusing applications for export licences for strategic goods, however, the Central Import and Export Office acts on the instructions and under the responsibility of the minister of EAA&I. With respect to applications for exports to non-sensitive destinations, such as allies of the Netherlands, the Office has been authorized to deal with the applications independently. All other applications, including applications for exports to so-called countries of concern, are dealt with as regards content by the ministry of EAA&I. For various reasons, exports to these countries require special controls. When an application for the export of dual-use goods concerns export to a country of concern, the ministry of EAA&I will as a rule obtain information from the joint counter-proliferation team of GISS and DISS, the Counter Proliferation Unit.

When GISS provides information to the ministry of EAA&I for this purpose, this is considered an official message because the information is provided to a body which is authorised to act on the information by taking measures. This is so because information from GISS may result in refusal of an export application or the ad hoc imposition of an obligation to obtain a licence. It is true that these official messages come from the joint GISS and DISS unit, but they fall under the responsibility of the head of GISS. The official messages to the ministry of EAA&I are issued in the context of the task of GISS based on Article 36 ISS Act 2002.

The current arrangement between GISS and the ministry of EAA&I is that GISS indicates whether information is available which shows that the final customer or a middleman has ties with proliferation-relevant and/or military-sensitive projects. The official message may also provide information about whether the goods in question can be used in WMD programmes or for making means of delivery (e.g. cruise missiles). Based on an oral arrangement with the ministry of EAA&I, GISS expresses an opinion on the usability of the goods if it is expressly requested to do so. The legislature has vested the ultimate assessment of all the interests involved in the ministry of EAA&I .[65] In its decision-making process the ministry devotes attention to the exporter, the end-user and the middleman, the goods and their stated end-use and also the risk that the goods will be put to a different end-use. Refused licence applications are periodically discussed at the interministerial committee on exports of strategic goods, of which GISS is a member.

The Committee has found that GISS has started consultations with the ministry of EAA&I about laying down the arrangements in the field of information provision in a covenant. The Committee endorses the usefulness of such a covenant.

In addition to the official message issued in response to requests from the ministry of EAA&I it also happens that GISS issues an official message to the ministry of EAA&I when indications have

[65] Strategic Goods Decree, *Stb*. 2008, 252, Article 3(1.

emerged during an investigation that a person or company is circumventing the rules applying to the export of strategic goods. Such an official message may result in an inspection visit to the company or the imposition of an ad hoc obligation to obtain a licence.

Unlike the Public Prosecution Service and INS (on request), the ministry of EAA&I is not granted inspection of the files underlying the official messages. Pursuant to Article 40(3) ISS Act 2002, the minister of the Interior or the head of GISS on his behalf may decide to grant a person or an agency inspection of the information underlying the official message to the extent necessary to assess the accuracy of the message. So far, this option has not been used yet in respect of official messages to the ministry of EAA&I.

Decisions of the ministry of EAA&I on applications for an export licence for strategic goods are open to objection and appeal. Appeal lies to the Trade and Industry Appeals Tribunal (Article 13(1) Import and Export Act). When the ministry of EAA&I decides to impose an ad hoc obligation to obtain a licence, the party concerned can lodge an objection to this decision with the ministry and file an appeal with the administrative courts. In such proceedings against a decision based among other things on information from GISS, the ministry of EAA&I may have to submit the official message from GISS to the administrative court in order to substantiate a decision. In that case the rules of Article 8:29 of the Dutch General Administrative Law Act ("GALA") are followed, which provide that the court is informed that the document will only be disclosed to the court. The reason for this is that the official messages issued by GISS to the ministry of EAA&I for the purposes of the supervision of exports are classified state-secret. If the court decides that the restriction on disclosure is justified, the other party (the exporter) will also have to consent to the court partially basing its judgment on the official message (Article 8:29(5) GALA).

6.2 Procedure for making official messages to the ministry of Economic Affairs, Agriculture and Innovation

If an application for an export licence is submitted to GISS, the ministry of EAA&I submits the entire file containing the licence application, the underlying technical documentation and the preliminary report of the Central Import and Export Office[66]. Upon receiving the file, the Counter Proliferation Unit first examines whether any relevant information on the end-user and/or middleman concerned can be found in the databases of GISS and DISS. In certain cases the Unit will submit a request for information to foreign counterparts of GISS.

Generally, no preliminary consultations take place between the recipient body and GISS concerning official messages to the ministry of EAA&I, thus making the procedure different from the one applying to official messages to the Public Prosecution Services and INS.

[66] The Central Import and Export Office issues a preliminary report that is based on administrative checks in a number of databases and on information supplied by the exporter.

There are, however, periodical bilateral consultations concerning official messages in a general sense. For example, the parties discuss the use of certain standard phrases and terms. In principle, the Counter Proliferation Unit does not provide oral information on the substance of specific official messages, because ultimately the ministry can only base its decisions on information it has received in writing. Questions serving to elucidate official messages already issued may, however, be answered.

Just like the official messages to other recipients, official messages to the ministry of EAA&I are successively approved by the team head, the legal department, the unit head and finally the management of GISS.

6.3 Findings of the Committee

6.3.1 The number of official messages issued in the review period

Because GISS plays a standard role in the procedure for assessing licence applications for exports of dual-use goods to countries of concern, the annual number of official messages issued to the ministry of EAA&I is high. In the review period GISS issued 340 official messages to the ministry of EAA&I; about 60% of the total number.

6.3.2 Classification

The official messages issued by GISS to the ministry of EAA&I differ from other types of official messages because they are classified state-secret and for this reason cannot be provided to the person or company concerned. This is not consistent with the basic principle emerging from the Explanatory Memorandum to the bill containing the ISS Act 2002 (underlining by the Committee):

> "If it is expected that the competent authority will, on the basis of the information to be provided, take measures against the person concerned which may prejudice his legitimate interests, the information shall be provided by means of a written (unclassified) official message."

A footnote to the Explanatory Memorandum states that the term unclassified official message means an official message that is drafted in such a way that the person to whom the official message relates can without any objection take note of its content.The Explanatory Memorandum puts forward two reasons for the principle:

> "On the one hand it creates the possibility for the agency concerned to take the measures with due care and substantiated by reasons and on the other hand the procedure makes it possible for the person concerned to defend himself in court."

The interviews conducted by the Committee with employees of GISS showed that GISS takes the position that the main reason for classifying the official messages lies in what these messages reveal about the current level of knowledge at GISS. The messages indicate what is the information position of GISS with respect to specific end-users and/or middlemen in the intended countries of destination of the goods. Evilly-disposed persons having this knowledge might adjust their licence application, e.g. by stating different end-users. Usually, moreover, the information in question originates from ongoing investigations of GISS. Another factor that plays a role, so GISS stated, is that these official messages are often based on information from foreign counterpart services to which the third party rule applies.

The Committee observes in this context that the considerations mentioned by GISS apply to a certain extent to all official messages issued by GISS. Balancing interests, the service has decided to disclose its current level of knowledge concerning a specific person or organisation so that measures can be taken. The idea is that the measures will eliminate or reduce the threat emanating from the subject under investigation, so that it will perhaps no longer be necessary to conduct further investigations (at any rate of that specific person or organisation. This does not hold good in the case of official messages for the purpose of export applications. These official messages state in particular to what extent certain companies in foreign countries can be associated with the proliferation of WMD. It is not possible, however, to take measures against these companies, because they are established abroad. If an attempt to acquire goods is foiled, the threat emanating from these companies will not decrease. In this situation national security is best served by secretly identifying the attempts of these companies to acquire certain goods and by preventing the Netherlands from making a contribution to proliferation by enabling the ministry of EAA&I to refuse the licence applications concerned. If the information position of GISS regarding companies in certain countries becomes public knowledge, the possibility of monitoring their actions disappears. The Committee holds the opinion that in those cases the general interest of national security must carry greater weight than the individual interest of the exporter in learning the content the official message. Taking into consideration that the information provided to the ministry of EAA&I in connection with export applications will by definition reveal nature be traced to the current level of knowledge of GISS regarding companies in countries of concern, the Committee holds the opinion that the classification of these official messages is justified.

This opinion of the Committee is supported by a recent judgment of the District Court of Haarlem.[67] The exporter in this case had lodged an appeal against the fact that he had not been

[67] District Court Haarlem 14 September 2010, AWB 10/2199, 10/3929, 10/3930, 10/3932, 10/3933. 10/3934, 10/3979 and 10/3990.

permitted to learn the content of the official messages from GISS that formed the basis of nine refusals of licence applications. The District Court ruled that restricted disclosure of the official messages was justified in the interest of keeping secret the current level of knowledge, the sources and the operational methods of GISS. Of decisive importance was the consideration that if the official messages were to be disclosed, the risk that the implementation and enforcement of legislative and other rules would be frustrated might materialise. Based on the information stated in the official messaged other exporters would be able to develop a method to circumvent the aforementioned legislative and other rules, in particular the restrictions on exports to Iran.

Although the Committee holds the opinion that the classification of the official messages is justified, it points out that the state-secret nature of the messages does not only have disadvantages for the exporter concerned, but also for the ministry of EAA&I which has based its decisions on secret information. If administrative proceedings should ensue, then because of the agreements made on the subject between GISS and the ministry of EAA&I it is for GISS to decide whether an official message may be disclosed to the court. If GISS decides that the official message may not be submitted in evidence, for example because of the third party rule, the court may draw such conclusions from this fact as it deems appropriate (Article (8:31 GALA). This might have the result that the decision of the ministry of EAA&I is reversed.

The problem discussed above can be illustrated with an example from the Committee's investigation. In 2006 and 2007 GISS, in response to export applications filed by a company, issued official messages to the ministry of EAA&I providing information on the ties of the named end-user with a nuclear programme. On the basis of this information the ministry of EAA&I imposed ad hoc licensing obligations on the company for certain types of goods. The company filed objections with the ministry, lodged an appeal with the district court and subsequently appealed to the Court of Appeal. For the purposes of the proceedings before the Court of Appeal the ministry of EAA&I asked GISS for permission to submit the information provided by GISS at an earlier stage to the Court of Appeal, in order to give insight into the substantiation of the decisions. In reply to the request GISS communicated that it preferred issuing a new official message instead of permitting the ministry to submit the earlier official messages in evidence. But the new official message that was issued for submission in the appeal proceedings contained less specific information than the earlier official messages. This posed a potential problem for the ministry of EAA&I in the proceedings, since it was not permitted to submit the information on which the challenged decisions were based. In this situation the ministry of EAA&I had no choice but to wait and see whether the appeal court would find that the new, more cautiously drafted official message also constituted a sufficient basis for the decision. In this particular case the exporter withdrew the appeal to the Court of Appeal, so that the court did not give a decision on the issue.

