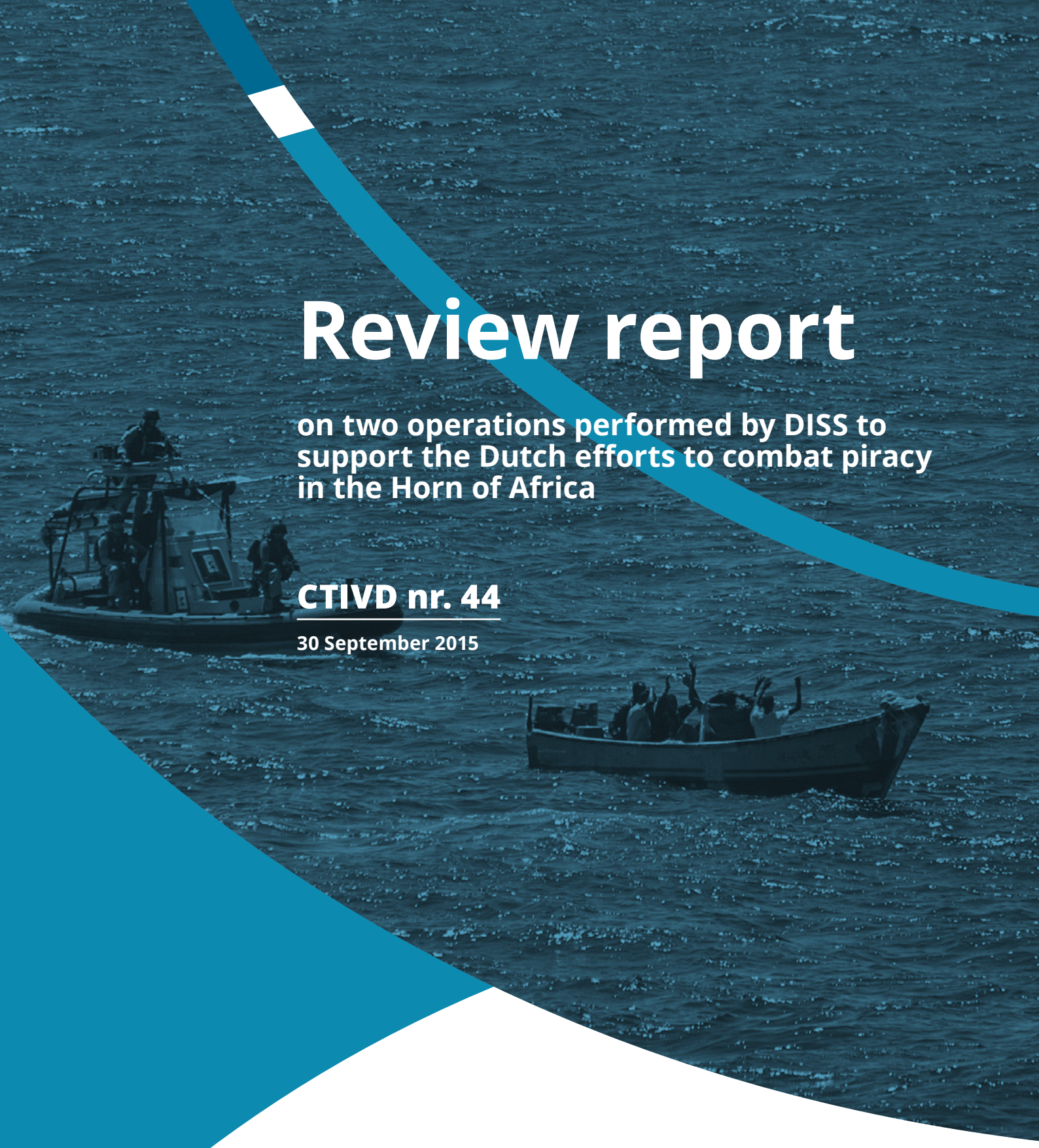

Review report

on two operations performed by DISS to support the Dutch efforts to combat piracy in the Horn of Africa

CTIVD nr. 44

30 September 2015

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence and
Security Services

CTIVD no. 44

REVIEW REPORT

On two operations performed by DISS to support the Dutch efforts
to combat piracy in the Horn of Africa

Inhoudsopgave

CTIVD no. 44

SUMMARY

**Of the review report on two operations performed by DISS
to support the Dutch efforts to combat piracy in the Horn of Africa**

Reasons for the investigation

Since 2008 Dutch military units have been taking part in anti-piracy missions in the waters around Somalia. During the deployment of HNLMS Rotterdam in 2012 and HNLMS Johan de Witt in 2013 DISS (Defence Intelligence and Security Service) used the power to examine content of telecommunications obtained by untargeted interception (the power to select sigint) in the area of operation to support these missions. DISS did so while derogating from the procedures prescribed by law. The service had obtained permission to examine the content of all telecommunications acquired by untargeted interception in the area of operation. Pursuant to the Intelligence and Security Services Act 2002 (ISS Act 2002), this must normally be done using selection criteria defined by law for which the service has obtained the prior permission of the Minister of Defence. This was reason for the Committee to investigate the procedure actually followed by DISS. The question the Committee will answer in this report is whether the manner in which DISS exercised this power in the area of operation was lawful.

