COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN

REVIEW REPORT

on

THE USE OF SIGINT
BY DISS

CTIVD NO. 28

23 August 2011

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 28

REVIEW REPORT

On the use of Sigint by DISS

Table of Contents

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 28

SUMMARY

Of the review report 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 COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 28

REVIEW REPORT

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.

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

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

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.

3.1.2 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.

[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.

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:

> "[…] 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.

---

[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.
[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*).

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 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]

---

[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*).
[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.

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 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.

---

[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.
[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 April 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.

> "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 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 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

---

[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.
[31] ECtHR 6 September 1978 (*Klass a.o.* v. *Germany*) §§ 46 and 48-50.

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.

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.

---

[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.

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 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.

---

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

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 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

[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.

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 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

---

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

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

[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.

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]

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

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

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 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

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

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 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]

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.

---

[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(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 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]

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

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.

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

[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.
[63] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 30.

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.

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]

---

[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.
[67] *Parliamentary Papers II*, 2000/01, 25 877, no. 59, p. 12.

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 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

[68] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 22.
[69] Idem, p. 23.
[70] *Parliamentary Papers II* 2000/01, 25 877, no. 14, pp. 36-37.
[71] Idem, p. 35.
[72] Idem.

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 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.

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

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.

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 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

---

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

security task. This is due 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]

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,

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

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 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.

[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.

[83] Examples are the right of nondisclosure or diplomatic immunity.

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:

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

[84] Also abbreviated as *RFI*.

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 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

[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.

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 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.

---

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

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.

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

[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.

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]

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.

---

[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.

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.

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

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.[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) 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).

---

[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.

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. 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.

[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.

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

[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.

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 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.

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

[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.

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

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

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.

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.

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.

---

[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.

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.

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]

---

[101] *Parliamentary Papers II* 1997/98, 25 877, no. 3, pp. 44-45.
[102] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 33.

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.

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

---

[103] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 45.

[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.

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 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

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

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 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

---

[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.

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).

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 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

[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.

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

[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.

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 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

---

[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.
[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.

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 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.

[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.

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 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

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.