The Committee has found that GISS' decision in this case to provide less specific information to the ministry of EAA&I for the purposes of the appeal proceedings was connected with an

ongoing investigation of the service. For operational reasons GISS considered it too great a risk to allow the earlier official messages to be submitted in evidence to the Court of Appeal. The Committee appreciates the arguments of GISS, but it holds nevertheless that it is not right that the ministry of EAA&I was entirely dependent on GISS in the matter. When classified information is disclosed to a third party for use in the decision-making process of an administrative body, then from the perspective of GISS there is no reason not to disclose this information to the courts, subject to secrecy. If the information is highly sensitive with a view to source protection and keeping secret the current level of knowledge and/or the operational methods of the service or if it has to observe the third party rule, these are reasons for not disclosing the information to the ministry of EAA&I. The Committee holds the opinion that once this step has been taken, GISS can hardly deprive the ministry of EAA&I of the possibility to substantiate its decision by submitting the official message to the court.

Now that the exporter cannot be given the possibility of learning the content of the official message and as a result is not in a position to question the statements of GISS, this emphasizes the importance of careful decision-making by the ministry of EAA&I. For this purpose the ministry of EAA&I must have sufficient factual information at its disposal. Because standard phrases are used that give a general description of the underlying information, the text of these official messages does not furnish a great deal of factual information (see on this issue section 6.3.3.1). Moreover, the ministry of EAA&I is not granted inspection of the documents underlying the official messages, in spite of the fact that GISS' contact at the ministry has A-level screening. The Committee draws attention to what the Explanatory Memorandum to the ISS Act 2002 stated about inspection of the documents underlying official messages:

> "Where a measure has far-reaching consequences for the party concerned and the decision-making authority has little or no other incriminating material in its possession, the competent authority will as a rule be given the opportunity, subject to secrecy, to inspect the information constituting the basis of the official message that has been issued. This serves the purpose of enabling the authority, acting as a careful administrative body, to make sure that the facts are supported by the underlying information which must be kept secret, for example for reasons of source protection."[68]

The regular bilateral consultations between GISS and the ministry of EAA&I about official messages generally, and sending intelligence reports in order to furnish certain background information are steps in the right direction, but in the opinion of the Committee they do not sufficiently overcome the problem of the ministry's limited information position. The Committee therefore recommends that GISS, in consultation with the ministry of EAA&I, seeks ways to promote that the ministry can make its decisions on the basis of an adequate information position. One possibility is that of granting the ministry of EAA&I, where necessary, inspection of the documents underlying the official messages.

---

[68] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 55.

6.3.3 Content

6.3.3.1 The use of standard phrases and terms

Since GISS issues many official messages to the ministry of EAA&I per year, it is increasingly using standards phrases in the official messages. In the summer of 2010 the ministry of EAA&I, in consultation with the Counter Proliferation Unit, prepared a matrix setting out how the information received from GISS will be reproduced in the decision to be received by the exporter. This 'translation' is necessary because of the classified nature of the official messages. The matrix mentions four categories of ties with proliferation-sensitive projects in the order of increasing seriousness:

1) no ties with proliferation-sensitive projects;
2) end-user/middleman is an entity of concern;
3) end-user/middleman has no direct ties or has indirect ties with proliferation-sensitive projects;
4) end-user/middleman has ties with proliferation-sensitive projects.

The Committee has established that in the past particularly the category "no direct ties" was not always applied consistently. GISS informed the Committee that this category is used when it has not been established that the middleman/end-user himself has ties with sensitive projects, but that he can be related to another company that has ties with sensitive projects. Although the matrix that has been prepared is primarily intended as a guideline for the ministry of EAA&I in its communications with exporters, the Committee expects that it will promote consistency in the official messages. The formalisation of the 'translation' of the different standard phrases has produced clarity.

The Committee points out, however, that the use of standard phrases having a fixed meaning entails the danger that certain qualifications disappear from the messages. It further observes that the chosen wordings have a low factual content. Where it is stated, for example, that a specific end-user/middleman has ties with proliferation-sensitive projects (further referred to as: sensitive projects), this does not show the exact nature of the ties. The Committee has found that general descriptions were chosen because in many cases the underlying information originated from foreign counterpart services. On account of the third party rule, the Counter Proliferation Unit usually does not have the option of passing on the information it has obtained, while it does consider it necessary to do so to give the ministry of EAA&I a signal for the purposes of its decision-making.

The Committee considers it important that GISS assesses for each official message separately whether the chosen standard phrase adequately represents the underlying information and

whether it is possible to provide more factual information than the standard phrase without affecting the agreements made with foreign counterpart services and the secrecy of sources, current level of knowledge and/or the service's operating procedure.

A frequent closing sentence of the official messages to the ministry of EAA&I is that it cannot be excluded that the goods will be used in sensitive projects. The Committee has noticed that this sentence is used inconsistently in the official messages issued to the ministry of EAA&I in the review period. When asked about this, GISS stated that there was no clarity as to when the sentence could be used. For this reason GISS had decided that it would no longer include the sentence in official messages in the future. The Committee agrees with this decision, since the sentence does not add any substantial information while the ministry of EAA&I did in fact interpret it as an aggravating note in the official messages.

As a result of the standardised nature of the official messages issued by GISS to the ministry of EAA&I, certain expressions keep recurring. This is understandable, but it entails the risk that certain matters are ranged under a common denominator which is not fully applicable in all cases. A frequently used expression in these official messages is "associated with". The Committee has found that this expression may refer to several types of connections. It can mean, for example, that there are commercial family or ownership connections. The expression is also used when the end-user/middleman in a certain project is the party that awarded a contract to another company. The Committee holds the opinion that where a company has merely awarded a contract in a certain project, this cannot be said to imply a lasting relationship. It holds that the expression "associated with" is not a correct description of temporary collaboration. The Committee considers it important that henceforth GISS chooses a description that is as closely as possible in keeping with the underlying information.

6.3.3.2 Substantiation

In the course of its investigation the Committee had a number of interviews with employees of GISS about the official messages issued to the ministry of EAA&I. During these interviews attention was paid to the nature of the messages. Initially, the discussion was about whether or not this form of providing information must be considered official messages. As was explained in section 6.1 above, the Committee holds the opinion – and by now GISS also does so – that the messages must indeed be considered official messages, since they provide information to an authority which is authorised to take measures. Precisely because official messages may lead to measures being taken, it is important that the information provided is substantiated by the underlying file.

It has emerged from the Committee's investigation that GISS, which formerly did not consider the messages to the ministry of EAA&I to be official messages, did not always set very high

requirements on the substantiation of the messages. The Committee will now discuss two cases in which the underlying information proved to be insufficient basis for the message.

In the first case, an official message issued in 2008, the ministry of EAA&I was informed that the end-user had connections with sensitive projects. Upon examining the file the Committee found that this allegation was based on a refusal of an application for an export licence by another country. In a European context and also in the context of certain multilateral forums, such refusals (further called "denials") are exchanged.[69] The reason stated for the denial was that there was an unacceptable risk of diversion to a ballistic missile programme. The Committee considered this denial to constitute insufficient substantiation for the allegation that the end-user had connections with sensitive projects. Apart from the end-user, the nature of the goods may also play an important role in the context of such denials. Since the aforementioned denial related to a different type of goods, the Committee deems it possible that the nature of the goods played a role in the decision-making of the country in question. Without making inquiries at the authorities of this country, GISS should not have concluded from the denial that the end-user had connections with sensitive projects. The Committee therefore holds the opinion that the official message in question is not substantiated by the underlying information. The official message was not drafted with proper and due care and is therefore unlawful.

The second example of an official message which in the Committee's opinion is not substantiated by the underlying information is another message issued in 2008. The conclusion that the end-user had ties with sensitive projects was substantiated by a message from a foreign counterpart service. The information from the counterpart service only showed that the end-user was included in the watchlist[70] of the country in question and that a denial had been issued in the past with respect to the end-user. The reason stated for the denial was the risk that the goods would be used to manufacture equipment which might be deployed against the armed forces of European Member States or their allies. In addition, the denial stated that there was a risk that the goods would be diverted within the country of destination or would be re-exported under undesirable circumstances. In the opinion of the Committee the information provided by the counterpart service does not show that the end-user actually had ties with sensitive projects. Since the further information in the file cannot substantiate the said ties with sensitive projects either, this official message, too, is not adequately substantiated. In the Committee's opinion, therefore, this official message is unlawful as well.

The Committee recommends that GISS, pursuant to Article 43(2) ISS Act 2002, makes a record of this fact in the relevant file and informs the ministry of EAA&I, with a view to possible

[69] The policy within Europe is that such a denial in one country constitutes reason for other countries not to grant export licences either in the case of similar transactions. Similar transaction in this context means: the same product, or a product having sufficiently similar technical characteristics, and also the same intended end-user.

[70] Some countries compile a so-called *watchlist* of companies which for various reasons are labelled "entity of concern". Such a list contains e.g. the end-users that have been reason for the country in question to deny an export licence. Watchlists are usually accessible to the public so that exporters can consult them.

future applications for export licences for the benefit of the end-users concerned, that the two aforementioned official messages are not substantiated by the information in the possession of the service.

6.3.4 Mention of denials

It emerged in section 6.2 that the Central Import and Export Office issues a preliminary report based on administrative checks in a number of databases before the file is sent to GISS. One of these databases is the database compiled at European level and containing all denials of the Member States. The exchanged denials from other regimes such as the Australia Group[71] and the Missile Technology Control Regime (MTCR)[72] are also included in this database. In addition to the Central Import and Export Office, the ministry of EAA&I and GISS also have access to this database. The Committee has established that it frequently happens that GISS mentions denials in the official messages. In 2010 it was agreed that GISS would only mention denials if the preliminary report of the Central Import and Export Office shows that it has not found the denials in question while they are in fact registered in the system.

The Committee observes here that double checking may have the result that ultimately neither party checks the information really carefully, because each party assumes that the other party has already done so. It should be clear who is responsible for consulting the database. The Committee was told by GISS that early in 2011 it was arranged with the ministry of EAA&I that the responsibility for checking the database would rest with this ministry.[73] Consequently, GISS will no longer mention denials in the official messages.

6.3.5 Indication of reliability or source reference

The Committee has found that the official messages issued by GISS to the ministry of EAA&I in the early part of the review period usually do not contain an indication of reliability. This means that in this period GISS did not comply with the statutory requirement of Article 12(4) ISS Act 2002. From early in 2009 GISS has included an indication of reliability in the official messages, with the result that the ministry of EAA&I now obtains an understanding of the quality of the information on which its decision-making is based.

---

[71] The Australia Group is an international forum within which non-binding rules have been drawn up for the export of certain 'sensitive' goods which rules are intended to prevent the proliferation of chemical and biological weapons. See also: www.australiagroup.net.