Scope for derogation from the statutory procedure in the area of operation

The general rule is that DISS must stay within the legal parameters of the ISS Act 2002, also when it is active in an area of operation abroad. In principle, DISS is only allowed to derogate from procedures prescribed in the ISS Act 2002 if 1) a mandate under international law provides a legal basis for doing so, and 2) serious reasons are present.

Mandate under public international law

The Committee has found that the mandate under public international law for the anti-piracy missions (the UN Convention on the Law of the Sea, supplemented with resolutions of the UN Security Council) provided a legal basis for *inter alia* the deployment of intelligence means. It also left DISS scope to derogate from procedures from the ISS Act 2002 for serious reasons. The UN resolutions show *inter alia* that the UN Security Council has in principle authorised states and regional organisations to take all necessary measures appropriate to combat piracy in Somalia (both on land and in the territorial waters) within the framework of international law.

Serious reasons

The Committee holds the opinion that in the cases it examined serious reasons existed for derogating from procedures of the ISS Act 2002. DISS was expected to provide the anti-piracy missions with timely and effective support, among other things, so that threats to the mission and to the personnel involved (threat to the force) could be eliminated or limited. The safety of Dutch soldiers was at stake. In the area of operation persons and groups were present that posed a real threat, making it essential that DISS would be able to take swift action. DISS took every possible measure to protect privacy. The Committee has established that during the anti-piracy missions DISS only derogated from the statutory procedures to the extent necessary, of which DISS kept adequate and sufficient records.

The Committee therefore concludes that DISS exercised its power of selection lawfully.

Review Committee
on the Intelligence and
Security Services

CTIVD nr. 44

REVIEW REPORT

On two operations performed by DISS to support the Dutch efforts to combat piracy in the Horn of Africa

1. Introduction

1.1 Reasons for the investigation

Since 2008 Dutch military units have been taking part in anti-piracy missions in the waters around Somalia. These missions, also known as operations Ocean Shield and Atalanta, take place in an international context (NATO and EU). Since 2008 the Netherlands has contributed to these two anti-piracy missions, mainly with Royal Netherlands Navy units. From August through December 2012, for instance, it deployed HNLMS Rotterdam to Ocean Shield. HNLMS Johan de Witt was deployed to Atalanta from August through December 2013. During these periods the Netherlands also provided the Force Commander and part of the staff for these operations.[1]

DISS has supported these anti-piracy missions by providing intelligence support. It has done so both from the Netherlands and from abroad, for instance in the area of operation. The support can take the form of providing political and strategic intelligence on the situation in the country where the armed forces are deployed. It includes, for instance, providing insight into different power factors and interests that play a role in national politics. DISS's support can also consist of providing tactical intelligence to units of the armed forces. This intelligence can be used in preparing and executing specific military actions.

While participating in the anti-piracy missions of HNLMS Rotterdam in 2012 and HNLMS Johan de Witt in 2013, DISS exercised the power to select sigint.[2] DISS used this power to examine the content of telecommunications obtained by untargeted interception. In doing so DISS deviated from the usual legal framework. This was reason for the Committee to investigate the exercise of the power.

---

[1] The tactical command of the anti-piracy missions is entrusted to the Force Commander, supported by his staff. The Force Commander takes command of all military units (regardless of nationality) available to him for executing the operation. The Force Commander's nationality varies; from August through December 2013 the Netherlands provided the Force Commander for Atalanta. The Netherlands provided the Force Commander for Ocean Shield from June 2012 through December 2012.

[2] Sigint stands for *signals intelligence*. See the definitions for a more detailed explanation.

1.2 Question to be answered by the investigation

The Committee investigated how the power to select sigint was exercised in support of the two anti-piracy missions. The question which the Committee will answer in this report is whether DISS exercised the power to select sigint in a lawful manner.

1.3 Structure of the report

The review report has the following structure. Chapter 2 explains the set-up and method of the investigation. The Committee describes how it shaped the investigation and which investigative activities it carried out. Chapter 3 describes the legal framework for DISS's operations abroad in support of military missions. Chapter 4 clarifies the normal procedure followed by DISS for the selection of sigint. In chapter 5 the Committee describes the sigint activities carried out by DISS in the context of the anti-piracy missions. In chapter 6 the Committee presents its opinion on the lawfulness of the activities of DISS it has described. Chapter 7 sets out the main conclusions of the Committee, followed by a list of definitions.