[72] The goal of the Missile Technology Control Regime is to prevent the proliferation of weapons of mass destruction by controls on the export of delivery systems for weapons of mass destruction (other than manned aircraft). Non-binding rules have been drawn up for this purpose. See also: www.mtcr.info.

[73] Although this arrangement falls outside the review period, the Committee mentions it for the sake of completeness.

It is the opinion of the Committee that the fact that in the earlier period the messages to the ministry of EAA&I were not considered official messages is not an adequate explanation for omitting to include an indication of reliability in the messages over a long period. The statutory requirement that data processed by GISS must be accompanied by an indication of reliability or source reference applies not only to official messages, but to all forms of data processing for the purposes of the performance by the service of its tasks. Consequently, this requirement would also have applied if the messages to the ministry of EAA&I had been advisory letters, as GISS used to think. Moreover, GISS knew that the ministry of EAA&I would include the information provided by GISS in its decision-making process, so that it should have been clear that an indication of its reliability was necessary for the ministry to be able to assess the value of the information.

Meanwhile, GISS has made arrangements with the ministry of EAA&I about how the reliability of information from various types of sources is assessed and how this is represented in the official messages. In March 2010 these arrangements have been formalised in a policy document which is applied consistently, so the official messages examined by the Committee show.

Pursuant to this policy document, information from public sources, for example the Internet, is represented in official messages as follows: *"from a publicly accessible source …"*. The interviews held by the Committee in the course of its investigation have shown that both the ministry of EAA&I and GISS collect information about end-users/middlemen from publicly accessible sources. At the ministry of EAA&I this is done during the stage following the despatch of the file to GISS. When GISS reports to the ministry of EAA&I that certain information on the end-user/middleman has emerged from a publicly accessible source, it may happen that it is not clear to the employees at the ministry whether this is the same information they had already found themselves. Although it is possible that the ministry of EAA&I will consult with GISS in case of doubt, the Committee fails to see why GISS does not mention the specific public source of information in the official messages, so that no misunderstandings can arise on this point. Transparency should be pursued wherever possible, certainly in the context of a task – in this case the collection of information from publicly accessible source – which is performed by two agencies.

As a result of recent interviews with the Committee, this point was the subject of internal consultations at GISS. It was decided that GISS will henceforth mention the specific source of the public information it has found.

Information from human sources is seldom used in official messages to the ministry of EAA&I. The Committee has established that the Counter Proliferation Unit, unlike the other departments of GISS, does not prepare reliability memorandums for the underlying file in such cases. This is not in keeping with general policy at GISS in this area. The Committee recommends that the Counter Proliferation Unit adjusts its procedure.

6.3.6 Requirements applying to the provision of personal data

By far the largest part of the official messages issued by GISS to the ministry of EAA&I relate to companies in the countries of destination of the goods. It is open to discussion whether the statutory provisions that are applicable to the external provision of personal data are also applicable to these official messages. The definition of personal data in the ISS Act 2002 is (virtually) identical to the definition in the Personal Data Protection Act:[74]

> "information relating to an identifiable or identified, individual natural person"
> (Article 1(e) ISS Act 2002)

When deciding this issue the Committee therefore followed the explanation given to this provision in the Personal Data Protection Act. The Guide for persons who process personal data, drawn up by the ministry of Justice, shows that as a rule data on enterprises are not personal data. Exceptions are only made for certain data on one-man businesses which can be traced directly to the owner of the business. The Committee therefore holds the opinion that the data provided by GISS to the ministry of EAA&I is not personal data.

Nevertheless, the Committee finds that where data is provided which may result in measures being taken against persons or companies, the same proper and due care must be exercised as in the case of the provision of personal data. An official message to the ministry of EAA&I may, for example result in denial of an export licence, which is a measure which, though not directed against the middleman or end-user with respect to whom data have been provided, may yet have far-reaching consequences for the applicant. Because of the potential consequences of the provision of such data the Committee considers it appropriate that the special requirements of proper and due care mentioned in Articles 40, 41 and 42 IIS Act 2002 apply to the official messages to the ministry of EAA&I.

One of the safeguards ensuring that personal data will be provided with proper and due care is the provision that personal data may not be provided if it cannot in reason be established that the data is accurate or if the data has been processed more than ten years ago and no new data has been collected regarding the person since then (Article 41(1) ISS Act 2002). According to the policy in place at the Counter Proliferation Unit, information used in official messages to the ministry of EAA&I must not be older than ten years. However, the information can also prove out-of date before then, for example if the situation in the country in question has changed dramatically. When the information is so incriminating that it really cannot be disregarded, the service may decide to include information older than ten years nevertheless. The Committee has established that the Counter Proliferation Unit applies these guidelines.

The Committee holds the opinion that this policy satisfies the requirements of due care to a

[74] Conceptually, the ISS Act 2002, where relevant, follows the Personal Data Protection Act. (*Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 17).

sufficient degree. By analogy with Article 41(3) ISS Act 2002, however, the degree of reliability and the age of the data must be mentioned if the data on which the official message or part of the official message is based is older than ten years.

In one case GISS issued an official message to the ministry of EAA&I containing information which dated back twelve years. The Committee points out that if this information was deemed so incriminating that it could not be disregarded, the official message should in any case have mentioned the degree of reliability and the age of this information, which did not happen in this case. The Committee considers this to be negligent.

Another requirement of due care which is appropriate in the case of the official messages to the ministry of EAA&I, given their purpose and the interests at stake, is the requirement that the information must be provided in writing. The Counter Proliferation Unit does indeed have a rule that all (specific) data provision to the ministry of EAA&I takes place in writing. The Committee has found that this rule is usually observed meticulously at the Counter Proliferation Unit. In two cases, however, the Committee has established derogation from this policy. In both cases the Counter Proliferation Unit had relevant information which – on the basis of the policy outlined above – was found too old to be provided to the ministry of EAA&I. The information was indeed not incorporated in the official messages that were issued. Oral information was, however, communicated from the Counter Proliferation Unit to the ministry of EAA&I that 'something' had been found. The exact content of these communications can no longer be retrieved. The Committee considers that the Counter Proliferation Unit has acted with due care in both cases by not wishing to include the outdated information in the official messages. It points out to GISS, however, that a communication that something has been found, without any indication of what the information consists of, can also influence the decision-making process. The Committee holds the opinion that for reasons of due care the service must refrain from making such remarks in its contacts with the ministry of EAA&I.

6.3.7 Documentation

In the past few years the files of the official messages to the ministry of EAA&I have distinctly gained in clarity. Although formerly, too, the files always included a so-called "investigation export form", on which it was recorded which investigative actions had been performed in response to the request from the ministry of EAA&I and certain documents from the underlying file were named, it was nevertheless not always easy to understand the underlying file, which was often fairly technical in nature. Early in 2009 the Counter Proliferation Unit started adding an annotated version of the official message to the underlying file, in which it stated the document numbers of the underlying documents supporting the information in the official message. In the opinion of the Committee this is a great improvement, since now it is immediately clear how the underlying documents have been used.

Sometimes, only the relevant pages of large documents are included in the files of the official messages issued to the ministry of EAA&I, or it is otherwise impossible to retrieve from which document the pages are taken. The Committee recommends that in such cases the Counter Proliferation Unit indicates what is the document concerned and mentions its date.

7. Official messages to political party chairpersons

7.1 Background and policy

In 1993 the media brought the news that members of organised crime had attempted to infiltrate politics by nominating candidates for municipal elections. In reaction to the news a discussion flared up in the Second Chamber about countering such attempts.[75] In this context the Second Chamber also discussed the role of the National Security Service (BVD), which had issued official messages regarding the political candidates to the political parties for which they were candidates.The minister of the Interior explained to the Second Chamber that the National Security Service had issued official messages to the parties themselves, because ultimately the party is the entity which the person concerned can call to account if consequences are attached to the information.The minister stated that four considerations play a role in deciding to provide incriminating information:

1. the importance of the position which the person concerned has or wishes to acquire in relation to politics;
2. the position of the person concerned relative to organised crime;
3. the question whether this fact could also become known without the interference of the National Security Service;
4. the question how the issue relates to the fundamental rights of the person concerned, such as his right to be elected and the right to be able to defend himself.

Summarising,the minister stated that the matter called for restraint and that the prime consideration should be the self-correcting capacity of politics.The National Security Service could only have a task in the matter if the facts and circumstances gave reason for serious suspicions and the party concerned could not itself become aware of them.

The basic principles of a political party's own responsibility and of subsidiarity described by the minister of the Interior were maintained in the agreements made in 1997 with the political parties. In May 1998 these agreements were laid down in the Memorandum "The National

[75] *Proceedings II*, 17 February 1994, 52, 3974-3975.

Security Service and integrity risks with respect to (candidate) political office holders".[76] The Memorandum outlines the procedure for dealing with a request for information from a party. The Memorandum states first of all that the National Security Service does not do security screenings of political office holders, because political offices cannot be considered to be offices of confidentiality.

The 1998 Memorandum provides that the National Security Service will provide information in two situations:

1. At the request of a political party the National Security Service has investigated a person who is suspected to pose a threat to the integrity of the public sector;
2. In the context of its ongoing performance of its tasks the National Security Service has come across a (candidate) political office holder who may pose a threat to the integrity of the public sector.

With regard to investigations by the National Security Service at the request of a political party, the Memorandum states that the National Security Service may only comply with such a request after the party has itself used all possibilities to investigate misgivings. For this purpose the party can ask the person concerned to submit a detailed resume, a statement of other positions he is holding and a certificate of good character. Furthermore, the party can hear informers and references about the person concerned. If after using the aforementioned means there is or continues to be a suspicion that the person concerned poses a threat to the integrity of the public sector in some form or other, then the National Security Service may investigate the person. Having regard to the principle of proportionality the National Security Service must, in doing so, take account of the seriousness of the suspicion and the gravity of the threatening impairment of the integrity of the public sector.

In October 2006 a new policy memorandum was drafted, on the basis of the ISS Act 2002, concerning GISS and integrity risks relating to (candidate) political office holders (further referred to as: the policy memorandum). This policy memorandum was sent to the political party chairpersons. As in the earlier version, the own responsibility of the political parties and the principle of subsidiarity are the guiding principles of the policy. Pursuant to the memorandum GISS may only be called in if, after using all means available to a party, a suspicion exists or continues to exist that a (candidate) political office holder poses a threat to the integrity of the public sector in some form or other. The greatest substantive difference with the earlier memorandum is that the new policy distinguishes between conducting an administrative check and conducting an investigation. The memorandum states that if a request from a political party gives reason to any action on the part of GISS, the first action will consist of doing an

[76] The term political office holders means: aldermen and members of the provincial executive, mayors and Queen's commissioners and people's representatives at the central and decentralized levels and representatives in the European Parliament. See also *Parliamentary Papers II* 2005/06, 28 479, no. 26, p. 1.

administrative check in the service's own databases. If the result of the administrative check, in combination with the information provided by the political party, gives rise to the serious suspicion that the (candidate) political office holder poses a threat to the democratic legal order, national security or other vital state interests, then GISS can conduct an investigation based on its task under (a). As regards legal basis, the policy memorandum places doing an administrative check in the same category as providing information (Article 36 ISS Act 2002).