2. Investigation set-up and method

DISS supported the anti-piracy missions *Ocean Shield* and *Atalanta* abroad by using its power of selection. The Committee investigated how it exercised the power. In this chapter it describes how it carried out the investigation.
The Committee examined what is the legal framework for operations of DISS abroad in support of military missions. For this purpose the Committee examined the files, which included analysing the applicable national and international regulations, Parliamentary Papers and the internal documentation at DISS on the subject.

Next, the Committee investigated how DISS carried out its task of supporting the anti-piracy missions. The Committee focused on the use made by DISS units of the power of selection in the area of operation during the deployment of the HNLMS Rotterdam in 2012 and the HNLMS Johan de Witt in 2013 in the context of the anti-piracy missions. Prior written applications for permission to exercise the power of selection were submitted to the Minister. These applications described why and how DISS planned to use the power of selection. The Committee examined the written applications. Their content was in fact the reason for conducting the present investigation.

In addition to examining the written applications, the Committee carried out an independent investigation in the information systems of DISS. It examined the relevant documents relating to the two anti-piracy missions. Where necessary, it requested DISS to provide certain documents. These concerned among other things the results of the exercise of the power of selection (the intelligence information that DISS had obtained thereby) and the evaluations carried out after the operations. In the opinion of the Committee it has thus been able to gain a full picture of the subject matter.

The exercise of other powers and the cooperation (e.g. exchange of data) of DISS with foreign services in the context of the anti-piracy missions fell outside the scope of this investigation.

On several occasions the Committee conducted exploratory interviews with employees of DISS. They were employees working at the legal department of DISS and employees who had been directly involved in the activities in the context of the anti-piracy missions investigated by the Committee. Additionally, the Committee met with external experts to discuss the legal framework for activities carried out abroad by DISS in support of military missions.

3. Legal framework for operations of DISS abroad

3.1 Introduction

DISS supports the armed forces in areas of operation abroad. In this chapter the Committee explores the legal framework which DISS is bound to respect when engaging in such activities. First of all, it describes the statutory task of DISS and the applicability of the ISS Act 2002 in foreign countries. Next, the Committee addresses the situation that the provisions of the ISS Act 2002 cannot be fully complied with abroad. And it considers the safeguards that need to be in place if, in those cases, it is necessary to derogate from the procedures prescribed in the ISS Act 2002.

3.2 Statutory task of DISS

The tasks and the statutory powers and obligations of DISS are set out in de ISS Act 2002. DISS performs its tasks on the basis of this Act and must in principle stay within the parameters laid down in this Act. The Minister of Defence bears political responsibility for the activities of DISS, whose tasks are listed in article 7(2) ISS Act 2002. Not all the tasks mentioned in article 7 are relevant to the subject of this report. The following tasks are relevant:

a. Conducting investigations:
   1. into the potential and the armed forces of other powers, in order to achieve a balanced composition and an effective use of our armed forces;
   2. of factors that are or may be of influence on maintaining and promoting the international legal system, in so far as the armed forces are, or are expected to become, involved (...)

c. conducting investigations necessary for taking measures:
   1. to prevent activities aimed at damaging the security or readiness of the armed forces;
   2. to promote a proper organisation of the mobilisation and concentration of the armed forces;
   3. for a smooth preparation and deployment of the armed forces as referred to in part a, under 2 (...).

e. Conducting investigations concerning other countries regarding matters with military relevance that have been designated by the Prime Minister (...);

When performing the aforementioned tasks (also referred to as the a-, c- and e-task, respectively) DISS may use special powers (article 18 ISS Act 2002), subject to certain conditions. These powers usually infringe fundamental rights, for instance the right to privacy. Examples are the power to conduct surveillance (article 20 ISS Act 2002) or the power to select sigint (article 27 ISS Act 2002).

3.3 Operations of DISS abroad

Given its tasks, it will come as no surprise that DISS performs its tasks mainly outside the Netherlands. Both the a-task and the c-task focus explicitly on supporting the armed forces. The armed forces are to a considerable extent deployed outside the Netherlands, for instance in the context of international peace-keeping missions. Hence, if DISS wants to provide effective intelligence support to the armed forces, it will also have to conduct activities abroad. Indeed, the intelligence need of the armed forces can usually not be met from the Netherlands alone.

The ISS Act 2002 does not contain an explicit provision stating that this Act is also applicable outside the Netherlands (no extraterritorial effect). This does not mean, however, that DISS is not permitted to deploy activities abroad. The fact that it may do so ensues from the tasks of DISS. Nor does it mean that DISS does not have to abide by the rules when conducting activities abroad because the ISS Act 2002 does not have extraterritorial effect. Legislative history shows that it was the legislator's intention that DISS, when exercising special powers abroad, would have to operate within the limits that would apply in the Netherlands, too.[3] That is why DISS is *de facto* bound by the ISS Act 2002 when acting abroad, even though formally this Act is not applicable there. In other words: DISS must apply the ISS Act 2002 by analogy when it operates abroad.[4]

In addition to the ISS Act 2002, DISS must also take into account the possible effect of the European Convention on Human Rights in foreign areas of operation. The fact is that the European Court of Human Rights (ECtHR) has ruled that in some cases the scope of application of this convention extends to foreign areas in which the Dutch armed forces operate.[5]

3.4 Mandate under public international law

According to the government, any operation abroad of the armed forces always requires an adequate mandate under international law.[6] This means that the deployment of Dutch military units must in any case take place in accordance with international law.

A basis for such an international mandate is found in a resolution of the United Nations Security Council. Under international law the Security Council has the far-reaching power to adopt resolutions authorizing (for instance) armed intervention on the territory of a state in order to achieve a predefined objective in the context of international peace and security. In such resolutions the Security Council often includes the expression 'using all necessary means' to attain the objectives set in that resolution. All necessary means is a broad definition and may even entail the use of lethal force. A resolution of the Security Council must be regarded as a decision which the Member States of the United Nations must accept and carry out.[7] Often, however, such a resolution is phrased in general terms and usually it does not lay down specific frameworks prescribing, for instance, how intelligence may be acquired.

---

3 Parliamentary Papers II 2000/01, 25 877, no. 59.

4 See review report CTIVD no. 28 on the use of Sigint by DISS, Parliamentary papers II 2011/12, 29 924, no. 74 (attached), available on www.ctivd.nl), p. 31-33, and Evaluation of the Intelligence and Security Services Act 2002: Towards a new balance between powers and safeguards Parliamentary Papers II 2013/14, 33 820, no. 1, appendix), p. 41.

5 See for a recent example ECtHR 20 November 2014, 47708/08 (Jaloud/Netherlands).

6 See Parliamentary Papers II 2006/07, 29 521, no. 41.

7 See article 24 and chapter VII of the UN Charter.

Subsequently, however, states or international organizations will elaborate and specify the powers under the international law mandate in e.g. operation plans, guidelines, instructions or other documents of an operational nature (for instance the so-called rules of engagement), in which they lay down specific rules on the use of military means in an area of operation. As a rule, these documents are not made public. Furthermore, resolutions often refer to legal frameworks in general, such as international humanitarian law and international human rights.

In an earlier report, the Committee devoted attention to the role of an international mandate in operations of DISS abroad.[8] In 2006, moreover, the Ministry of Defence established a research group to consider inter alia this subject.[9] Furthermore, in his reaction to the Committee's review report no. 28 on sigint and (also speaking on behalf of the minister of the Interior and Kingdom Relations) in other Parliamentary Papers, the Minister of Defence explained his views on the role of mandates under public international law when DISS operates abroad.[10] Finally, the ISS Act 2002 Evaluation Committee (known as the Committee Dessens) also touched upon the subject.[11] In view of its relevance to this report, the Committee sees reason to clarify its position on the matter.

3.5 Concurrence of the ISS Act 2002 and an international mandate

When providing support to the armed forces in an area of operation, DISS may have to take account of both the ISS Act 2002 (by analogous application) and an international mandate governing the deployment of resources in an area of operation. In those situations factual concurrence of legal frameworks may arise. How should DISS deal with that?

The Committee holds the opinion that an international mandate can provide a legal basis for DISS to deploy intelligence resources in an area of operation in support of the armed forces. Such deployment can, for instance, fall within the scope of 'all necessary means'. Usually, however, an international mandate is broader and more general than the ISS Act 2002. Often, the mandate contains no specific or detailed safeguards with respect to the deployment of intelligence means comparable to those included in the ISS Act 2002. In view of the legal history and the position of the Minister of Defence on this issue, DISS will in principle have to apply the ISS Act 2002 by analogy within the framework of the international mandate.

There are situations, however, in which the strict application of the ISS Act 2002 by DISS in the area of operation would lead to undesirable consequences. In such situations the presence of an international mandate makes it possible for DISS to derogate (to the extent necessary), from the procedures prescribed in the ISS Act 2002 without this being unlawful. The Committee will discuss this in further detail in the next section.

---

[8] See CTIVD review report no. 15 on the investigation of the conduct of DISS personnel when questioning detainees in Iraq, *Parliamentary papers II* 2006/07, 23 432, no. 228 (appendix), available on www.ctivd.nl. Furthermore, in 2007 the Committee organised an afternoon study meeting at which the subject was discussed.

[9] See the report *Defence Intelligence and Security: Quality, Capacity and Cooperation*, Defence Intelligence and Security Research Group2006.

[10] See for instance *Parliamentary Papers II* 2000/01, 25 877, no. 58, p. 42, *Parliamentary Papers II* 2011/12, 29 924, no. 74, Proceedings I 2014/15, 1-11-8; *Parliamentary Papers II* 2014/15, 33 321, no. 5.

[11] See Evaluation of the Law on the Intelligence and Security Services 2002: Towards a new balance between powers and guarantees (*Parliamentary Papers II* 2013/14, 33 820, no. 1, appendix), p.41.