In September 2010 GISS revised the policy memorandum and sent it the chairpersons of the political parties in the Second Chamber. The most recent version of the policy memorandum is directed at candidate members of parliament, instead of the wider group of (candidate) political office holders. The reason stated by GISS for this adjustment is that in recent practice the rules had been applied only to candidate members of parliament. Another change is that the new version states more emphatically that it is the responsibility of the political parties to investigate the integrity of (candidate) political office holders.[77] In addition, it has now become an element of the procedure that the Committee is informed whenever information is provided on a (candidate) political office holder. For the rest the text drafted in 2006 has been maintained.

The Committee holds that the provision of information on a (candidate) political office holder to a party chairperson in response to a request or on the own initiative of GISS is an official message, since the information is provided to the body that is authorised to take measures as a result of the information, for example withdrawing or replacing a candidate for a specific political office.

The policy memorandum defines an administrative check as a form of providing information pursuant to Article 36 ISS Act 2002. As was already discussed in section 5.2, the Committee considers this definition to be incorrect. Pursuant to Article 1(f) ISS Act 2002, consulting and/or compiling data falls under the term data processing. GISS has power to do this pursuant to Article 12(1) ISS Act 2002. Providing data is another form of data processing on which the law imposes special requirements (Articles 36-42 ISS Act 2002). Every act of data processing by GISS must in itself be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act (Article 12(2) ISS Act 2002). The legislative history shows that this provision means that the service may process data either for the purpose of the performance by the service of its tasks, or for the purpose of the statutory activities of the service falling outside the performance by the service of its tasks (see section 3.1.1). GISS may only do an administrative check in reaction to a request for information from a party chairperson in the context of its statutory tasks. This must be assessed directly; the objective of the administrative check must form part of the performance of the statutory tasks under Article 6(2) ISS Act 2002. In the absence of a legal basis for processing or providing data for the purpose of the tasks of the party chairpersons, providing data to party chairpersons cannot be a separate purpose of the administrative check.

[77] The policy memorandum of 2006 states that it is "advisable to a high degree" that the parties investigate misgivings themselves. The recent version states that political parties are themselves respons ble for ascertaining that the political office holders of their party do not pose a risk for the integrity of the public administration.

As was stated in section 3.1 of this review report, Article 12 ISS Act 2002 sets a number of general requirements for data processing including the requirement that the data processing must be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. In the case of an administrative check in response to a request for information from a party chairperson, the data processing must be necessary for the performance by GISS of its task, in the interest of national security. In addition, the data must be processed with proper and due care and the data must be accompanied by an indication of reliability or a source reference. Since in the situation under consideration here the data processed are personal data, it must also be examined whether the person in question falls in any of the categories mentioned in Article 13(1) of the Act. Providing the processed data is a separate step, which must be assessed against the statutory requirements set for providing (personal) data to external recipients.

The Committee observes that the policy memorandum makes no mention at all of the fact that the processed data must be accompanied by an indication of the degree of reliability or a reference to the source from which the data have been obtained (Article 12(4) ISS Act 2002).

The policy memorandum does on the other hand devote attention to certain conditions that must have been satisfied before a request for an administrative check can be complied with. The memorandum states that the possibility of calling in GISS does not enter the picture until it emerges, after all means available to the party have been exhausted, that a suspicion exists or continues to exist that a (candidate) political office holder poses a risk in any shape or form to the integrity of the public sector. First of all the Committee observes in regard to this criterion that the integrity of the public sector is not mentioned in the description of the tasks of GISS as one of the interest which the service is to protect. The Committee points out that the terms "continued existence of the democratic legal order" and "national security or other serious state interests" provide sufficient starting points for investigating certain integrity issues. The Committee considers it important, however, that GISS assesses critically on a case-by-case basis whether the misgivings that have arisen, in combination with the position for which the person in question is eligible, offer sufficient connecting points with the statutory mandate of GISS.

Naturally it is important that GISS is given sufficient information to be able to assess what is the basis for the suspicion of the party chairperson and whether there are sufficient connecting points with the service's statutory mandate. For this purpose the policy memorandum provides that a request for an administrative check must be filed in writing and must state the suspicions that have arisen against (candidate) political office holder and the grounds on which they are based. A policy document on searches and administrative checks by GISS that was recently approved by the service for internal purposes sets an additional requirement for requests from party chairpersons: the request letter must also state the means the party has used itself. This requirement is not included, however, in the policy memorandum furnished to the party chairpersons. The Committee draws the attention of GISS to the fact that if the misgivings that have arisen against a (candidate) political office holder are already sufficiently specific and if the

nature of the misgivings shows that it would be useless or even counterproductive for the party to start investigating the matter itself, the mere mention of the misgivings that have arisen may constitute sufficient reason for an administrative check. In other cases the Committee considers it appropriate, for the purposes of assessing the necessity criterion which includes the element of subsidiarity, that the party chairperson states which means the party has used to investigate the misgivings against the (candidate) policy office holder. It recommends that GISS includes a requirement in the policy memorandum that party chairpersons, when filing a request for information with GISS, either state the means which the party has already used to investigate the misgivings, or state brief reasons why the party has not itself used any means.

The group of persons about whom data may be processed pursuant to the policy memorandum consists of the (candidate) political office holders with respect to whom a suspicion exists that they pose a risk to the integrity of the public sector.The Committee holds the opinion that these are persons who fall in one of the following two statutory categories:

1. persons who give cause for serious suspicion that they pose a danger to the democratic legal order, or to national security or other vital state interests (Article 13(1)(a) ISS Act 2002);
2. persons whose data are necessary to support the proper performance by the service of its tasks (Article 13(1)(e) ISS Act 2002).

The Committee holds the opinion that insofar as no cause for serious suspicion exists with respect to the persons regarding whom an administrative check is done, these persons fall in the second category. This is based on the fact that the check is often a necessary first (supporting) step to assess whether there is cause for serious suspicion and for conducting an investigation for the purposes of GISS' task under (a).

The policy memorandum prescribes that GISS must report the findings of the administrative check and/or any investigation conducted pursuant to GISS' task under (a) to the party chairperson insofar as necessary having regard to the purpose of the administrative check or investigation. This is in accordance with Article 12(2) in conjunction with Article 36 ISS Act 2002. Data must be provided in writing, in accordance with Article 40(1) ISS Act 2002.

With regard to the most recent adjustment of the scope of the policy memorandum[78] the Committee observes that from a legal perspective there are no reasons to exclude regional (candidate) political office holders from these rules in advance.When the nature of the misgivings that have arisen is such that there might be a risk to the interests which GISS must protect given the position to which the person in question is aspiring or which he is holding, it will be lawful for GISS to do an administrative check in its own databases and provide any data found to the party chairperson.

[78] The policy memorandum currently relates only to candidate members of parliament instead of the wider concept of (candidate) political office holders.

With regard to the restriction of the scope of the rules to candidates for political offices the Committee has asked itself whether it is legally permitted to issue an official message to a party chairperson concerning an incumbent political office holder against whom certain misgivings exist. One objection might be that the party chairperson is not in a position to remove the person in question from office. Viewed in this light the requirement of necessity might preclude issuing such an official message. The Committee finds that it can only be necessary to issue an official message in the interest of national security if the risk posed to national security can be reduced by the measures which the recipient is authorised to take. In the case of incumbent political office holders with respect to whom misgivings exist, the risk to national security lies in the powers attached to the office. For example, the office holder has access to certain rooms, documents and persons and could moreover abuse the attention paid to his or her statements. A party chairperson has a number of means at his disposal to take action against the political office holder. Examples of such measures are that of depriving the office holder in question of his membership of the parliamentary group or of his or her position as spokesperson. It is true that these measures are aimed at changing the position of the office holder within the party, but they will not bring about a reduction of the risk attached to his position as a political office holder. The Committee considers it possible, however, that the party chairperson is in a position to induce the office holder in question to resign by talking to him. Bearing in mind the possible effectiveness of this approach, the Committee therefore holds the opinion that the law does not preclude the issue of an official message concerning an incumbent political office holder.

In view of the special nature of the procedure discussed here, it is the opinion of the Committee that it is important that the policy memorandum provides a clear and complete framework for both party chairpersons and GISS. This requires among other things that the memorandum correctly represents the legal basis pursuant to which GISS may do administrative checks in its own databases. The Committee recommends that GISS adjusts the policy memorandum where necessary.

7.2 Procedure for making official messages to political party chairpersons

The internal procedure for handling a request for information from a party chairperson has been laid down in a policy document drafted in June 2004. This policy document describes the procedure as follows.

The first step is that a request from the party chairperson for an administrative check by GISS must be lodged in writing with the minister of the Interior and Kingdom Relations. The request is then passed on to the head of GISS. He examines whether the party itself has used all possible means to investigate the misgivings and assesses whether the seriousness of the suspicion and the gravity of the threatening impairment justify an administrative check and/or (closer) investigation

by GISS. The head of the service may be advised on the matter by the legal department and the security officer of the service. If it is decided to comply with the request, the head of the service instructs the security officer to conduct an administrative check in the internal databases. The security officer, acting in consultation with the legal department, reports back the results to the head of the service, adding an opinion whether there is cause to conduct a closer investigation. Subsequently, the security officer, acting in consultation with the legal department, drafts an official message to be issued on behalf of the minister of the Interior and Kingdom Relations to the party chairperson.

The Committee has found in its investigation that in any case since 2007 the internal procedure described in the aforementioned policy documents has not been followed, although it must be noted in this context that since 2007 only one official message was issued as a result of a request for information from a party chairperson. Besides, the Committee was told by GISS that the legal department is no longer involved in issuing official messages to party chairpersons. The Committee therefore recommends that GISS adjusts either its practice or the procedure.

The Committee has not found any evidence that the procedure for making official messages issued to party chairpersons on GISS' own initiative deviates from the usual procedure for making official messages.

7.3 Findings of the Committee

7.3.1 The number of official messages in the review period

In the period from October 2005 – May 2010 GISS issued five official messages to party chairpersons. Three of these messages were issued in reaction to a request for information from the party chairperson. Two messages were issued on the initiative of GISS. All but one of the official messages related to candidate members of the Second Chamber of Parliament. For clarity's sake the Committee notes that the elections to the Second Chamber in June 2010 fell outside the review period and consequently outside the scope of this investigation.