3.6 Exceptions to the application by analogy of the ISS Act 2002

Operations of the armed forces in foreign areas of operation are inherently different from their operations in the Netherlands. They often find themselves in a complex and dynamic environment in which they must be able to act quickly and decisively to achieve the mission's objective and to identify and effectively combat potential threats at an early stage.

For this reason the Committee has already stated before, in its review report on sigint, that it could imagine the existence of serious reasons because of which DISS could not reasonably be expected to act in (full) compliance with the ISS Act 2002 when operating abroad.[12] It was suggested by, or on behalf of, the minister of Defence that on account of the operational conditions in an area of operation DISS should, when operating abroad, comply with the safeguards of the ISS Act 2002 to *the extent possible*.[13] This position of the minister implies that the ISS Act 2002 will be applied to the extent possible, but that there may be serious reasons making it necessary to derogate from the procedures prescribed by law.

It is therefore important for this investigation to describe reasons of such a serious nature that DISS may lawfully derogate from the procedures prescribed by the ISS Act 2002. The Committee holds the opinion that it must be assessed on a case-by-case basis whether derogation from those procedures is permitted, because the operational situation on the ground can also differ from case to case.

Serious reasons may e.g. lie in the fact that DISS is investigating acute threats directed against Dutch or allied troops (threat to the force). They may also arise in connection with investigations into equally imminent threats to the achievement of the objective of the military mission (threat to the mission). DISS is expected to support the armed forces in these areas by providing early information to ensure the safety and effectiveness of Dutch soldiers and coalition troops. DISS would not be able to meet this expectation in all cases if the service should always have to satisfy all the requirements of the ISS Act 2002 when active in an area of operation. The fact is that there will usually be no time for complying with all procedural requirements of the ISS Act 2002 without unnecessarily endangering lives or harming the mission. Given the existence of an international mandate, the Committee holds the opinion that in those cases it is lawful for DISS to derogate from the statutory procedures when exercising special powers to the extent necessary and if permitted under the international mandate. The Committee can also imagine exceptional circumstances in which DISS derogates from the procedures prescribed in the ISS Act 2002 when operating abroad without the existence of an international mandate. The Committee holds that this can only be the case if it is absolutely necessary for DISS to derogate from the procedures prescribed by the ISS Act 2002, for instance because the life of an employee of the Ministry of Defence threatens to be put in immediate danger.[14]

---

[12] See review report CTIVD no. 28 on the use of Sigint by DISS, *Parliamentary papers II* 2011/12, 29 924, no. 74 (appendix), available on www.ctivd.nl), p.31-33.

[13] See e.g. Parliamentary Papers II 2000/01, 25 877, no. 58, p. 42; Minutes I 2014/15, 1-11-8; *Parliamentary Papers* 2014/15, 33 321, no. 5 and *Parliamentary Papers II* 2013/14, 33 820, no. 2.

[14] See also *Parliamentary Papers II* 2000/01, 25 877, no. 58, p. 42.

3.7 Safeguards covering derogation from statutory procedures

The Committee is aware that it is often possible to foresee situations in which it will be impossible to (fully) comply with procedures. For instance, because during the military mission the armed forces will conduct operations for which DISS is expected to immediately supply tactical intelligence to a commander for the purposes of Force Protection.[15] The Committee therefore considers it necessary that DISS prepares descriptions of such situations to the extent possible and submits them to the Minister in an application for approval. The application must deal with the following aspects, substantiated by reasons:

- the special power that will be exercised;
- how DISS will derogate from the statutory procedures in exercising the power;
- how the protection of privacy can be safeguarded as much as possible;
- the situations in which this will be the case;
- the serious reasons compelling DISS to conclude that it should derogate from the statutory procedures prescribed by the ISS Act 2002;

Furthermore, the Committee holds that it is also necessary to prepare adequate reports on the exercise of a special power in an area of operation if the procedure followed derogates from the procedures prescribed by law. The report must show in which cases the special power was exercised and how. The report must also show when and how the procedure followed derogated from the standard procedures. The Committee considers such reporting important for the purposes of internal accountability, external verification and from the perspective of due care.

3.8 Conclusion

A mandate under public international law generally provides a legal basis for DISS to deploy intelligence means abroad in support of the armed forces. Within the parameters of the international mandate DISS must in principle apply the ISS Act 2002 by analogy. If necessary, however, DISS may derogate from the procedures prescribed by law. However, there must be serious reasons for doing so and the international mandate must permit the actions of DISS. DISS must follow a procedure which as far as possible safeguards the protection of privacy. Furthermore, it is important that DISS keeps adequate records for the purposes of internal accountability, external verification and due care.

[15] Force protection entails the efforts of the armed forces to protect the (physical) safety of dispatched Dutch or allied units.

4. Regular procedure followed by DISS for sigint operations

4.1 Introduction

In this chapter the Committee describes the regular procedure used by DISS for the selection of sigint. The procedure actually followed by DISS while participating in the anti-piracy missions of HNLMS Rotterdam in 2012 and HNLMS Johan de Witt in 2013 will be discussed in the next chapter.

4.2 The regular procedure used by DISS for sigint operations

With the technical means available to it, DISS can receive and record non cable-bound telecommunications by untargeted interception. 'Untargeted' means that the interception is not targeted at messages sent by a specific person or organisation or related to a technical characteristic but that, for instance, all communication being transmitted is as it were plucked from the air and then stored (the so-called bulk).

It is for the examination of the content of the intercepted telecommunication that the power to select was included in the ISS Act 2002.[16] This power permits DISS to examine the content of the intercepted telecommunication on the basis of certain selection criteria. DISS requires the prior authorisation by the Minister for doing this.

There are three kinds of selection criteria:

(a) data on the identity of a person or organisation (e.g. name, alias);
(b) a number or technical characteristic (e.g. email address, phone number), and;
(c) a search term (e.g. name of a weapon-system, type number of an airplane).

The application for permission must satisfy a number of minimum requirements. The application must at least contain the name (of the person or organisation) or their number. Additionally, it must specify the reason why selection is necessary. The reason stated must show that the selection (and therefore the examination of the content of certain telecommunication sessions) satisfies the requirements of necessity, proportionality and subsidiarity. The approval is valid for a maximum period of three months for the selection criteria under (a) and (b) and can be renewed. Permission for search terms (criterion (c)) is valid for a maximum period of one year. DISS may not examine content of intercepted telecommunication related to the selection criteria until it has obtained the minister's permission.

Furthermore, the Minister of Defence may, and in this case did, grant DISS permission to select data using generic identities.[17] If a person falls within the scope of a generic identity (for instance because DISS has good reason to believe that he or she is linked to groups engaged in piracy), then under the

---

[16] Using a technical characteristic, however, DISS may already explore the communications, which is known as searching. See article 26 ISS Act 2002.

[17] Generic identities are broadly formulated identities covering a certain 'type' of persons or organisations. An example is "pirates active in the territorial waters of Somalia". See also review report CTIVD no. 28 on the use of Sigint by DISS, *Parliamentary papers II* 2011/12, 29 924, no. 74 (appendix), available on www.ctivd.nl), p. 52-54. The Committee has expressed its understanding for the use of generic identities for selection purposes. The need to be able to quickly build up an adequate information position arises in particular in the case of a military mission abroad. In such situations it may be necessary to initially deploy a wide range of powers in order to build up such information position. The Committee has described above that the statutory rules and the requirements of actual practice diverge on this point.

permission already obtained DISS may immediately select this person's communications. In the next application for renewal of the permission by the Minister, DISS must then still submit and render account of the selection to the Minister. In this application DISS describes the number or technical characteristic and (as far as known) the name of the person and the reason for using the power of selection.

5. The procedure followed by DISS during the anti-piracy missions

5.1 Introduction

In this chapter the Committee describes the procedure followed by DISS during the two anti-piracy missions in the waters around Somalia. It first considers the background of the anti-piracy missions. Subsequently, it sets out the procedure followed by DISS. Finally, the Committee examines the difference between the regular procedure and the procedure actually followed.

5.2 The legal background of the anti-piracy missions Ocean Shield and Atalanta

The international mandate for the anti-piracy missions derives from the United Nations Convention on the Law of the Sea (UNCLOS), supplemented with a number of UN Security Council resolutions.[18] UNCLOS provides the legal basis for taking action against piracy on the high seas. The UN resolutions show, moreover, that the UN Security Council authorized states and regional organizations to take all necessary measures appropriate to combat piracy in Somalia (both on land and in the territorial waters). These measures, as can be read in those resolutions, must respect international law (including human rights and humanitarian war law). NATO and EU worked out the details of certain powers ensuing from the international mandate in rules of engagement. These rules did not provide for the deployment of intelligence means.

5.3 The procedure followed by DISS during the anti-piracy missions

When the HNLMS Rotterdam and the HNLMS Johan de Witt were deployed to the anti-piracy missions, DISS was asked to provide support by supplying intelligence.

For this purpose DISS placed a unit on the Dutch vessels, a so-called National Deployed Sigint Section (NDSS). It had the task of investigating communications that were relevant to the protection of the deployed troops (*threat to the force*) and to threats endangering the achievement of the objectives of the anti-piracy missions (*threat to the mission*).

The relevant communications were immediately used to provide tactical intelligence support to, amongst others, the Force Commander and the vessel commander. After examining the telecommunications content, the DISS employees in the area of operation assessed whether it contained relevant tactical data for the execution of the anti-piracy mission.

DISS kept records of the information it provided to the commanders. It recorded in the reports what was communicated to the commanders, on the basis of which data, and what was the source of that data.