Due to the small number of official messages issued to party chairpersons in the review period, the Committee will discuss some official messages more than once, each time addressing a different aspect of the message.

7.3.2 Legal basis

Since the Designation Order pursuant to Article 39 ISS Act 2002 does not mention political

parties or their chairpersons, only Article 36 ISS Act 202 remains as a legal basis for these official messages. This means that official messages to party chairpersons must be issued for the purpose of the performance by GISS of its tasks, in the interest of national security. The Committee holds the opinion that with the exception of one official message, all official messages issued to party chairpersons in the review period could be based on Article 36 ISS Act 2002.

In 2006 GISS, on its own initiative, issued an official message to a political party concerning a person who had been on the list of candidates for the municipal council, while the service knew that the person in question had not been elected to the council. The Committee makes the following observation. In the case of official messages to party chairpersons, the political office for which the person concerned is a candidate constitutes a link to the interests mentioned in the statutory tasks of the service. This link is absent, however, if the person in question is not or no longer a candidate for political office. In this situation the connection with the tasks of GISS will as a rule be too slight to justify providing information based on Article 36 ISS Act 2002.

The Committee therefore holds the opinion that in this case there was insufficient connection with the statutory tasks of GISS for this official message to be based on Article 36 ISS Act 2002. Consequently, this official message lacks a legal basis and was therefore issued contrary to the closed system of information provision under the ISS Act 2002.

The Committee recommends that GISS makes a record of this fact in the file of the official message (Article 43(2) ISS Act 2002). The Committee does not find it useful in this case to inform the political party in question of the fact that the official message lacks a legal basis.

7.3.3 Content

Three of the five official messages issued by GISS to party chairpersons in the review period provided substantive information. The two other official messages stated that the administrative check had not produced relevant information on the person or persons in question. The Committee has established for two of the official messages providing substantive information that the text of the message was substantiated by the underlying file. These official messages also reflected the underlying information with sufficient care and accuracy.

In the case of the third official message, information was provided orally during a conversation with the secretary of a political party.[79] Prior to this conversation a letter had been sent to the party chairperson stating that GISS had certain information, described in broad terms, concerning an unnamed person who had been on the party's list of candidates for municipal elections. The party chairperson was invited to an interview with the minister of the Interior

[79] This official message was already discussed above in a different context in section 7.3.2.

and Kingdom Relations and the head of GISS. The report of the conversation of the minister and the head of the service with the party secretary does not show exactly what was said about the person in question. It merely states that the party secretary was informed of the name of the municipal council candidate and of the concerns existing with respect to this person. As a result, the Committee cannot trace what exactly was communicated and therefore cannot assess either whether the information provided was covered by the underlying file. Nor can the Committee assess whether the information was formulated with sufficient care and accuracy.

7.3.4 Indication of reliability or source reference

In two of the aforementioned three official messages providing substantial information GISS omitted stating the reliability of the information or referring to the source of the information. In one of these messages it was stated that the information "appears from the available data" and the other message (a written confirmation of an oral message) states that GISS had established certain things in the course of performing its regular task.[80]

GISS thus failed to comply with its statutory duty under Article 12(4) ISS Act 2002.

7.3.5 The lawfulness of the underlying data processing

The policy memorandum that is applicable to the procedure for handling a request for information from a party chairperson provides that GISS may only comply with such a request if the party, after using all means at its disposal, finds that a suspicion exists or continues to exists that the (candidate) political office holder poses a risk in any way whatsoever to the integrity of the public sector. This requirement was also included in the older version of the policy memorandum dating from 1998. With this requirement, so the Committee already concluded in section 7.1, the policy memorandum adequately implements the statutory requirements applying to data processing, although the link with the statutory tasks of GISS must be watched carefully.

Three of the five official messages were issued to party chairpersons as a result of a request for information. This means that in those three cases GISS did an administrative check in its own databases. The Committee has found that there was insufficient basis for these checks. In one of these cases the request from the party chairperson was based on an anonymous report received by the candidates committee, to the effect that a candidate for parliamentary elections of this party posed a great risk to the party. In the second case there were signals from various sides about the 'fundamentalist, radical leanings of a candidate in parliamentary elections.[81] In the latter request no misgivings were mentioned at all. The request stated that there were four

[80] This official message was already discussed above in a different context in sections 7.3.2 and 7.3.3.
[81] This official message was already discussed above in a different context in section 7.3.3.

candidates for parliamentary elections with respect to whom internet searches had not produced sufficiently definite answers.

In the first case, GISS had been provided with too little concrete information to be able to conclude that it was necessary to do an administrative check in its own databases for the purposes of the proper performance by the service of its tasks, in the interest of national security. An anonymous report that a person poses a risk does not constitute sufficient concrete information, since it has not been explained to what the risk relates. In the case of the request for information about four candidates for parliamentary elections where internet searches had not produced sufficiently decisive answers, the party chairperson had likewise provided too little concrete information to constitute grounds on which GISS could base the administrative check.

In the third case: signals from various sides that a candidate in parliamentary elections has fundamentalist, radical leanings, constitute more concrete information. The Committee holds the opinion, however, that it would have been for the party first to question the person concerned and possibly also references and/or informers about the religious ideas of the person concerned. Conducting an administrative check without these steps having been taken first, while it was also not clear in advance that questioning the person concerned or persons moving in his circles would be useless or counterproductive, was not in accordance with the statutory criterion that data processing must be necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act, meaning in the case under discussion the proper performance by GISS of its statutory tasks.

7.3.6 Requirements applying to the provision of personal data

Concerning two of the five official messages to party chairpersons the information was provided to the party orally and by text message, respectively.

It was already described in section 7.3.3 how the information was provided in one of these cases. An internal memorandum shows that in this case GISS decided not to provide information in writing because the candidate for municipal elections had not been elected. The Committee points out that if GISS holds the opinion that providing information orally is less infringing than providing it in writing, this opinion is incorrect. Putting down the information in writing makes it possible for the person concerned to defend himself in court at some point in time. It is subsequently always possible to find out which information was provided. Moreover, preparing a written message encourages providing the information more carefully. The legislature has indeed excluded the possibility of providing personal data orally, except in urgent cases. This must always be followed by a written confirmation, stating what personal data have been provided. This did not happen either in the case in question. Due to the absence of a written confirmation and/or a verbatim report of the conversation with the party secretary, it is now no longer possible,

as was already observed in section 7.3.3, what was the exact content of what the head of GISS communicated about the candidate for municipal elections in question.

In 2010 the head of GISS informed a party chairperson by text message that no detrimental information had been found in the service's databases concerning the four candidates mentioned in the request.[82] In this case, too, the message was not confirmed in writing as prescribed, in spite of the fact that a report that no detrimental data exist concerning a person definitely constitutes personal data provision.

The Committee holds the opinion that by providing personal data orally and by text message, respectively, without subsequently sending written confirmation of the data provided, GISS acted contrary to Article 40(1) and (2) ISS Act 2002 in both the above cases. This also means that GISS did not comply either with the requirement that records must be kept of any personal data that has been provided (Article 42 ISS Act 2002).

7.3.7 Formal requirements pursuant to the policy memorandum

The irregularities established by the Committee in the preceding sections are also contrary to the rules laid down in the policy memorandum. Furthermore, the policy memorandum sets certain additional procedural requirements which are not laid down by law, but which in the eyes of the Committee promote careful data processing. One of these requirements is that the results of the administrative check must be notified to the party chairperson. The Committee has established, however, that in one case GISS first provided the result of an administrative check by telephone to the parliamentary party leader, and in one other case provided information to the party secretary.[83] The Committee points out to GISS that on account of the sensitive nature of the information provision and on account of the employee confidentiality aspects involved, the service should aim at exclusively communicating the results of a administrative check with the party chairperson.

Another requirement of due care that emerges from the policy memorandum is that the request from a party chairperson for an administrative check must be filed with the minister of the Interior and Kingdom Relations in writing. The request filed in 2010 concerning four candidates in parliamentary elections did not satisfy this requirement. In spite of repeated requests to the party chairperson to file a written request with the minister, this took nearly five months. Probably, this had to do with the fact that a mere few weeks after the request GISS had already communicated the results to the party chairperson. Based on the policy, the request should not have been taken up.

---

[82] This official message was already discussed in a different context in section 7.3.5.

[83] These official messages were already discussed in a different context in sections 7.3.5, 7.3.2, 7.3.3 and 7.3.6, respectively.

For reasons of due care the Committee considers it highly important that the procedure laid down in the policy memorandum is followed, which prescribes that both the request for and the provision of information must be made in writing. It recommends that henceforth GISS will not comply with a request for information until the request has been filed in accordance with the requirements.

7.3.8 Documentation

The Committee has established that it took some time for GISS to produce a list of the official messages that had been issued to party chairpersons in the review period. Furthermore, it emerged from the communications with GISS that it had been difficult for the service to put together the corresponding documents underlying each of the messages, since these documents had not been filed together with the messages.

In the opinion of the Committee the fact that it took some time for GISS to produce a list of the official messages that had been issued to party chairpersons in the review period shows a lack of management in this area. GISS should keep transparent records showing clearly what data has been provided concerning which (candidate) political office holders, especially in view of the sensitivity of this type of information provision. The Committee recommends that GISS keep more transparent records of this category of official messages.

The fact that GISS apparently had not filed the underlying documents together with the official messages shows that it did not adhere to the documentation method prescribed by the 2006 policy document.

The Committee already recommended above in section 7.2 that GISS either formalise in writing the current practice for dealing with a request for information from a party chairperson, or brings its practice in line with the policy document. The Committee finds it important that attention is paid in this context to safeguarding the thorough compilation of complete files. In the case of voluminous files the Committee considers it important that a supplementary memorandum is prepared containing references to the documents underlying the official messages.

8. Official messages to the person charged with forming a new government or the prime minister

8.1 Background and policy

In 2002 the prime minister sent a letter to the Second Chamber informing it about the procedure followed for assessing candidate ministers and vice ministers.[84] The reason for doing so was that there had recently been so many new developments in actual practice that it was considered advisable to reformalize the procedure in writing. After the formation of the government in the summer of 2002, moreover, there had been an incident involving the resignation immediately after her appointment of the vice minister for emancipation, Philomena Bijlhout, because the media had brought to light that she had been a member of the people's militia in Surinam not only before the December Murders in 1982, but still was so at the time they happened.[85] In reply to Parliamentary questions about this incident, the minister of the Interior and Kingdom Relations said he would order an investigation whether it would be advisable to widen the possibilities of screening candidates for government posts.[86] A subsequent letter to the Second Chamber made it clear that there would be no changes to the fact that political offices cannot be designated as offices involving confidentiality. Consequently, it is not possible to subject candidates for government posts to security screening. Their investigation continues to be restricted to an administrative check in the databases of GISS. GISS can only further investigate candidates for a government post if its task under (a) gives cause for doing so.

The procedure laid down in the prime minister's letter of 20 December 2002 and in the manual for government members taking up office[87] is as follows. The person charged with forming a new government holds interviews with each candidate, at which among other things they discuss matters past and present concerning the candidate which form or may form an impediment to his or her taking office. Prior to this interview, three examinations of facts are carried out. By declaring themselves as candidates they are deemed to have given their consent for these examinations. These are an administrative check in the Criminal Records Register, an administrative check for relevant data by GISS in their own databases and an administrative check by the Tax Authorities of the tax file of the person concerned. The result of the check done by GISS is provided to the person charged with forming a new government, who will inform the candidate of any relevant data and discuss them with him or her during the interview. The basic principle is, however, that it is the responsibility of the candidate to raise all relevant facts and circumstances on his or her own initiative.

---

[84] *Parliamentary Papers II* 2002/03, 28 754, no. 1.
[85] "Resignation vice minister Bijlhout (LPF)" *NRC Handelsblad*, 22 July 2002.
[86] *Parliamentary Papers II* 2001/02, appendix 1465.
[87] *Handboek voor aantredende bewindspersonen*, ministry of General Affairs, dated 25 October 2010, www.rijksoverheid.nl (consulted on 7 April 2011).

When a new government member takes up office during the government's term of office, GISS provides the result of the administrative check to the prime minister

The Committee considers the provision of information by GISS about candidates for a government office to be official messages, because the person charged with forming a new government or the prime minister, as the case may be, is authorised to decide as a result of the information that the candidate in question is not eligible for the office. This is not changed by the fact that the information is in principle provided as input for the interview to be held with the candidate. Ultimately, when the information provided by GISS concerns serious facts it can be the decisive factor.

The Committee notes that unlike administrative checks concerning (candidate) political office holders, administrative checks concerning candidates for a government post are not subject to the requirement that there must be a suspicion that the candidate in question in any way poses a risk to national security and/or other serious interests of the state or the democratic legal order. Such a threshold is indeed not necessary in the opinion of the Committee, since it may be assumed that the candidates will have been informed of the administrative check by GISS and have taken this into account in deciding to stand as candidates for a post as minister or vice minister. The situation is therefore comparable to a security screening: the position itself is sufficient cause for doing an administrative check within the scope of the statutory tasks of the service and candidates have agreed (implicitly) to the check being done.

8.2 Procedure for making official messages to the person charged with forming a new government or the prime minister

The applicable policy document of GISS shows that communications about candidates for government posts are not in actual fact conducted with the person charged with forming a new government or the prime minister, but with the secretary-general of the ministry of General Affairs. Request from the secretary-general to GISS to do administrative checks are made orally. The head of GISS notes down the names and dates of birth of the candidates and hands the list to the security officer, asking him to check the databases of the service for relevant data concerning the candidates.

The security officer discusses the result of the administrative checks with the head of the service. If the check regarding a specific candidate has produced relevant data, the security officer prepares a memorandum for the purpose of this discussion, in which he states what information has been found and how the information is characterised. The decision to provide the data to the secretary-general of the ministry of General Affairs is then taken by the head of GISS. This information is provided orally. The policy document prescribes that the head of the

service must draw up a report of the conversation with the secretary-general. An interview of the Committee with GISS has shown that in practice the report merely contains a record that the information was provided to the secretary-general on a certain date. Subsequently, a letter confirming with respect to which persons administrative checks have been done is sent to the secretary-general of the ministry of General Affairs. The letter does not, however, include the results of the checks.

The Committee holds the opinion that there are a number of points on which the policy of GISS is not in accordance with the law. Personal data must at all times be provided in writing except in cases of urgency (Article 40(1) and (2) ISS Act 2002). In urgent cases, personal data may be communicated orally, but the communication must be confirmed in writing as soon as possible (Article 40(2) ISS Act 2002). The policy of GISS does not translate these requirements into specific rules. The head of GISS orally communicates the results of the administrative checks to the secretary-general of the ministry of General Affairs. The Committee has not found any evidence that as a category these cases have such urgency as to make it impossible to prepare an official message – which the head of GISS can, if necessary, hand to the secretary-general in person. In addition, there is no written confirmation of the oral communication. The letter confirming with respect to which persons administrative checks have been done does not suffice in this respect, since it does not state the results of the checks. It is precisely the point of the written confirmation that it shows exactly what was communicated orally.

The Committee therefore recommends that GISS revise the internal procedure and makes it consistent with Article 40(1) and (2) ISS Act 2002. In this context the Committee suggests that GISS involve the legal department in making the messages, just as it is involved in the case of other types of official messages.

8.3 Findings of the Committee

For the purposes of the present investigation the Committee examined 38 files relating to the administrative checks done for the purposes of the parliamentary elections in 2007 and the subsequent government formation. In addition to these, three administrative checks were done in connection with persons taking up government posts in between elections. The administrative checks done for the purposes of the government formation in 2010 fall outside the scope of this investigation.

The Committee has found that two of the 38 administrative checks done by GISS in 2007 with respect to candidates for government posts produced data that was relevant in the context of the tasks of GISS. The three checks done in between elections did not produce any relevant data. The written confirmations of the administrative checks in 2007 sent to the secretary-general of the ministry of General Affairs in accordance with policy, mention one case in which information was

provided. Since there is no record whatsoever of this information provision, it proved impossible for the Committee to find out in which of the two likely cases information was actually provided to the secretary-general of the ministry of General Affairs. Nor is it now possible to establish the content of the information. As a result, the Committee is unable to assess whether the content of this official message satisfied the statutory requirements.

As was already observed in the preceding subsection, GISS' policy does not implement the statutory requirement that personal data must be provided in writing unless there are reasons for urgency. It is true that the applicable policy document provides that the head of the service must draw up a report of his conversation with the secretary-general. If this report should state exactly what data relating to candidates for government posts has been provided to the secretary-general, this would in the opinion of the Committee satisfy the requirement that a record must be kept of any provision of personal data (Article 42 ISS Act 2002). The Committee's investigation has shown that in recent practice the report merely contains a record that the information found was provided to the secretary-general on a certain date. As regards the provisions of information in 2007, either no record was made at all of reporting back to the secretary-general, or these records have not been filed in a retrievable way.

In the opinion of the Committee both the policy and its implementation by GISS in 2007 fall seriously short of what is required. It is noticeable that the entire procedure has an informal structure. Names and dates of birth of the candidates are stated orally to the head of GISS, he notes them down and instructs the security officer to do the administrative checks. The results of the checks are also reported back orally, without subsequent written confirmation of what personal data has been provided. As observed above, the written confirmation administrative checks does not suffice, because it does not include the result of the administrative checks. At best, the head of GISS records that he has reported back the results of the administrative checks to the secretary-general. In any case he does not record what exactly he told the secretary-general.

The Committee suspects that the political sensitivity of the provision of information concerning candidates for government posts played a role in the fact that GISS has opted for a procedure in which it does not lay down very much in writing. The Committee emphasizes, however, that the sensitivity of such provisions of information is precisely a reason for thoroughly recording all the steps in writing.

9. Official messages to other recipients

9.1 Types of official messages to other recipients

In addition to the recipients of official messages discussed in the preceding sections, GISS also issues official messages to other bodies. The most frequent categories are mentioned below.

GISS contributes to the enforcement of the freezing lists of the EU and the UN by stating whether a specific person is identical with a person included in one of these lists.[88] If the financial institutions have insufficient certainty that a person on one of the lists is identical with a person included in their files, this is known as a "possible hit". At this stage the institutions do not freeze the bank balances of the person in question yet. In such a case GISS is requested to start investigating the possible hit. This investigation is restricted to an administrative check in GISS' own databases and, if necessary, the collection of relevant data using its general powers under Article 17 Act 2002. If GISS succeeds in establishing that it is an "exact hit" or if there are special circumstances, GISS will inform the ministry of Finance and if appropriate the National Public Prosecutor of this fact by means of an official message. Since 2005 an arrangement has been in place that GISS will not issue an official message if GISS is unable to give an opinion on the matter.

Another role of GISS in the context of the freezing lists is that of proposing persons and organisations for freezing measures. For this purpose an official message is issued to the ministry of Foreign Affairs. Based on such an official message the ministry of Foreign Affairs may convene an interdepartmental consultative freezing meeting, which in addition to GISS is attended by the ministry of Finance and the National Coordinator for Counterterrorism and Security. Pursuant to Article 40 ISS Act 2002, GISS may grant inspection of the documents underlying the official message to the authorities involved in the freezing consultations. If the consultations result in a freezing measure, the minister of Foreign Affairs issues a sanctions measure. Subsequently, it may be decided whether the Netherlands will attempt to propose the person or organisation in question at the EU or the UN as a sanction target.

Furthermore, GISS may issue a message to the ministry of Foreign Affairs stating whether there is cause to maintain a freezing measure. Such official messages are issued in response to a request for information from the ministry of Foreign Affairs for the purpose of the regular review of freezing measures. At the interministerial level it has been agreed to review national sanctions measures every six months. EU or VN freezing measures can only be terminated in accordance with the applicable international procedures. Member states can request the removal of a person or organisation from the UN or EU freezing list. At the interministerial consultative meetings the persons and organisations that have been included in an international freezing list at the proposal of the Netherlands are examined every six months. When GISS has not responded to a

[88] See for a more detailed consideration of this issue the Committee's review report no. 20 on financial and economic investigations by GISS, *Parliamentary Papers II* 2008/09, 29 924, no. 35 (annex), see also www.ctivd.nl.

request for information from the ministry of Foreign Affairs within 15 working days, this means that the service sees no cause to maintain the freezing measure in question, or that there are no reasons that can be disclosed for maintaining the freezing measure.

In addition to providing information for the purpose of freezing measures, GISS occasionally provides information to the ministry of Foreign Affairs in connection with visa applications. The ministry of Foreign Affairs deals with visa applications for the purposes of *inter alia* business visits, diplomatic affairs, conferences and visits of a political nature. The same 'silent procedure' that applies to the regular reviews of freezing measures, applies to requests to GISS for information from the ministry of Foreign Affairs: GISS will issue an official message when it has found that there is cause to do so in the interest of national security.[89]

When in the course of performing its tasks GISS obtains information that is relevant to maintaining public order, this information may be provided to the relevant mayor by means of an official message. Usually, official messages to mayors relate to demonstrations planned by extremist groups or to organisations receiving municipal subsidies. Official messages for the purpose of maintaining public order may also be issued to regional chiefs of the police force.

Finally, GISS sporadically issues official messages to other persons and bodies. It may, for example, inform an employer of security-relevant information with respect to an employee or alert the customs to security-relevant information concerning travellers.

9.2 Procedure for making official messages to other recipients

A detailed discussion of the particulars of the specific procedures for making the different types of official messages described in the preceding subsection would go beyond the scope of the present investigation. In all cases the general structure of these procedures is that first the text of the message is drafted by the team concerned, then the text and the underlying file are coordinated with the legal department and subsequently the message and the file are approved by the team head, the legal department, the unit head and the service management.

9.3 Findings of the Committee

9.3.1 The number of official messages issued in the review period

In the review period a total of 42 official messages were issued to recipients in the category of other recipients, of which 23 were issued to mayors and chiefs of police, and the rest to the

[89] See also the Committee's review report no. 13 on the exchange of information between GISS and the Immigration and Naturalisation Service, *Parliamentary Papers II* 2006/07, 29 924, no. 19 (annex), section 5.1.4, See also www.ctivd.nl.

ministry of Finance, the ministry of Foreign Affairs, the chief of the National Police Force, the customs, Interpol, the Royal Netherlands Military Constabulary and a place of detention. The Committee noticed that the ministry of Finance did not receive any official messages in the final years of the review period. This may be due to a revised procedure for implementing freezing measures, according to which GISS is only required to issue an official message if information is available.[90]

9.3.2 Legal basis

As a rule, official messages to recipients other than the Public Prosecution Service must be issued under Article 36 ISS Act 2002 and therefore for the purpose of the performance by GISS of its tasks, in the interest of national security. An exception to this rule is the provision of information for an urgent and serious reason pursuant to Article 39 ISS Act 2002. The Designation Order under Article 39 ISS Act 2002 shows that under Article 39 data may be provided to ministers, mayors, the Dutch central bank Nederlandsche Bank N.V. and the financial markets authority Stichting Autoriteit Financiële Markten.

The Committee has established that the official messages which GISS issued to other recipients in the review period were rightly based on Article 36 or Article 39 ISS Act 2002.

9.3.3 Content

The official messages issued to other recipients investigated by the Committee are substantiated by the underlying information. The wording of a number of official messages calls for some observations, however.

In 2006 GISS issued two official messages to the ministry of Foreign Affairs for the purpose of freezing measures against the financial assets of two persons. The Committee made several remarks about these official messages in the secret annex to its review report on financial and economic investigations by GISS. In the present review report it will suffice to note that there is one term that is used in the official messages which in the opinion of the Committee is not sufficiently clear and concrete.

The Committee has further established that in the review period GISS issued two official messages to mayors relating to demonstrations. The messages stated that the protesters intended using everyday items that can be used as (striking) weapons. The Committee has found that in

[90] Review report of the Committee no. 20 on financial and economic investigations by GISS, *Parliamentary Papers II* 2008/09, 29 924, no. 35 (annex), section 5.7.3, see also www.ctivd.nl.

these cases GISS used this description to refer to a variety of items. It is open to question whether it was clear to the recipient what it should understand this term to mean. In this case, too, GISS should in the opinion of the Committee have chosen a more concrete wording.

9.3.4 Indication of reliability or source reference

The Committee's investigation has shown that the official messages in the category under discussion usually contain an indication of reliability or a source reference.

An exception is an official message issued in 2009 to the ministry of Foreign Affairs in connection with a visa application. In this message GISS recommended that the ministry should refuse a visa application for reasons of national security. No further explanation of these reasons was given. Moreover, the message did not state whether the information was reliable. The Committee holds the opinion that this means that GISS has not complied with its statutory obligation under Article 12(4) ISS Act 2002.

In 2010 GISS issued an official message containing a report that a certain group was planning an action. The information, qualified as reliable, originated mainly from a human source. However, the Committee has not found a reliability memorandum regarding this human source in the file. This is not in keeping with the policy at GISS. Due to the absence of an assessment of the reliability of the information it is impossible to verify on the basis of the underlying file whether the indication of reliability in the message is correct.

9.3.5 Documentation

The Committee has established that the files of the official messages in the category under consideration were usually complete and transparent. There is one file on which the Committee wishes to make a comment.

In 2009 GISS informed the customs of certain information relating to the luggage of a passenger. This enabled the customs to search the luggage. It is true that certain indications emerged from the file examined by the Committee, but these were insufficient to substantiate the official message. GISS told the Committee that the official message was actually based on information from a human source. At the time of issuing the official message this had not yet been laid down in writing in an intelligence report. Subsequently, the intelligence report was drawn up, but not added to the documents underlying the official message. The supplementary memorandum to the official message does not mention this information either. The Committee considers this procedure to be negligent, since the official message was based predominantly on the information from the human source.

10. Conclusions and recommendations

Official messages issued to the Public Prosecution Service

10.1 In the opinion of the Committee all but one of the official messages issued by GISS to the Public Prosecution Service are rightly based on Article 38 ISS Act 2002. The Committee holds the opinion that in one case GISS wrongly opted to provide data to the Public Prosecution Service.There were no indications that the person concerned had committed any offences. Given the office held by the person concerned, GISS could in this case have opted to issue an official message to his employer pursuant to Article 36 ISS Act 2002. (section 4.4.2)

10.2 In the course of its investigation the Committee came across two cases in which GISS provided data to the Public Prosecution Service which GISS knew to be already in the possession of the Public Prosecution Service. In both cases the Committee found that by issuing the messages GISS sought to influence the follow-up steps to be taken by the Public Prosecution Service.
However, issuing an official message containing information that is already known to the recipient is not the appropriate procedure for achieving this. When GISS has specific wishes or advice concerning the steps which the Public Prosecution Service should undertake in a certain investigation, it can consult with the Service – through the National Public Prosecutor. The Committee holds the opinion that in such cases the provision of information is not necessary for the purpose of the investigation and prosecution of offences since the Public Prosecution Service already has the information. (section 4.4.3)

10.3 The Committee has found that the content of the official messages issued by GISS to the Public Prosecution Service in the review period is substantiated by the underlying files. In a number of cases, however, GISS should have exercised greater care in formulating the message. (section 4.4.4)

10.4 The policy of GISS regarding the provision of detailed information to the Public Prosecution Service is that there must be urgent reasons to provide such information in the context of the tasks of GISS. The Committee holds the opinion that in this respect GISS exercises greater restraint than was envisaged by the legislature. It points out that the interests of investigation and prosecution must carry great weight.Whenever it is possible for GISS to reveal (detailed) information, it should only decide not to do so if providing the information would harm the interests of the service. (section 4.4.5)

10.5 The Committee has established that as a rule GISS consistently includes an indication of reliability in the official messages to the Public Prosecution Service. Two related official messages issued in 2006 and an official message issued in 2008 are an exception to this rule. (section 4.4.6)

10.6 In its investigation the Committee came across some examples of official messages to the Public Prosecution Service in which information from one single human source formed the basis of part of the message. The Committee holds the opinion that in these cases GISS exercised due care in establishing the reliability of the information. (section 4.4.6)

10.7 The Committee points out that because GISS does not include exculpatory information which it has not found reliable in the file underlying official messages, such information will not be found by the National Public Prosecutor who checks the content of the official messages issued to the Public Prosecution Service. It will also not be possible for the Committee to review the assessment in retrospect. As a result, the assessments made by GISS regarding the reliability of this information are unverifiable. In the opinion of the Committee it is advisable to arrange the files underlying official messages in such a way that they show whether exculpatory information is available and how GISS assessed the reliability of this information. (section 4.4.7)

10.8 In connection with two official messages to the Public Prosecution Service the Committee saw reason to investigate the underlying use of special powers. In both cases the special powers were used in an intelligence investigation conducted in parallel with a criminal investigation. The Committee holds the opinion that in view of the relevant facts and circumstances the powers were used lawfully in these two cases. (section 4.4.8)

10.9 The Committee has established that generally the official messages that have been issued to the Public Prosecution Service are supported by thorough documentation. In one case GISS added an earlier official message on the relevant persons to the file of a subsequent official message to substantiate certain information. It is the opinion of the Committee that in such cases GISS should add (copies of) the relevant documents from the file of the earlier official message to the new file. (section 4.4.9)

Official messages issued to the Immigration and Naturalisation Services (INS)

10.10 The Committee recommends that GISS correctly sets out in the applicable policy document the legal basis for doing an administrative check at the request of INS as well as the related statutory requirements. (section 5.2)

10.11 The Committee has found that in practice the requests from INS always lead to an administrative check by the front office of GISS, which is where these requests are received. The front office conducts the check to examine whether the request can be passed on to a specific team, which will then further deal with the request. Since this first check is a form of data processing, the Committee holds that GISS must first assess the request against the requirement of necessity before it tries to link it to a team. The assessment can be made using the form supplied by INS which among other things states the reason for the request for information. (section 5.2)

10.12 The Committee recommends that GISS, in consultation with INS, formalises the current practice of exchanging information between GISS and INS in a written procedure as soon as possible. (section 5.2)

10.13 The legal basis for providing data to INS for the purpose of the performance by GISS of its tasks, in the interest of national security, is Article 36 ISS Act 2002. The Committee holds the opinion that the official messages issued by GISS to INS in the review period could be based on Article 36 ISS Act. (section 5.3.2)

10.14 The Committee's investigation has shown that all but one of the official messages issued by GISS to INS in the review period are substantiated by the underlying information. The messages are, moreover, carefully formulated, so that they are in line with the underlying information. (section 5.3.3)

10.15 The Committee has found that GISS does not use a consistent definition of the term "threat to national security". GISS considers on a case-by-case basis whether this conclusion applies. Each of the official messages examined by the Committee concerned activities having such a clear connection with national security, that in the opinion of the Committee they justified the conclusion. (section 5.3.3)

10.16 The Committee draws the attention of GISS to the fact that it is important for the alien about whom the service issues an official message that he receives sufficient factual information at the earliest possible stage. When the protection of sources, the secrecy of the current level of knowledge and/or the operational methods of the service or the third party rule do not constitute a reason to withhold concrete details, then in the opinion of the Committee GISS should therefore seek to provide INS with as much concrete information as possible. (section 5.3.3)

10.17 The Committee has established that the official messages issued by GISS to INS contain an indication of reliability. In one case the Committee has established that with respect to part of the information provided the indication of reliability in the official message was not substantiated by the underlying file. In this respect the official message is unlawful.

The Committee therefore recommends that GISS records this in the relevant file pursuant to Article 43(2) ISS Act 2002 and informs INS that the reliability of the sources on which the first part of the official message is based has not been established. (section 5.3.4)

10.18 The Committee has found that when the Regional Intelligence Services provide information to GISS pursuant to Article 60 ISS Act 2002, they often omit including an indication of the reliability of the information. Where they have included a reliability indication, the indication is often ambiguous, since different coding systems and qualifications are used. This way of processing information is contrary to Article 12(4) ISS Act 2002. The Committee recommends introducing clear and unambiguous indications of the reliability of the information which the Regional Intelligence Services pass on to GISS. (section 5.3.4)

Official messages issued to the ministry of Economic Affairs, Agriculture and Innovation (EAA&I)

10.19 The Committee has found that GISS has started consultations with the ministry of EAA&I about laying down the arrangements in the field of information provision in a covenant. The Committee endorses the usefulness of such a covenant. (section 6.1)

10.20 Taking into consideration that the information provided to the ministry of EAA&I in connection with export applications will by definition reveal the current level of knowledge of GISS regarding companies in countries of concern, the Committee holds the opinion that the classification of these official messages is justified. It holds the opinion that in those cases the general interest of national security must carry greater weight than the individual interest of the exporter in learning the content of the official message. (section 6.3.2)

10.21 The Committee recommends that GISS, in consultation with the ministry of EAA&I, seeks ways to promote that the ministry can make its decisions on the basis of an adequate information position. One possibility is that of granting the ministry of EAA&I, where necessary, inspection of the documents underlying the official messages. (section 6.3.2)

10.22 The Committee expects that the use of a matrix of standard phrases will promote consistency in the official messages issued to the ministry of EAA&I. The formalisation of the different standard phrases has produced clarity. The Committee considers it important, however, that GISS assesses for each official message separately whether the chosen standard phrase adequately represents the underlying information and whether it is possible to provide more factual information than the standard phrase without affecting the agreements made with foreign counterpart services and the secrecy of sources, current level of knowledge and/or operating procedure of the service. (section 6.3.3.1)

10.23 It has emerged from the Committee's investigation that GISS, which formerly did not consider the messages to the ministry of EAA&I to be official messages, did not always set very high requirements on the substantiation of the messages. It is the opinion of the Committee that in two cases the official message is not substantiated by the underlying information. These official messages were not made with proper and due care and are therefore unlawful. The Committee recommends that GISS, pursuant to Article 43(2) ISS Act 2002, makes a record of this fact in the relevant file and informs the ministry of EAA&I, with a view to possible future applications for export licences for the benefit of the end-users concerned, that the two aforementioned official messages are not substantiated by the information in the possession of the service. (section 6.3.3.2)

10.24 The Committee has found that the official messages issued by GISS to the ministry of EAA&I in the early part of the review period usually do not contain an indication of reliability. This means that in this period GISS did not comply with the statutory requirement of Article 12(4) ISS Act 2002. From early in 2009 GISS has included an indication of reliability in the official messages. (section 6.3.5)

10.25 Information from human sources is seldom used in official messages to the ministry of EAA&I. The Committee has established that the Counter Proliferation Unit, unlike the other departments of GISS, does not prepare reliability memorandums for the underlying file in such cases. This is not in keeping with general policy at GISS in this area. The Committee recommends that the Counter Proliferation Unit adjusts its procedure. (section 6.3.5)

10.26 The Committee holds the opinion that the data provided by GISS to the ministry of EAA&I is not personal data. Nevertheless, the Committee finds that where data is provided which may result in measures being taken against persons or companies, the same proper and due care must be exercised as in the case of the provision of personal data. Because of the potential consequences of the provision of such data the Committee considers it appropriate that the special requirements of proper and due care mentioned in Articles 40, 41 and 42 IIS Act 2002 apply to the official messages to the ministry of EAA&I. (section 6.3.6)

10.27 The Committee holds the opinion that the policy of the Counter Proliferation Unit satisfies the requirements of due care to a sufficient degree. The Committee has found that the Counter Proliferation Unit observes the policy, with a few exceptions. In one case information was provided which dated back twelve years. The Committee points out that if this information was deemed so incriminating that it could not be disregarded, the official message should in any case have mentioned the degree of reliability and the age of this information, which did not happen in this case. The Committee considers this to be negligent. The Committee has established that in two cases oral information was communicated from the Counter Proliferation Unit to the ministry of EAA&K that

'something' had been found.The exact content of these communications can no longer be retrieved.The Committee holds the opinion that for reasons of due care the service must refrain from making such remarks in its contacts with the ministry of EAA&I. (section 6.3.6)

10.28 Sometimes, only the relevant pages of large documents are included in the files of the official messages issued to the ministry of EAA&I, or it is otherwise impossible to retrieve from which document the pages are taken.The Committee recommends that in such cases the Counter Proliferation Unit indicates what is the document concerned and mentions its date. (section 6.3.7)

Official messages issued to political party chairpersons

10.29 When a party chairperson has addressed a request to GISS for information concerning a (candidate) political office holder, the Committee considers it appropriate, for the purposes of assessing the necessity which includes the element of subsidiarity, that the party chairperson states which means the party has already used to investigate the misgivings against the (candidate) policy office holder.The Committee recommends that GISS include a requirement in the policy memorandum applicable to this procedure and furnished to the party chairpersons, that party chairpersons either state the means which the party has already used to investigate the misgivings, or state reasons why the party has not itself used any means. (section 7.1)

10.30 In view of the special nature of the procedure for providing information to party chairpersons, it is the opinion of the Committee that it is important that the applicable policy memorandum provides a clear and complete framework for both the party chairpersons, to whom the memorandum is furnished, and GISS. This requires among other things that the memorandum correctly sets out the legal basis pursuant to which GISS may do administrative checks in its own databases.The Committee recommends that GISS adjusts the policy memorandum where necessary. (section 7.1)

10.31 The Committee has found in its investigation that the internal procedure followed in practice for dealing with a request for information from a party chairperson differs from the procedure described in the applicable policy document. The Committee therefore recommends that GISS adjusts either its practice or the procedure. (section 7.2)

10.32 The legal basis for providing information to the political party chairpersons is Article 36 ISS Act 202.This means that these official messages must be issued for the purpose of the performance by GISS of its tasks, in the interest of national security.The Committee holds the opinion that with the exception of one official message, all official messages issued

to party chairpersons in the review period could be based on Article 36 ISS Act 2002. The Committee holds the opinion that in one case there was insufficient connection with the statutory tasks of GISS for this official message to be based on Article 36 ISS Act 2002. Consequently, this official message lacked a legal basis and was therefore issued contrary to the closed system of information provision under the ISS Act 2002. The Committee recommends that GISS makes a record of this fact in the file of the official message (Article 43(2) ISS Act 2002). It does not find it useful in this case to inform the political party in question of the fact that the official message lacked a legal basis. (section 7.3.2)

10.33 Three of the five official messages issued by GISS to party chairpersons in the review period provided substantive information. In two cases the Committee has been able to establish that the text of the message was substantiated by the underlying file. These messages also represented the underlying information with sufficient care and accuracy. In the third case, information was provided orally. The report of the conversation does not show exactly what was said about the person in question. As a result, the Committee cannot trace what exactly was communicated and therefore cannot assess either whether the information provided was covered by the underlying file. Nor can it be assessed whether the information was formulated with sufficient care and accuracy. (section 7.3.3)

10.34 In two of the three official messages providing substantial information to party chairpersons GISS omitted stating the reliability of the information or referring to the source of the information. GISS thus failed to comply with its statutory obligation under Article 12(4) ISS Act 2002. (section 7.3.4)

10.35 The Committee has found that the basis for the administrative checks done in response to requests for information from a party chairperson was insufficient in three of these cases. In two cases GISS had been provided with too little concrete information to be able to conclude that it was necessary to do an administrative check in its own databases for the purposes of the proper performance by the service of its tasks, in the interest of national security. In one case the Committee holds the opinion that it would have been for the party to first investigate the misgivings that had arisen itself. (section 7.3.5)

10.36 The Committee holds the opinion that in two cases in which GISS provided personal data orally and by text message, respectively, without subsequently sending written confirmation of the data provided, GISS thus acted contrary to Article 40(1) and (2) ISS Act 2002. This also means that GISS did not comply either with the requirement that records must be kept of any personal data that have been provided (Article 42 ISS Act 2002). (section 7.3.6)

10.37 For reasons of due care the Committee considers it highly important that the procedure laid down in the policy memorandum is followed, which prescribes that both the request

for and the provision of information must be made in writing. It recommends that henceforth GISS will not comply with a request for information until the request has been filed in accordance with the requirements. (section 7.3.7)

10.38 In the opinion of the Committee the fact that it took some time to produce a list of the official messages that had been issued to party chairpersons in the review period shows a lack of management in this area. GISS should keep transparent records showing clearly what data has been provided concerning which (candidate) political office holders, especially in view of the sensitivity of this type of information provision. The Committee recommends that GISS keep more transparent records of this category of official messages. (section 7.3.8)

Official messages to the person charged with forming a government or the prime minister

10.39 The Committee holds the opinion that the internal procedure for making official messages to the person charged with forming a government or the prime minister is not in accordance with the statutory requirements applying to the external provision of personal data. The Committee therefore recommends that GISS revise the internal procedure and make it consistent with Article 40(1) and (2) ISS Act 2002. In this context the Committee suggests that GISS involve the legal department in making the messages, just as it is involved in the case of other types of official messages. (section 8.2)

10.40 The Committee has found that two of the 38 administrative checks done by GISS in 2007 with respect to candidates for government posts produced data that was relevant in the context of the tasks of GISS. The written confirmation of the administrative checks sent to the secretary-general of the ministry of General Affairs, however, mentions one case of information provision. Since there is no record whatsoever of this information provision, it proved impossible for the Committee to find out in which of the two likely cases information was actually provided to the secretary-general of the ministry of General Affairs. It is also no longer possible to establish the content of the information. As a result, the Committee is unable to assess whether the content of this official message satisfied the statutory requirements. (section 8.3)

Official messages to other recipients

10.41 The Committee has established that the official messages which GISS issued to other recipients in the review period were rightly based on Article 36 or Article 39 ISS Act 2002. (section 9.3.2)

10.42 The official messages issued to other recipients investigated by the Committee are substantiated by the underlying information. The Committee holds the opinion that in three cases GISS should have chosen more clear and concrete wordings. (section 9.3.3)

10.43 The Committee's investigation has shown that the official messages issued to other recipients in the review period usually contain an indication of reliability or a source reference. One exception is an official message issued in 2009 to the ministry of Foreign Affairs. (section 9.3.4)

10.44 The Committee has established that the files of the official messages in this category were usually complete and transparent. With respect to one file the Committee observes that the information constituting the main basis of the message had not been included in the underlying file nor in the supplementary memorandum. The Committee considers this to be negligent. (section 9.3.5)

Thus adopted at the meeting of the Committee held on 28 September 2011.