---

[18] The legal basis for the operations of the Dutch armed forces at EU level (Atalanta) and at NATO level (Ocean Shield) in the territorial waters of Somalia lies in the following UN Security Council resolutions: 1846 (2008), 1851 (2008) and 2067 (2012). The international mandate following from *inter alia* these resolutions, was renewed each time for one year.

It also happened that intercepted communications did not have direct relevance for the intelligence support of the anti-piracy mission, but might be relevant for another ongoing DISS investigation. DISS had to obtain permission via the regular procedure before it was allowed to use such data for such an ongoing investigation.

Finally, the deviating procedure also implied examination of communication content that had no relevance at all for DISS. DISS made no further use of such communications.

Since it was impracticable to analyse all intercepted communications for relevance, the NDSS among other things carried out its investigation using metadata analysis and data from other intelligence sources. An example: by exercising another special power DISS had identified a number or technical characteristic of a person who might be involved in piracy. NDSS could immediately investigate this new and so far unknown number or technical characteristic and the communication sessions in which it was used, on location. Another example: on-site investigation revealed that a known pirate frequently communicated with an as yet unknown person. This unknown person could be investigated immediately by selecting his communications.

5.4 The difference between the regular procedure and the procedure actually used

Comparison of the regular procedure and the procedure actually used shows up the following difference:

The regular procedure requires that prior to targeted examination of telecommunications DISS must obtain the minister's permission on the basis of specific selection criteria or generic entities. In the procedure actually used, DISS had obtained prior permission to examine the content of all locally intercepted telecommunications.

5.5 The reasons for DISS to derogate from the regular procedure

DISS stated the following reasons for derogating from the regular procedure:

- The intelligence support was inherently *time-critical*. A basic prerequisite for providing such support is the early identification of relevant communication sessions followed by reporting its content to the commanders as soon as possible. These relevant communication sessions may contain information on intentions, capacities and activities of pirates or other armed groups in the area. Under the operational circumstances of the anti-piracy missions any delay in communicating this information to the commanders constituted too large a risk, because it would then be impossible to contribute effectively to the effective execution of the mission in terms of protection of the armed forces deployed and/or achieving the mission's objectives.

- Furthermore, the intelligence support was inherently *dynamic*. The interception took place from a marine vessel at sea. After each shipping movement, communications were intercepted from an entirely different and new area with other, unknown potential targets. Working under such operational circumstances requires the processing chain for locally intercepted communications to be set up as efficiently as possible, so that time-critical information obtained from these communications will reach the commanders in time.

In the next chapter the Committee will deal with the question whether the procedure followed by DISS was lawful within the framework of the anti-piracy missions abroad.

6. Review of the lawfulness of the procedure used

6.1 Introduction

In this chapter the Committee will answer the question whether the procedure followed by DISS during the anti-piracy missions was lawful. It reviews the procedure actually used against the legal framework. The Committee answers the question whether there were serious reasons to derogate from the procedures prescribed by the ISS Act 2002. Was the derogation sufficiently substantiated by reasons? Subsequently, it will assess whether DISS kept adequate records of the procedure as actually used.

6.1 Derogation from the procedures prescribed by the ISS Act 2002

The Committee has found that there was a mandate under public international law for the anti-piracy missions. The international mandate derived from the United Nations Convention on the Law of the Sea (UNCLOS), supplemented with several UN Security Council resolutions.19 The international mandate provided a legal basis for the deployment of intelligence means by DISS to combat piracy, provided it did not violate international law. DISS also had to operate within the framework of the ISS Act 2002, unless serious reasons justified derogation from the procedures prescribed by this Act. Were such serious grounds present?

DISS was expected to provide timely and effective support for the anti-piracy missions so that among other things *threats to the mission* and to the personnel involved (*threat to the force*) could be eliminated or limited. The safety of Dutch soldiers was at stake. Persons and groups were present in the area of operation that posed a real threat and against whom the operational forces must be able to act quickly.

The Committee holds the opinion that in the cases it investigated DISS had sufficiently substantiated that there were serious reasons to derogate from the prescribed procedures. DISS demonstrated that permission for the immediate examination of content of all locally intercepted telecommunications was essential for the adequate performance of its task of supporting the anti-piracy missions. Strict application of the ISS Act 2002 on this point would have prevented effective and timely support of the commanders. It was in particular the time-critical nature of the intelligence support adduced by DISS which the Committee considered decisive in this respect. The procedure actually used enabled DISS to provide the missions' commanders with relevant and timely information.

[19] UN Security Council Resolutions 1846 (2008), 1851 (2008) and 2067 (2012). The international mandate following inter alia from these resolutions, was renewed each time for one year. NATO and EU worked out the details of certain powers ensuing from the mandate under international law in rules of engagement. These rules did not provide for deployment of intelligence means..

DISS made clear in which way it was going to derogate from the statutory procedures. The Committee has established that DISS would only use the deviating procedure if this was necessary for the provision of intelligence support to the mission's commanders. DISS would not use the procedure for its regular investigations. The Committee holds that the protection of privacy was thus safeguarded as far as possible. The Committee holds the opinion that DISS has adequately substantiated that it only derogated from the statutory procedures to the extent necessary to provide the requested intelligence support.

6.3 Reporting

In chapter 3 the Committee described the necessity of keeping adequate records of the exercise of special powers in an area of operation. This applies in particular where DISS considered it necessary to derogate from the procedures prescribed in the ISS Act 2002.

The Committee holds that adequate records have been kept of the procedure actually used. It was recorded in the internal systems used by DISS in which situations the power of selection was exercised and on the basis of which telecommunication characteristics DISS intercepted communications. The records also show whether these characteristics could be linked to a person or organisation.

The reporting on the results of the procedure is also considered adequate by the Committee. DISS reported on the provision of information to the commanders. The records give an adequate picture of the data underlying the information provided (for example: a specific communication session). In addition, the Committee considers it to be sufficiently verifiable from the records whether the information provided was indispensable for the intelligence support of the anti-piracy missions. The reporting shows that the commanders were only provided with information that was relevant in the context of the intelligence support of the anti-piracy missions.

6.4 Conclusion

In view of the above the Committee concludes that the exercise of the power of selection in the context of the deployment of HNLMS Johan de Witt and HNLMS Rotterdam for the purpose of the anti-piracy missions was lawful.

7. Conclusions

In the context of the participation in the anti-piracy missions of HNLMS Rotterdam in 2012 and HNLMS Johan de Witt in 2013, DISS used the power to select sigint. DISS exercised this power in a manner deviating from the normal method and by doing so derogated from the procedures prescribed in the ISS Act 2002.

A mandate under international law is generally considered to provide a legal basis for DISS to exercise intelligence means abroad in support of the armed forces. Within the framework of the international mandate DISS will in principle have to apply the ISS Act 2002 by analogy. If necessary, DISS may derogate from the procedures prescribed in the ISS Act 2002. There must be serious reasons for doing so, however, and the international mandate must permit the activities of DISS. DISS must follow a procedure which as far as possible safeguards the protection of privacy. Furthermore, it is important that DISS keeps adequate records in view of internal accountability, external verification and due care.

The Committee has found that there was a mandate under international law for the anti-piracy missions. It provided a legal basis for the exercise of intelligence means by DISS to combat piracy, provided it did not violate international law.

It is the opinion of the Committee that in the cases it examined DISS has adequately substantiated that there were serious reasons to derogate from the procedures prescribed in the ISS Act 2002. DISS has demonstrated that strict application of the ISS Act 2002 would have prevented the effective and timely support of the commanders. In this context the Committee attaches particular importance to the argument put forward by DISS of the time-critical nature of the intelligence support since this support served to contribute to the timely and effective limitation of threats to the mission and to the personnel involved (threat to the force).

DISS made clear in which way it was going to derogate from the statutory procedures. The Committee has established that DISS would only use the procedure if this was necessary for the provision of intelligence support to the mission's commanders. DISS would not use the procedure for its normal investigations. The Committee holds that the protection of privacy was safeguarded as far as possible;

The Committee considers the reporting on the procedure actually used to have been adequate. The same applies to the reporting on the results of the procedure.

The Committee concludes that the exercise of the power to select sigint in the context of the two anti-piracy missions was lawful.

CTIVD no. 44

DEFINITIONS

To the review report on two operations performed by DISS to support the Dutch efforts to combating piracy in the Horn of Africa

Special power	A power conferred on the service which entails a specific infringement of privacy. Special powers are usually exercised in secret. The special powers and the conditions under which they may be exercised are laid down in articles 20-30 ISS Act 2002 (e.g. tapping or deploying an agent).
Interception	The interception of data.
National Deployed Sigint Section (NDSS)	An advanced sigint post in an armed forces deployment zone.
Non cable-bound communication	Communication via a wireless connection, i.e. over the air (e.g. satellite connections).
Untargeted interception	Interception where the person, organisation or technical characteristic at whom/which the interception is targeted cannot be specified in advance.
Power of selection	The power to select (i.e. examine content) of non cable-bound communications (e.g. satellite connections) obtained by untargeted interception.
Signals intelligence (sigint)	Intelligence collected from intercepted electronic signals received. It is made up of two types: communications intelligence (comint), which concerns communications over the air between two parties (taking place via satellite or HF radio links) and electronic intelligence (elint), which concerns radar signals over the air. In this report Sigint only refers to comint, communication between two parties.
Technical characteristic	Characteristic traceable to various elements of (tele) communication, for instance a phone number or an email address.
Telecommunication	Communications at a distance by electronic means (e.g. telephone, radio, fax or the internet).

Anna van Saksenlaan 50 | 2593 HT Den Haag
T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl