Review Committee on the Intelligence and Security Services (CTIVD)

ANNUAL REPORT

2009 - 2010

The annual report covers the period that ended on 31 March 2010.

Table of contents

ANNUAL REPORT 2009-2010

Introduction

This year the Review Committee for the Intelligence and Security Services (CTIVD) had to bid farewell to its first chairperson, Ms I.P. Michiels van Kessenich-Hoogendam. The Committee also took leave of Mr B.A. Lutken, who likewise was a member of CTIVD from the start. It took a long time for new members to take up office. The year included a certain period of transition.
At the same time the Committee was asked more and more frequently to conduct certain investigations, causing the Committee's workload to increase. Since an intended staff expansion could not take place on account of economy measures, the Committee was compelled to make choices as to what it could and could not take in hand immediately.

In the reporting year the two intelligence and security services were confronted with affairs that drew a lot of attention. In both cases the Committee was requested to investigate how the services had handled the affairs.

In reaction to a publication by daily newspaper De Telegraaf on 28 March 2009, the General Intelligence and Security Service (GISS) investigated a supposed leak in its own organisation. The investigation resulted in an official report dated 11 June 2009 to the Public Prosecutor's Office, following which an employee and a former employee of GISS were arrested and the author of the publication, a journalist at De Telegraaf, had her home searched. De Telegraaf alleged that some of its journalists had been tapped by GISS and instituted proceedings against the service. The court considered it important that the journalist whose home had been searched had the right to lodge a complaint with the minister of the Interior and Kingdom Affairs, in which it is established procedure for the Review Committee to act as complaints advisory committee. De Telegraaf then lodged a complaint. The Committee advised the minister to declare the complaint partly well-founded, namely the part concerning the violation of the principle of proportionality when the special powers were first exercised against two of the journalists. Contrary to usual practice, the minister sent the Committee's advice to the Second Chamber of Parliament. The minister fully adopted the Committee's advice and discussed the consequences with the Second Chamber in an emergency debate held on 17 December 2009.

Early in 2009 the first newspaper reports appeared about two suspended employees of the Defence Intelligence and Security Service (DISS), who accused the service of negligent, and even unlawful conduct towards them. The minister of Defence was asked questions about the matter in parliament. Further publications followed and the questions from members of parliament also continued, which caused the minister of Defence to request the Committee, on 12 May 2009, to investigate the matter. The minister not only requested the Committee to investigate whether the conduct of DISS with respect to the two suspended employees had been lawful, but also the possible measures that could prevent such situations in the future, as well as certain measures already taken within DISS. Even after the Committee had started its investigation, various publications concerning the matter continued to give rise to questions in parliament. The Committee has conducted an extensive investigation and expects to be able to complete it fairly soon.

The Committee considers it to be one of its tasks to provide answers to questions that politicians and the general public have concerning matters like the ones mentioned above. The Committee is eminently equipped to do so, because of its ensured independence and its wide powers, which enable it to conduct in-depth investigations into the services. When there is a public allegation that a service has made a faux pas, it is important that the Committee investigates the matter and provides clarity on the issue by means of a public report or advice. The Committee attaches great importance to giving the best possible support to the review task of the two Chambers of the States General by means of its investigative activities and reports.

It is important, though, to realise that the attention devoted in the public debate to the matters mentioned above, serious as they are, is disproportionate in relation to other activities of the services. The vast majority of the work done by the services is and remains invisible to the public. Indeed, little attention is paid to this work in the public debate. And yet it is important work. Think of the investigation by GISS of terrorist networks in our country and of the many activities undertaken by DISS in Afghanistan to protect the Dutch soldiers who are active in that country.

Bearing this in mind, the Committee also considers it one of its tasks to initiate investigations itself, investigations that are not inspired by media attention or interest shown by parliament. The various monitoring activities of the Committee and the interviews it holds with employees of the services give it a good overview of the activities of the services. Based on this overview, which is continuously updated, the Committee is able to make a sound assessment of subjects that are worthy of investigation. So the Committee does not merely respond to what goes on in the public debate, but also provides context by investigations it initiates itself.

In section 2 of this annual report the Committee will describe its activities in broad outline. In sections 3 through 6 it will present a more detailed discussion of a number of noteworthy subjects. Section 7 briefly considers a bill that will have consequences for the Committee's tasks and activities. Section 8 deals briefly with international contacts. The part containing appendices includes a general explanation of the tasks, organisation and activities of the Committee, as well as an overview of the reports that have been published so far. At the end of this annual report, the public parts of two reports published in the reporting year which have been translated into English are included in full.

Chapter 1

The reporting year in broad outline

General

In the past year the Committee underwent a number of staff changes. On 1 June 2009 the term of appointment of Ms I.P. Michiels van Kessenich-Hoogendam, chairperson of the Committee, expired. The term of Mr B.A. Lutken, member of the Committee, ended one month later. Both had been involved with the Committee from the beginning. They shaped the Committee and contributed to the reputation acquired by the Committee and the appreciation it presently enjoys. Indeed, we owe a large debt of gratitude to both of them for the way in which they performed their duties in the past six years.
After serving as acting chairman for a short period, Mr A.H. van Delden, who joined the Committee on 1 January 2008, was appointed chairman as of 1 July 2009. On 1 September 2009 Mr E.T. van Hoorn was appointed a member of the Committee, followed by Ms S.J.E. Horstink-Von Meyenfeldt, who was appointed on 1 January 2010.

At present the Committee is therefore composed as follows:

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

The Committee members all work part-time.
On 1 May 2009 Mr N. Verhoeven succeeded Mr P.D. van Hees as secretary to the Committee. The staff is further made up of four full-time review officers and a secretary.
In connection with its increasing workload the Committee expressed a desire to expand its staff. So far, this expansion has not been realised on account of economy measures.

Pursuant to Article 64(2) of the Intelligence and Security Services Act 2002 (further referred to as the ISS Act 2002), the Committee is charged with reviewing whether the tasks laid down in or pursuant to this Act and the Security Screening Act are performed lawfully. For this purpose the Committee conducts in-depth investigations, each of which results in a review report that is ultimately sent to the two Chambers of the States General by the minister concerned (the minister of the Interior and Kingdom Relations in the case of GISS and the minister of Defence in the case of DISS). In addition, the Committee performs systematic monitoring with respect to a number of issues. It also acts as complaints advisory committee.

In-depth investigations

The Committee issued four review reports in the reporting year, three regarding GISS and one regarding DISS. In regard to GISS the Committee issued reports on financial and economic investigations, on the performance of the security screening of the (former) chief of the police force of the province of Zeeland, and on the cooperation with foreign services (see also section 3). In regard to DISS the Committee issued a report on the conduct of DISS towards a former agent. The public parts of the reports that have been translated into English are included in this annual report as an appendix (appendix 3).

At the close of this reporting year, moreover, the Committee had already adopted the report on the performance by GISS of the obligation to notify, but the minister of the Interior and Kingdom Relations has not yet sent this report to the Second Chamber. By the time this annual report is published it will have been sent to parliament, and therefore the Committee, bearing in mind the importance of being up to date, considered it advisable to attach the report as an appendix (see also section 5 on this subject).

A number of the Committee's in-depth investigations are nearing completion. These are investigations of the official reports of GISS, the performance by GISS of its foreign intelligence task, the activities of DISS in the field of signal interception and the conduct of DISS towards two suspended employees. There are also investigations that have not yet reached such an advanced stage. These are the investigation of the official reports of DISS and of the cooperation between DISS and foreign services. With respect to the investigation of the classification of state secrets by GISS the Committee communicated that for the time being it feels compelled to give priority to the (complicated) investigations it has already started and which are subject to a certain time pressure. This means that the classification investigation has not been started yet.

Systematic monitoring

In the reporting year the Committee continued its systematic monitoring of both services in regard to a number of subject matters. These are:

- official reports issued by the services;
- exercise of powers under Art. 25 (*inter alia* telephone taps) and Art. 27 (signal interception) of the ISS Act 2002;
- performance of security screenings;
- processing of applications for inspection of files;
- performance of the obligation to notify.

The monitoring is done by random inspections. In this way the Committee obtains a picture of the key activities of the services which, though not complete, is sufficiently reliable.

The monitoring findings may give the Committee reason to institute an in-depth investigation. When the Committee considers it necessary to do so, it will also contact the services or the minister concerned in response to monitoring findings. This may be about actual cases as well as policy matters. In the reporting year the Committee corresponded, among other things, about official reports of DISS, a number of security screenings done by the services and the policies of GISS in regard to applications for inspection of files and in regard to notification. In one case the Committee requested the two ministers in this context to pass on a letter to the Second Chamber. This was a letter concerning the reasons stated by the services for their refusal to grant inspection of documents to an individual based on the argument that inspection would result in disproportionate harm to the Committee of Inquiry into the Iraq decision-making process (Davids Committee) as long as this committee had not completed its report. The minister of the Interior and Kingdom relations sent the letter to the Second Chamber on 27 January 2010.[1] Meanwhile, the administrative court has examined the case in appeal proceedings commenced by the person concerned and has decided in his favour (see also section 6).

Complaints

A person with a complaint about GISS or DISS must lodge the complaint with the minister of the Interior and Kingdom Relations or the minister of Defence, respectively. The minister then calls in the Committee as independent advisory complaint committee. The Committee assumes full charge of handling the complaint. It hears persons concerned in the matter and examines the files of the service in question. The Committee submits an advice to the minister, following which the minister takes the ultimate decision. If, however, the minister departs from the Committee's advice, the advice must be sent to the complainant.

In the reporting year the Committee handled ten complaints, eight regarding GISS and two regarding DISS. At the time of closing this annual report it is still dealing with one complaint in respect of GISS.
In regard to four complaints concerning GISS the Committee advised the minister of the Interior and Kingdom Relations to declare the complaint manifestly ill-founded. In the opinion of the Committee it was immediately clear from the relevant notices of complaint

[1] *Parliamentary papers II* 2009/10, 30 977, no. 29.

that there could not be any reasonable doubt about the opinion that in each case the complaint was manifestly ill-founded.
In regard to two complaints concerning GISS and one complaint concerning DISS the Committee advised the minister concerned to declare the complaint ill-founded.
The Committee advised the minister of the Interior and Kingdom Relations to declare the complaint of De Telegraaf et al. partly well-founded (see also section 4 below). The minister sent the Committee's advice in its entirety to the Second Chamber.[2]
In regard to one complaint concerning GISS and one complaint concerning DISS the Committee advised the minister concerned to declare the complaint partly well-founded. Since the minister has not yet given a decision on these two cases and the complainant has therefore not been notified yet of the outcome of the procedure, the Committee can say no more about them in this annual report.

In eight cases the two ministers followed the advice of the Committee. In the two other cases the minister has not yet taken a decision in reaction to the advice.

In addition to the above, the Committee also monitors the complaints that are not taken up by the ministers of the two ministries concerned. The Committee examines whether they made the decision on valid grounds.

The Committee has surveyed to what extent complaints about GISS and DISS were disposed of within the term prescribed by law. It has established that time limits are exceeded systematically, usually by a number of weeks, which it considers unacceptable. Since both the ministers and the Committee play a role in disposing of complaints, it is important that they take joint action regarding this failure to comply with time limits. In a letter dated 24 February 2010 the Committee called the attention of the ministers of the Interior and Kingdom Relations and of Defence to this issue. Both ministers have now informed the Committee that they will make an effort to prevent future failures to meet time limits as much as possible.

Working procedure of the Committee

In this reporting year, as in the preceding years, the Committee had the full cooperation of GISS and DISS. The Committee has found several times, though, that obtaining information from DISS was delayed by the internal procedures of this service, which hampered the Committee's investigations. In consultation with DISS the Committee is considering how this situation can be improved.

2 *Parliamentary papers II* 2009/10, 30 977, no. 26.

By letter of 14 July 2009 the Committee informed the Second Chamber that it found it odd that pursuant to current law it required the permission of the ministers concerned to hear *former* employees of the services. It questions the fact that in performing its statutory review task it is dependent on the permission of the persons who are subject to its review. By letter of 7 September 2009 the minister of the Interior and Kingdom Relations sent her reply to the Second Chamber. The minister stated that if the Second Chamber considered it necessary to amend the law on this point, she was willing to examine how an adjustment could be included in an amendment to the ISS Act 2002 to be set in motion at the proper time. She also stated that permission to hear former employees was always given. For the Committee, this point has thus been satisfactorily settled for the time being.

Regular contacts

The Committee meets with the Second Chamber, the ministers concerned and the management of GISS and of DISS on a regular basis. On 12 May 2009 the Committee discussed its annual report, just issued then, with the parliamentary Standing Committee on the Interior and Kingdom Affairs. On 14 May 2009 it also talked about the same subject with the parliamentary Committee on the Intelligence and Security Services. On 11 March 2010, at a closed meeting, the Committee consulted with the Parliamentary Standing Committees on Defence and on the Interior and Kingdom Affairs, addressing matters concerning both DISS and GISS.

On 31 May 2009 the Committee had a meeting with the minister of Defence to discuss its annual report. On account of various circumstances the Committee did not meet with the minister of the Interior and Kingdom Affairs in the reporting year. The Committee met for consultation with the management of GISS and of DISS twice in the reporting year. At these meetings they discussed, among other things, the reports issued by the Committee, ongoing investigations and the results of the Committee's monitoring activities.

On 21 April 2009 the Committee met with the secretary-general of the ministry of General Affairs, to discuss among other things the tasks of the Committee and the role of the secretary-general in his capacity as coordinator of the intelligence and security services.

In addition to the above, the Committee spoke with the National Public Prosecutor, who is the link between GISS and DISS on the one hand and the Public Prosecutor's Office on the other hand. At this meeting it was arranged that henceforth they would meet at least once a year.

In the following the Committee will consider a number of subjects in greater detail.

Chapter 2

Cooperation of GISS with foreign services

On 30 September 2009 the minister of the Interior and Kingdom Affairs sent the Committee's report on the cooperation of GISS with foreign intelligence and/or security services to the Second Chamber.[3] The report is the result of a large investigation, in the course of which the Committee devoted attention to a number of close cooperative relations existing of old, a number of close cooperative relations of a more recent nature, and relations with foreign services of relatively recent date. The files examined by the Committee related to the cooperation of GISS with foreign services in the period from early 2005 until mid-2008. In addition to the examination of files the Committee conducted a large number of interviews with officers of GISS.

In its report the Committee among other things considered the cooperation with services of countries that hardly have a democratic tradition and where human rights are violated (on a structural basis). It did so because this is where the tension between the interest of protecting human rights and legitimate operational interests makes itself felt most strongly. In the report the Committee takes the position that GISS should exercise utmost restraint in cooperating with services of such countries. In practice, however, precluding all and any cooperation with such services in advance could lead to undesirable and even disastrous situations. If such services possess information relating to a direct (terrorist) threat, it must be possible for GISS to apply to the services in question for information. And when GISS possesses indications of a concrete threat to another country, then for the purpose of preventing innocent victims it may be necessary to share information with the service or services concerned. This requires some degree of contact, albeit limited, between GISS and such services. At the same time GISS should not lose sight of the fact that it is bound by the parameters and restraints imposed by law.

The Committee also established in the report that in practice GISS often does not assess in a general sense whether or not to enter into a cooperative relation or does so only to a limited extent. There is no structured decision-making, for each individual foreign service separately, on the possibilities of entering into a cooperative relation with the foreign service. It is the opinion of the Committee that GISS must first make a fundamental assessment of the extent to which the criteria set for cooperation are satisfied and must do so at management level and for each individual foreign service separately. Subsequently,

[3] *Parliamentary papers II* 2009/10, 29 924, no. 39 (appendix).

in a concrete (operational) case the result of balancing the various interests involved can be examined against the general assessment of the foreign service. It is the opinion of the Committee that this system will do justice to both the restraints on cooperation with foreign services set forth in the law and legislative history, and daily practice in which actually cooperating with a counterpart may be essential to the adequate performance of its statutory tasks by GISS. The Committee observes in this context that this is not and indeed should not be a static process. While a cooperative relation with a foreign service continues and develops, GISS may at any time adjust the assessment of the service in question. But it must do so on the basis of the generally applicable criteria for cooperation, supported by reasons and at the proper level.

In the report the Committee established that in some cases GISS acted unlawfully when providing personal data to foreign intelligence and security services. It also established that a number of requests for assistance involving the exercise of special powers made by GISS to foreign services of which it is doubtful whether they satisfy the prescribed criteria for cooperation, did not satisfy the requirements of necessity, proportionality and/or subsidiarity.

In her reaction to the report the minister of the Interior and Kingdom Relations extensively discussed the above issues.[4] They were also discussed in the six-monthly consultations of the Committee and the management of GISS.

There has been a lot of interest abroad in the Committee's report, since cooperation between intelligence and/or security services is an issue that has hardly ever been investigated at the international level, while it certainly attracts the interest of the general public and parliaments, both in the Netherlands and abroad. In this context the Committee was asked to present further comments on the report at a workshop of the Office of the High Commissioner for Human Rights of the United Nations held on 1 and 2 March 2010 in Geneva.

[4] *Parliamentary papers II* 2009/10, 29 923, no. 39.

Chapter 3

Tapping journalists

On 28 March 2009 De Telegraaf ran an article on the role played by GISS in determining the government's position on giving political support to the war in Iraq, under the heading "GISS failed on Iraq". The authors of the article were the journalists Van der Graaf and De Haas. The article stated that GISS had unquestioningly taken over the threat assessments of foreign intelligence and security services. This emerged, so the article stated, from recent official evaluations. On 4 June 2009 De Telegraaf published an article by Van der Graaf and Kuitert, likewise a Telegraaf journalist, which reported increased security measures in reaction to threats against the Dalai Lama.

On 18 June 2009 an employee of GISS and her partner, a former employee of GISS, were arrested by the national department of criminal investigation on suspicion of disclosing state secrets. The criminal investigation of both persons included searches at their workplaces as well as the house they shared. In addition, one of the two journalists of the articles of 28 March 2009 and 4 June 2009 (Van der Graaf) was formally considered a suspect, but she was not arrested. Her house was searched and a number of items were seized. The basis for the arrests and searches was an official report of GISS, in which it reported the results of an operational investigation of a leak within the services to the Public Prosecutor's Office.

Court judgment

De Telegraaf instituted interim injunction proceedings against the State and claimed (*inter alia*) an injunction ordering termination of the exercise of special powers which they supposed were being exercised in regard to Van der Graaf, De Haas and editor in chief Paradijs. In her judgment of 23 July 2009 the judge hearing the interim injunction proceedings partly allowed the claims of De Telegraaf.[5] On the issue of the (supposed) exercise of special powers in regard to Paradijs and De Haas the judge took the ground that these persons could not be considered targets and that the State had failed to demonstrate sufficiently that the exercise of special powers satisfied the requirements of proportionality and subsidiarity. Under these circumstances the right to protection of a journalist's sources outweighed the interest of national security, so the judge ruled. The

[5] District Court of Amsterdam (pres.) 23 July 2009, *LJN BJ3552*.

judge prohibited GISS from further exercising special powers in regard to Paradijs and De Haas and prohibited GISS from inspecting or otherwise using any data already collected insofar as they related to the publications of 28 March and 4 June 2009.

On the issue of the exercise of special powers in regard to Van der Graaf the judge ruled that in the context of the interim injunction proceedings it could not be ruled out that GISS had considered Van der Graaf a target on valid grounds. The judge held that Van der Graaf was in a position in which she could be expected to lodge a complaint about the matter with the minister, who must then seek the Committee's advice on the complaint. The judge issued an injunction prohibiting GISS from inspecting or processing any data relating to Van der Graaf until the Committee would have stated its opinion and an injunction ordering GISS to cease exercising special powers in regard to Van der Graaf insofar as these related to the publications of 28 March and 4 June 2009. Both the State and De Telegraaf appealed the judgment given in the interim injunction proceedings. On appeal, the Court of Appeal of Amsterdam on 13 October 2009 confirmed the judgment given in the first instance.[6]

After judgment had been given in the interim injunction proceedings, De Telegraaf et al. lodged a complaint with the minister of the Interior and Kingdom Relations, following which the Committee, in its capacity as complaints advisory committee, undertook the task of handling the complaint. On 4 December 2009 the minister sent her decision to adopt the advice of the Committee, as well as the advice itself, to the Second Chamber.[7] In an explanatory note the minister explained that although handling an individual complaint was as a rule a procedure that concerned only the complainant(s) and the minister, she had decided to share the information with the Second Chamber since it concerned accountability for policy in the light of the obligation to provide information pursuant to Article 68 of the Constitution.

The Committee's advice

In the most conspicuous conclusion of its advisory report the Committee stated that the complaint was partly well-founded, namely insofar as it concerned the violation of the principle of proportionality when the special powers were first exercised against the two journalists Van der Graaf and De Haas. The Committee further established that GISS had not exercised any special powers in regard to editor in chief Paradijs.

---

[6] Court of Appeal of Amsterdam 13 October 2009, *LJN BK0003*.
[7] *Parliamentary papers II* 2009/10, 30 977, no. 26 (appendix).

The Committee stated that it was sympathetic towards the operational considerations that had induced GISS to commence exercising the special powers. Nevertheless, greater weight should have been attached at that moment to the interest of protecting a journalist's sources. The Committee substantiated this with the following considerations.

The question whether GISS observed the required proportionality when exercising special powers involves a balancing of interests. GISS has a special interest in safeguarding its integrity and reliability, which are impaired by the existence of a leak and by the disclosure of state-secret information. In this context it is relevant that the information was not only state secret, but had also not left the service by regular channels and could therefore only have come from an employee of GISS. Furthermore, the period between the draft memorandum and the publication was short, which was reason to suspect direct contact between the leak and the two journalists. Leaking a confidential internal document can impair the incorruptible functioning of GISS and harm contacts with foreign services and (other) sources of the service.

This interest of GISS must be balanced against the interest of the complainants in their capacity as journalists. The exercise of special powers violated the complainants' right to journalistic source protection. Journalists, who have the function of "public watchdogs" in the democratic legal system, have a legitimate interest in being able to publish on themes that are relevant to society. The right to source protection is essential for journalists in the performance of their task. In addition to the interest of the journalists on account of their profession, the protection of their privacy obviously also played a role, as embodied in Article 8 of the ECHR.

The Committee endorses the opinion that tracing a leak and establishing whether the two journalists had possession of a state-secret document serve the interest of protecting national security. The Committee holds, however, that this interest does not automatically outweigh the interest of journalistic source protection.[8] The outcome of this balancing of interests depends on the actual circumstances of the case.

The Committee takes the ground that at the time when the special powers were first exercised there were no *concrete* indications that more documents had been leaked or were still going to be leaked.

The Committee further takes the ground that though it is true that a state-secret draft memorandum had been leaked, which had not left the service by regular channels, the leaking of this memorandum could not directly harm national security.[9] The leaked memorandum did not pose a direct threat to the cornerstones on which the statutory obligation of secrecy embodied in the ISS Act 2002 is founded, namely source protection,

[8] See also ECtHR 10 December 2007, no. 69698/01, grounds 128-129 *(Stoll v. Switzerland)*.
[9] See e.g. ECtHR 9 February 1995, no. 16616/90, grounds 39-46 *(Weekblad Bluf! v. the Netherlands)*.

current level of information and method.[10] These three interests constitute the rationale behind the necessity of secrecy. The leak did not endanger the lives of others.[11]

On the other hand the Committee holds the opinion that as a result of the publication of the second article (on the Dalai Lama) the exercise of special powers in regard to journalists should be considered proportional in view of the intended purpose. The possibility, which GISS had already mentioned before, that other documents had been or would be leaked in addition to the draft memorandum that had already been leaked, could now be substantiated by concrete indications. There were concrete indications that it was not a once-only leakage of state-secret information relating to one specific subject topic. At the same time the information that had been leaked and the second article published as a result of the leak now did constitute a direct threat to the protection of the current level of information of GISS. It concerned recent information relating to the security of the Dalai Lama. The current level of information must be protected because persons threatening national security can adapt their tactics to it once it has been disclosed. This was in fact the case here: the publication of the article might endanger the safety of a person to be protected, the Dalai Lama.

This means that if at the time the special powers were first exercised there had been concrete indications that more documents had been leaked or would still be leaked, or that the leakage of the document could in fact have directly harmed national security, exercising them at that time would have been proportional.

It should be noted that the Committee advised the minister to declare ill-founded the primary part of the complaint, namely that GISS allegedly had had no authority to act on the basis of its a-task and that the two journalists of De Telegraaf should not have been considered targets. The Committee also established, though, that there had been several instances of negligence in the manner in which the telephone tapping was executed.

In an emergency debate on 17 December 2009 the minister of the Interior and Kingdom Affairs extensively discussed both the advice of the Committee with the Second Chamber and her decision to adopt the advice.[12]

---

[10] Contrary to threats to long-term interests, such as the aforementioned integrity of GISS and contacts with foreign services and (other) sources of the service.

[11] A criterion that played a role in earlier grounds taken by the Supreme Court. See HR 11 July 2008, LJN BC8421, paras. 3.7.4.3. *(Telegraaf)*.

[12] *Proceedings II* 2009/10, 39, p. 3768-3782.

Chapter 4

Notification

In the reporting year the Committee conducted a large investigation into the performance by GISS of the obligation to notify.

The statutory rules

When GISS and DISS exercise certain special powers that are listed exhaustively by law, this creates an obligation to notify pursuant to Article 34 of the Intelligence and Security Services Act 2002 (further referred to as the ISS Act 2002). Special powers that are subject to the obligation to notify are, for example, telephone tapping and forcing entry into a home. The obligation to notify means that five years after a special power has been exercised the services must examine whether a report of the exercise of the special power can be submitted to the person with regard to whom the power was exercised. The purpose of the obligation to notify is to (better) enable individuals to effectuate their fundamental rights. It is not possible in all cases to notify the person concerned. The obligation to notify may lapse, be suspended or be cancelled. The examination preceding notification may lead to the conclusion that the person concerned cannot be traced or has died. In these cases the obligation to notify lapses. If the notification examination shows that the special power is relevant to the current information level of the services, the obligation to notify will be suspended until the relevance has ceased. Furthermore, the notification examination may lead to the conclusion that the obligation to notify must be (permanently) cancelled if – briefly stated – notification can reasonably be expected to result in a source of the services being disclosed, in relations with other countries being seriously damaged, or in a specific use of a method of the services being disclosed.

Background

The *de facto* effective date of the obligation to notify was 29 May 2007, five years after the ISS Act 2002 entered into effect. The Committee has been monitoring the performance of the obligation to notify since its *de facto* entry into effect. For the purposes of better enabling the Committee to perform this review task, Article 34(2) of the ISS Act 2002 requires both GISS and DISS to inform the Committee if it is not possible to submit a report to the person concerned. The notice to the Committee must be accompanied by the reasons why the report cannot be submitted.

On 3 September 2008, at a general consultation of the minister of the Interior and Kingdom Relations with the Second Chamber, the minister reported that up to that moment no-one had been notified yet.[13] This came as a surprise to some parliamentarians. The minister then informed them that the Committee was already monitoring the performance of the obligation to notify and promised that she would ask the Committee to report on the matter after a reasonable period of time had passed. The minister also held out the prospect of a letter about the performance of the obligation to notify. In this letter, dated 4 December 2008, the minister stated that in practice the examination whether notification was possible was by no means a matter of routine and involved a very labour-intensive procedure.[14] This fact, together with the opinion of the minister that the statutory rules were not too stringent and that the obligation to notify was not a requirement of European law, induced the minister to remark that there should be no taboo about debating the benefits and necessity of the obligation to notify. The minister thought it too early, however, to conduct the debate at that time. She further drew attention to the fact that the findings of the Committee, which were still forthcoming, would have to be included in the discussion.

On 23 April 2009 the Committee reported that it had conducted an in-depth investigation into the performance of the obligation to notify. The investigation comprised the examination of the notification decisions – together with the underlying files - taken in the period from 29 May 2007 to 11 November 2009, inspection of the documents pertaining to the obligation to notify (establishing the parameters) and interviews with various employees of GISS involved in performing the obligation to notify. On 24 February 2010 the Committee adopted the report and sent it to the minister of the Interior and Kingdom Relations. At the time of closing this annual report the review report has not yet been sent to the Second Chamber, but at the time of its publication it will have been sent. On account of its topicality, the Committee has nevertheless opted to attach the report to this annual report as an appendix.

The findings of the Committee

The Committee established in the course of the investigation that in 43 per cent of the cases the outcome of the examination whether notification was possible was that the person concerned could not be traced. In 25 per cent of the notification decisions the obligation to notify was suspended and in 27 per cent of the notification decisions it was concluded that a ground for cancellation applied. In the remaining 5 per cent of cases the

[13] *Parliamentary papers II* 2008/09, 30 977, no. 12, pp.12-13.
[14] *Parliamentary papers II* 2008/09, 30 977, no. 18, pp. 5-7.

person concerned had died, or the special power had been exercised in regard to an organisation or it was eventually decided not to exercise the special power although permission to do so had been obtained.

Although no person has been notified so far, the Committee has established that as a rule GISS performed its obligation to notify in conformity with the statutory requirements. In the course of its investigation the Committee encountered a number of exceptional cases, in which the service had invoked an incorrect ground for establishing that the obligation to notify had lapsed or for postponing or cancelling notification. The Committee has recommended GISS to reconsider these cases. This does not mean to say, however, that reconsideration would result in notification, because there may be other grounds for deciding not to notify.

The Committee further holds the opinion that there are two points on which GISS follows a policy that is too restrictive or too stringent, namely with respect to tracing persons to be notified and with respect to postponing notification on account of ongoing investigations. The Committee has established in regard to the latter, though, that the policy is not implemented very stringently and is therefore consistent with the intention of the legislator, except in one single case.

The Committee has established that performing the obligation to notify takes up a considerable part of the capacity of GISS and this will probably only increase in the future. The Committee also has established that even though GISS generally performs the obligation to notify in a lawful manner, no notification letters have been sent so far. It is the opinion of the Committee that it is not possible to explicitly infer an active obligation to notify from the ECHR and the relevant case law of the ECtHR on this issue, and that the weight of such an obligation must be balanced against the complex of other existing legal safeguards. In this context the Committee draws attention to the means of redress already available to individuals, such as filing a complaint in response to alleged improper conduct by GISS and the possibility of filing an application for inspection of the personal data processed by GISS. In regard to the latter the Committee comments that such applications must be dealt with on the basis of the same principles that underlie the obligation to notify. The point, therefore, is the added value of the obligation to notify for the Dutch system of legal protection. This may also raise the question whether the costs of performing the obligation to notify are justified by its benefits. This involves a balancing of interests, however, which is not the responsibility of the Committee but of the legislator.

The Committee has not yet investigated how DISS deals with notification. So far, though, this service has not notified anyone either.

Chapter 5

Refusal of inspection of Iraq documents

In the course of its monitoring activities the Committee came across a refusal of an application filed by investigative journalist Wil van der Schans for inspection of all sorts of documents in the possession of GISS and DISS concerning the preparation and decision-making for providing political support to the invasion of Iraq. Both services refused the application, among other things by invoking Article 55(2)(g) of the ISS Act 2002:

> "An application will also be dismissed in so far as the importance of furnishing the information to which the application pertains is outweighed by the importance of […] preventing disproportionate preference or prejudice to the natural persons or legal entities or third parties involved in the matter."

GISS took the position that providing information on the Iraq issue would result in disproportionate prejudice to the Committee of Inquiry into the Iraq decision-making process (Davids Committee) as long as the committee in question had not completed its report. DISS took the same position. The Committee did not agree with the position taken by GISS and expressed this in a letter of 24 June 2009 to the head of GISS. The Committee stated that it appreciated the great significance of the activities of the Davids Committee. It failed to see, however, how providing information – suitable for publication – would result in prejudice to the committee in question, let alone in disproportionate prejudice. The Committee held the opinion that even if it should result in prejudice to the Davids Committee, this could not carry such weight as to justify a moratorium on providing information. In the opinion of the Committee, greater weight must be attached to the general interest of public access to information. The Committee held the opinion that the fact that the Davids Committee was conducting an inquiry into the Iraq issue did not mean that journalistic investigative activities had become superfluous. In the opinion of the Committee these investigative activities should in any case not be frustrated by a refusal to give journalists access to information which otherwise is public.

In their reactions of 1 October 2009 to the aforementioned letter, GISS and DISS tried to give further reasons for the position they had taken. In the first place GISS drew the Committee's attention to the fact that it was a policy agreed between the various ministries. GISS attached great importance to the Davids Committee being able to form its opinion in peace and quiet and without a public debate. For this reason there would in principle not be a debate between government and parliament on the substance of the matter prior to the presentation of the report. A public debate would unnecessarily

hamper the work of the Davids Committee and its progress. GISS took the position that the premature provision of information would result in disproportionate prejudice to both the Davids Committee and the authority that had commissioned the committee's report, that is: the cabinet. In the opinion of GISS the interest of providing information prior to the presentation of the report of the Davids Committee was outweighed by the interest of the Davids Committee being able to carry out its work in the intervening period without being disturbed. In order to safeguard the independence of the Davids Committee, every effort had to be made to avoid creating the appearance that the government was influencing the debate – and thus the inquiry by the Davids Committee – and wished to steer it in a certain direction by giving the public only limited access to information.

In response, the Committee sent a letter to the ministers of the Interior and Kingdom Relations and of Defence, requesting them to pass it on to the two Chambers of the States General at the proper time.[15] In the letter the Committee stated its opinion that it was not convinced by the answer it had received. The Committee took the position that the answer appeared to have been inspired primarily by the need, apparently felt to be a political necessity, of falling in with the ministries concerned and thus keeping the ranks closed. Although the concern expressed in the answer about safeguarding the independence of the Davids Committee did credit to the services, the Committee argued that the means used for this purpose in the present case – not providing information that previously had been freely accessible – did not strike the Committee as convincing.

After publication of the report of the Davids Committee, the Minister of the Interior and Kingdom Relations sent the Committee's letter to the two Chambers of the States General.[16] The minister enclosed her comment that now that the report had been published, the ground for refusal (ground g) no longer constituted a reason for not granting the application for inspection of files and that a new application for inspection of documents would be assessed anew.

The aforementioned journalist lodged an appeal with the administrative court against the decision to refuse inspection of files on the basis of on ground g. The case came before the court on 4 February 2010. The journalist had summoned the chairman of the Committee as a witness, and the chairman complied with the summons. It must be stated in this context that on account of the secrecy to be observed with respect to the Committee's work, such testimony could not go much further than what had already been discussed in the correspondence that has been made public. At the hearing the journalist also stated that he had filed a new application for inspection of documents. On 3 March 2010 the

[15] *Parliamentary papers II* 2009/10, 30 977, no, 29 (appendix).
[16] *Parliamentary papers II* 2009/10, 30 977, no. 29.

District Court of The Hague declared the appeal well-founded.[17] The court stated in the judgment that it endorsed the position taken by the Committee.

[17] District Court of The Hague 3 March 2010, AWB 09/8194 WIVD and AWB 09/8272 WIVD.

Chapter 6

Accession of the BES islands and the Committee

On 26 may 2009 the bill amending several laws in connection with the accession of the so-called BES islands (Bonaire, St Eustatius and Saba) was presented to the Second Chamber.[18] This bill implements the intention to have these islands accede to the Netherlands as a public body. One of the results will be that the responsibility of the Netherlands for national security will extend to include these three islands. Provision for this is made by declaring the ISS Act 2002 applicable to the BES islands, thus making GISS and DISS the competent intelligence and security services for the islands. By operation of law (by virtue of Article 60(1) of the ISS Act 2002), the chief of the police force of the BES islands will then be designated as a functionary who performs activities for GISS under Article 60. The second paragraph of Article 60 of the Act provides that subordinates of the chief of the police force may be charged with the actual performance and oversight of the activities. The activities will be performed under the responsibility of the Minister of the Interior and Kingdom Relations and according to the instructions of the Head of GISS. In addition, the police officers in the employment of this police force will be required to send relevant data to GISS and/or DISS (Article 62 of the ISS Act 2002).

Another result of declaring the ISS Act 2002 and the Security Screening Act applicable to the three islands will be that these activities will come to fall under the Committee's review task, as will the other activities of GISS and/or DISS on the islands. The bill describes the expectation that the consequences for the Committee will be limited since, as far as the implementation of both Acts is concerned, the decision-making processes in respect of their application will continue to take place centrally in the Netherlands.[19] The possibility exists, however, that witnesses and/or experts or complainants will have to be heard on one of the islands. The bill states that it will have to be analyzed in consultation with the Committee what the consequences for the Committee's work will be and what measures will have to be taken.

The bill was still being debated in the Second Chamber at the close of the reporting year.

---

[18] *Parliamentary papers II* 2008/09, 31 959, no. 2.
[19] *Parliamentary papers II* 2008/09, 31 959, no. 3 (MvT), p. 13.

Chapter 7

International contacts

The Committee considers it important to maintain international contacts. In the reporting year it participated in a number of international conferences on the oversight of intelligence and security services. In May 2009 the Committee, together with the chairman and the secretary of the parliamentary Committee on the intelligence and security services, attended the fifth *Conference of the parliamentary committees for the oversight of intelligence and security services of the European Union member states,* organised by the parliamentary oversight committee of Estonia. It also attended a conference of the European Consortium for Political Research (ECPR) in September 2009, which had devoted a special part of the programme to intelligence and security services. In March 2010 the Committee went to the International Intelligence Review Agencies Conference in Sydney, organised by the Australian Inspector-General of Intelligence and Security. The chairman of the Committee gave a presentation about the Dutch oversight system at this conference.

The Committee also gave presentations on the Dutch oversight system at a seminar of the Brunel University Centre for Intelligence and Security Studies and at several workshops organised by the Swiss institute Democratic Control of the Armed Forces (DCAF) in Geneva, one of them in collaboration with the UN.

And finally, the Committee maintains good contacts with similar committees abroad, of which in particular the contacts with the Belgian Comité I should not go unmentioned. In the reporting year the Committee visited Comité I in Brussels and it also attended an afternoon seminar on the new Belgian Special Intelligence means Act, which had been co-organised by the Comité.
The Committee has found that the Dutch oversight system meets with great appreciation abroad.

APPENDIX 1

The Committee (background)

Statutory tasks

The Review Committee on the Intelligence and Security Services commenced its duties on 1 July 2003. The Committee was established pursuant to the Intelligence and Security Services Act 2002 (hereinafter referred to as: the ISS Act 2002), which became effective on 29 May 2002.[20] Article 1 of the Act defines the term 'services' to comprise the General Intelligence and Security Service (GISS) and the Military Intelligence and Security Services (DISS), which fall under the political responsibility of the minister of the Interior and Kingdom Relations and the minister of Defence, respectively. In addition, the oversight task of the Committee covers the coordinator of the intelligence and security services, who is accountable to the minister of General Affairs (see Art. 4 of the ISS Act 2002).

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

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

By virtue of Article 64(2) of the ISS Act 2002 the Committee is charged with:

a. oversight of whether the provisions laid down in or pursuant to the ISS Act 2002 and the Security Screening Act[21] are implemented lawfully;
b. informing and advising the ministers concerned on the findings of the Committee (both on request and on its own initiative);
c. advising the ministers concerned on the investigation and assessment of complaints;

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

d. advising the ministers concerned on the obligation to notify, which is embodied in Article 34 of the Act and which entered into effect five years after the ISS Act 2002 entered into effect – from 29 May 2007, therefore.

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

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

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

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

In accordance with paragraphs (3) and (4) of Article 8 of the ISS Act 2002, which pursuant to Article 80 apply to the annual reports of the Committee as well, these public reports do

not mention any data giving an insight into the means the services have used in concrete cases, into secret sources or into the current level of information of the services, but the minister concerned may confidentially disclose such data to the States General. So far, all annual reports of the Committee, including the present one, have been fully public; there are no secret appendices. The annual reports are also published on the website of the Committee: www.ctivd.nl.

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

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

Investigations

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

Once the Committee has decided to conduct a specific investigation (on its own initiative or at the request of one of the ministers concerned or one of the Chambers of the States General), the ministers concerned and the presidents of the two Chambers are informed of this intention.

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

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

Furthermore, any person involved in the implementation of these two Acts, first of all the employees of the services therefore, are required, if so requested, to furnish such information and render such assistance to the Committee as it requires for the proper performance of its task. The only reservation made with respect to this twofold power is that if there is reason to do so, the services may state which data may, in the interest of national security, not be disclosed beyond the Committee.

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

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

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

The parliamentary history of the ISS Act 2002 shows that the legislator took the position that it was not advisable to let the Committee send the review reports it has produced directly to the two Chambers of the States General, because the minister had to be able to

assess publication of the information presented in the reports against state interests and the interests of national security. For this reason the reports are sent to the States General through the intermediary of the minister concerned, who then adds his or her comments on the report.

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

Complaints handling

Any person who wishes to submit a complaint about conduct of the services[22] must first – before filing his complaint with the National Ombudsman – apply to the minister responsible for the service concerned. The Committee plays an advisory role in the minister's handling of such complaints. Before giving a decision whether or not the complaint is well-founded, so Article 83(3) of the ISS Act 2002 provides, the minister must obtain the advice of the Committee. In this way the Committee acts as a mandatory external advisory body. Division 9.1.3 of the General Administrative Law Act (further referred to as "GALA") is applicable with respect to the advisory role of the Committee. However, in derogation of Article 9:14(2) GALA, the minister concerned may not give the Committee any instructions. This provision has been included in connection with the independence of the Committee.

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

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

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

After examining the files and hearing the persons concerned, the Committee assesses whether the conduct of the challenged service meets the standards of proper conduct. For this task the Committee has a broader assessment framework than for its review task, since the latter is restricted to review as to lawfulness.[23] Subsequently, the Committee sends a report of its findings accompanied by an advice and possibly by recommendations to the minister concerned (Article 9:15 GALA). The minister may depart from the Committee's advice, but in that case the minister must state the reason for departing from the advice in his or her reply to the complainant, and also must send the Committee's advice to the complainant.
In formulating its advice the Committee must therefore bear in mind that the advice may be made public. This will inevitably result in the Committee sometimes using vague and abstract wordings in its advice.

Before asking the Committee to give an advice on the merits of a complaint, the minister will first give the service concerned the opportunity to dispose of the complaint informally. This is in keeping with the view taken by the legislator that unnecessary formal and bureaucratic procedures are to be avoided.[24] The Committee likewise holds the opinion that the services must first be given an opportunity to dispose of complaints informally themselves, unless there are indications that this will be in vain.

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

[23] But lawfulness forms part of the standards of proper conduct applied as a criterion in handling complaints. *Parliamentary papers II* 1997/98, 25 837, B, p. 6.
[24] *Parliamentary papers II* 1997/98, 25 837, no. 3, p. 7.

complaint is inadmissible pursuant to Article 9:4 GALA or if it is not taken up pursuant to the provisions of Article 9:8 GALA. The requirement to call in the Committee only applies if the assessment whether a complaint is well-founded calls for a substantive assessment. In other words: the minister is not required to obtain the advice of the Committee if he refrains from giving a decision on the conduct. Manifestly ill-founded complaints, on the contrary, are not excluded from the minister's obligation to consider all complaints.[25] In principle the Committee must give an advice on such complaints as well. In these cases, however (and also if the complainant has stated that he does not wish to exercise the right to be heard), Article 9:10 GALA releases the Committee from the obligation to hear the complainant.[26]

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

26 *Parliamentary papers II* 1997/98, 25 837, B, p. 4.

APPENDIX 2

List of review reports

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

* Available in English

APPENDIX 3

Translated review reports issued in the reporting year

Review report 22A	On the cooperation of GISS with foreign intelligence and/or security services (Inzake de samenwerking van de AIVD met buitenlandse inlichtingen- en/of veiligheidsdiensten)
Review report 24	On the performance by GISS of the obligation to notify (Inzake de uitvoering van de notificatieplicht door de AIVD)

Review Report CTIVD no. 22A

On the cooperation of GISS with foreign intelligence and/or security services

Table of contents

Review Report CTIVD no. 22A

On the cooperation of GISS with foreign intelligence and/or security services

SUMMARY

Good cooperative relations with foreign services are essential for the adequate performance of its statutory tasks by the Dutch General Intelligence and Security Service, further referred to as GISS. They are essential because the information obtained by such cooperation considerably extends the existing information position[1] of GISS and thus increases its capability to assess national security risks and give the responsible authorities timely warning. Especially after the attacks of 11 September 2001, the need for international cooperation of intelligence and security services has emerged more clearly and the willingness to cooperate increased accordingly.

Cooperation of GISS with foreign services on Dutch territory must take place under the direction and control of GISS. GISS frequently investigates indications of possible interference. After identifying unwanted secret activities by intelligence services of other countries, GISS will usually take timely action and appropriate measures depending on the situation.

Before starting to cooperate with a foreign intelligence and/or security service GISS must first assess carefully whether the service qualifies for cooperation. Criteria to be considered are respect for human rights, democratic anchorage, the tasks, professionalism and reliability of the service, the advisability of cooperation in the context of international obligations, enhancement of the performance of statutory tasks and the degree of reciprocity *(quid pro quo)*.

It is the opinion of the Committee that GISS should exercise utmost restraint in cooperating with services of countries that have no or hardly any tradition of democracy and where human rights are violated (on a structural basis). In actual practice, however, precluding all and any cooperation with such services in advance could lead to undesirable and even disastrous situations. At the same time GISS should not lose sight of the fact that it is bound by the parameters and restraints imposed by law.

[1] In this report 'information position' means the information in the possession of and potentially available to GISS and its negotiating position in exchanging information with foreign counterparts.

The Committee has established that in concrete operational cases GISS will assess whether a specific way of cooperating with a specific service in a particular situation is permissible. The Committee draws attention to the fact that the process of exclusively making such an *ad hoc* assessment is too limited and may have undesirable consequences. It is the opinion of the Committee that for each foreign service with which GISS cooperates it should assess to what extent the service meets the criteria for cooperation. GISS should also state for each individual foreign service, supported by reasons, what forms of cooperation are in principle permissible.

The Foreign Relations department of GISS has an important task in helping to develop, maintain and safeguard the quality of cooperative relations. The Committee has found that in actual practice the steering role of the Foreign Relations department has not taken shape sufficiently.

GISS exchanges information with a large number of services on all kinds of matters. The information exchanged may vary from general information on certain themes and in-depth analyses of phenomena to highly concrete information on particular matters or persons. For each of these forms of information exchange GISS must always ask itself whether it is permissible to provide this specific information to this/these specific service(s) in this specific case. The opposite may apply as well. In some cases GISS must ask itself whether the service can afford not to provide certain information.

The provision of information must be effected in accordance with the so-called 'third party rule', which says that information thus obtained may only be passed on to third parties if the service from which the information was obtained has given permission to do so. The Committee has established that GISS adequately implements the third-party rule with respect to information received from counterpart foreign services, both in policy and in actual practice.

GISS increasingly exchanges personal data and information with foreign intelligence and security services of which it is doubtful whether they satisfy the criteria for cooperation. This can be explained by the growing international threat of terrorism, causing GISS to consider it increasingly advisable to exchange information with foreign counterpart services, in certain situations even with services of which it is doubtful whether they satisfy the criteria for cooperation. The Committee points out that in practice GISS is allowing itself widening scope in its assessments in a certain area.

The Committee has established that in some cases GISS acted unlawfully when it provided personal data to foreign services. The Committee recommends GISS to be more careful about providing personal data to foreign services.

GISS cooperates with foreign services by the reciprocal provision of technical and other forms of assistance. It is the opinion of the Committee that GISS interprets the term assistance too narrowly. The Committee has established that a number of requests for assistance in the form of the exercise of special powers made by GISS to foreign services of which it is doubtful whether they satisfy the criteria for cooperation did not meet the statutory requirements of necessity, proportionality and/or subsidiarity.

GISS conducts joint operations with counterpart services with which it has a long-term cooperative relation. The Committee has not found any indication that GISS, when carrying out joint operations with counterpart services, failed to satisfy the conditions imposed by law and legislative history on such operations.

GISS also cooperates with foreign intelligence and security services in the context of security screenings. GISS is required to make reasonable efforts to try and obtain the information necessary to make a proper assessment. When carrying out a security screening, however, GISS may be dependent on information from a foreign service. In that case it is in the interest of the person concerned that GISS can cooperate with a foreign service for the purposes of the security screening.

Prior to cooperating for security screening purposes GISS must first assess and decide whether the foreign service satisfies certain criteria for cooperation. The Committee has established that GISS sometimes cooperates for security screening purposes with services of which it is doubtful whether they satisfy the criteria for cooperation, without first having gone through the required assessment and decision processes.

See section 14 of the review report for a detailed overview of the conclusions and recommendations of the Committee.

Review Report CTIVD no. 22A

On the cooperation of GISS with foreign intelligence and/or security services

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 cooperation of the Dutch General Intelligence and Security Service (further referred to as: GISS) with foreign intelligence and/or security services. A similar investigation is being conducted into the cooperation of the Dutch Defence Intelligence and Security Service (further referred to as DISS) with foreign intelligence and/or security services. A separate review report on the latter investigation will be published in due time. Pursuant to article 78(3), ISS Act 2002, the Committee informed the Minister of the Interior and Kingdom Relations and the Presidents of the two Chambers of the Dutch parliament of the intended investigations on 27 September 2007.

This report is accompanied by a classified appendix.

2. Organisation of the investigation

The Committee's investigation was directed at the cooperation of GISS with a large number of foreign intelligence and/or security services. In this review report the Committee devotes attention to the general standards that foreign intelligence and/or security services must meet before GISS is permitted to cooperate with a service or to continue or intensify an existing cooperative relation. The Committee will also discuss the intensity and the development of cooperative relations maintained by GISS and the different ways in which cooperation with foreign services takes shape in actual practice. GISS cooperates in different degrees of intensity with a large number of foreign services; contact is maintained with more than 170 foreign services. For this reason the Committee's investigation was conducted based on random checks.

In addition, the Committee carried out a more in-depth investigation of the cooperative relations of GISS with a limited number of counterpart services. This investigation devoted attention to some close cooperative relationships existing of old, to a number of more recent close cooperative relationships and to relations with foreign services that were set up fairly recently.

The Committee examined the files at GISS. The file examination related to the cooperation of GISS with foreign services in the period from early 2005 until mid-2008. However, the Committee's examination also included some files dating from before 2005 insofar as they related to GISS entering into new cooperative relations with foreign services or to important developments in cooperative relations. One file was investigated by the Committee right up to the moment when it prepared the present review report on 19 May 2009.

In addition to the file examination the Committee held a large number of interviews with officers of GISS, including lawyers, liaison officers, employees and managers of the Foreign Relations department, employees and managers of the various Directorates and the service management of GISS.

The review report has the following structure. Section 3 deals with the legal framework within which cooperation with foreign services must take place. Section 4 sets forth the responsibility of GISS for maintaining Dutch sovereignty. Sections 5 and 6 discuss the conditions set on entering into and maintaining cooperative relations with foreign services and how these are given shape in policy and practice at GISS. Section 6 also discusses a number of bilateral cooperative relations with foreign services. Sections 7 to 9 deal with various forms of cooperation – information exchange, assistance and joint operations. Cooperation for security screening purposes is the subject of section 10. Section 11 deals with multilateral cooperation in an institutionalized context. Section 12 deals with cooperation within the Kingdom of the Netherlands and section 13 with the coordination between GISS and DISS in the field of international cooperation. The conclusions and recommendations of the Committee are presented in section 14.

3. Legal framework

Cooperation by GISS with foreign intelligence and security services is governed mainly by article 59 , ISS Act 2002, the first paragraph of which provides that the head of the service is responsible for maintaining contact with the appropriate intelligence and security services of other countries. Article 59 distinguishes between two kinds of cooperation, namely the provision of information (paragraph 2) and rendering technical and other forms of assistance (paragraph 4). Pursuant to this article both forms of cooperation may only take place if the interests to be served by the foreign services are not incompatible with the interests to be served by the Dutch service and if the cooperation is not incompatible with the proper performance of its statutory tasks by the Dutch service.

According to the legislative history of the ISS Act 2002 the assessment whether a conflict of interests exists is based among other things on Dutch foreign policy, including human

rights policy.[2] Sometimes the interests to be served by GISS have been translated into expressly adopted government policy, for instance human rights policy, but often they have not. A multitude of interests is involved.[3] It is stated in both the law and its legislative history that GISS will perform its tasks in subordination to the law. This means that the interests to be served by GISS 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.[4]

An example mentioned in legislative history of a situation in which the proper performance of its statutory tasks by the Dutch service is incompatible with cooperation with a foreign service is the situation where cooperation would frustrate the own ongoing operations of GISS. It is also pointed out that the type of assistance that is requested is relevant, too. It must, among other things, fit within the legal parameters to be observed by GISS. If a certain form of assistance is incompatible with those parameters, it would be contrary to the proper performance of its statutory tasks by the service if GISS were to provide the assistance notwithstanding.[5]

Article 36(1)(d), ISS Act 2002, provides that GISS is authorized to supply information to the appropriate intelligence and security services of other countries. The Explanatory Memorandum to the Bill containing the ISS Act 2002 shows that providing information to foreign services under article 59, ISS Act 2002, must be distinguished from providing information under article 36, ISS Act 2002. If information is provided under the former article, the interest of the foreign service is the guiding principle, whereas the provision of information under article 36, ISS Act 2002, takes place in connection with the proper performance of its statutory tasks by the Dutch service.[6] It follows from the legal history of the ISS Act 2002 that where information is provided to a foreign service under article 59, ISS Act 2002, this usually happens after the foreign service has made a request for the information, without GISS having a direct interest in providing it. Such a situation occurs, for example, when GISS does an administrative check in a security screening for the benefit of a foreign service and provides the results to the service (see also section 10). When information is supplied under section 59, ISS Act 2002, the guiding principle is the wish to maintain a good cooperative relationship with the foreign service. If, on the other hand, GISS does have a direct interest in providing the requested information to the foreign service, the performance of its statutory tasks by GISS is the guiding principle and according to legislative history the information must then be provided under article 36, ISS

[2] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 74.
[3] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.
[4] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 65.
[5] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 64.
[6] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.

Act 2002. In most cases GISS provides information to foreign services under article 36, ISS Act 2002.

The provision of information is subject to the so-called 'third party rule', which says that information obtained from a counterpart may only be passed on to third parties if the service that originally provided the information has given permission to do so. This requirement has been incorporated in article 37, ISS Act 2002. According to the legislative history of the Act this rule is an essential condition for international cooperation:

> "If a service cannot rely on the service in the addressee country keeping the information secret and using it exclusively for its own information, there can be no question of any real cooperation between the services concerned. If a service gets the impression that the rule is not observed, it will stop or marginalize the exchange of information with that counterpart."[7]

Some intelligence and/or security services proceed on the basis of the 'third country rule', which gives a wider interpretation to the international rule. In principle the third country rule allows information originating from a foreign counterpart to be passed on between the intelligence and security services of the same country, unless the providing service has expressly precluded it. The ISS Act 2002 and its legislative history do not leave the Dutch intelligence and security services scope for applying the third country rule. So when a foreign service has thus obtained information from GISS and wishes to furnish this information to colleagues at another intelligence and/or security service of the same country, it requires the permission of GISS. The same applies in the Dutch situation. When GISS receives information from a foreign counterpart, it may only pass on this information to e.g. DISS if the foreign counterpart from which the information originates has given permission to do so.

Article 59(5) and (6) provide that technical assistance and other forms of assistance (article 59(4)), for example tailing and surveillance activities for the benefit of a foreign counterpart, may only be rendered with the permission of the Minister of the Interior and Kingdom Relations. The Minister may only grant the head of the service a mandate for giving such permission with respect to requests of an urgent nature (for example cross-border tailing and surveillance activities), with the proviso that the Minister must be informed immediately of any permission granted. According to the legislative history, power to give permission to render technical and other forms of assistance has been vested at this (high) level because of the potential political aspects that may be attached

[7] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 57.

to rendering assistance.[8] If the Minister has given permission to assist a foreign service, the assistance is rendered by GISS under the responsibility of the Minister. It is not permitted to authorize a foreign service to operate independently on Dutch territory.[9] In principle, responsibility for intelligence activities on Dutch territory has been placed with the Minister of the Interior and Kingdom Relations and GISS. Responsibility for activities involving places in use by the Ministry of Defence lies with the Minister of Defence and DISS.[10]

It is mentioned in the legislative history of the Act that it has been agreed that GISS will maintain contact with civil intelligence and/or security services and DISS with defence intelligence and/or security services and with signals intelligence service. The heads of GISS and DISS will inform each other when they need to contact defence or civil services, respectively.[11]

4. Maintaining Dutch sovereignty

Activities of foreign intelligence and security services on Dutch territory that take place without the knowledge and involvement of GISS violate Dutch sovereignty.[12] According to legislative history the deployment of foreign agents on Dutch territory is only permitted if permission has been granted by the Minister of the Interior and Kingdom Relations or by GISS on his behalf[13] and subject to the conditions attached to the permission. If permission is granted for the deployment of foreign agents on Dutch territory, the foreign agents are deployed under the responsibility of the Minister and under the direction of GISS. Such an operation must always be considered a joint operation, with the foreign service acting as an equal partner. It is the responsibility of GISS, moreover, to monitor the operational activities of the foreign agents and to check whether they operate in conformity with the conditions imposed.[14] If employees of foreign services fail to comply with the conditions and develop secret activities, GISS must initiate appropriate measures. As a last resort,

---

[8] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101 and no. 9, p. 37.
[9] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 38.
[10] The Act also provides for the possibility of DISS exercising special powers in spaces not in use by the Ministry of Defence, provided permission has been granted in consultation with the Minister of the Interior and Kingdom Relations. See articles 20(2), 22(2), 23(3), 24(2) and 25(3).
[11] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 73.
[12] See also CTIVD Review Report no. 14 on the investigation by GISS into unwanted interference by foreign powers (including espionage), *Parliamentary Papers II* 2006/07, 29 924, no. 18 (Annex). Available in Dutch at www.ctivd.nl.
[13] In the case of activities in places in use by the Ministry of Defence permission must be granted *mutatis mutandis* by the Minister of Defence or by the Director of DISS acting on his behalf.
[14] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 64.

employees of foreign services who undertake unauthorized activities may be declared *personae non gratae* or undesirable aliens.[15] This drastic measure is taken only in very rare cases. Usually, GISS will take action against such behaviour in other ways, sometimes in collaboration with the Ministry of Foreign Affairs. In September 2008, for example, measures were taken against unwanted intelligence activities of the Moroccan intelligence service.[16]

The extent to which employees of foreign intelligence and security services on Dutch territory are monitored depends on the circumstances of the case. Among the factors determining the manner and degree of monitoring done by GISS are the gravity of the Dutch interests that may possibly be harmed, the intensity of the cooperative relationship maintained by GISS with the service in question and the proven reliability of this service in other fields. GISS will conduct targeted investigations into the activities of employees of foreign services that have given cause for doing so.[17]

In its monitoring of employees of foreign services GISS must seek a balance between the principle of trust on which cooperation between intelligence and security services is based and the importance of countering possible unwanted interference by these services. If GISS keeps too strict an oversight over the activities of employees of a foreign service in the Netherlands, it may harm the cooperative relationship with the service in question. If oversight is too limited, however, then GISS fails to meet its statutory responsibilities in this respect. Furthermore, when it is actually established that a foreign intelligence and/or security service is carrying out secret activities on Dutch territory and is thus violating Dutch sovereignty, it follows from legislative history that this fact precludes cooperation with the service concerned. The fact is that in such a case there is incompatibility with the interests to be served by GISS, which must be deemed to include safeguarding Dutch sovereignty, with the result that the foreign service in question no longer qualifies for cooperation.[18] In this situation it is important that GISS takes timely and appropriate measures.

GISS, in collaboration with DISS, has prepared a code of conduct for employees of foreign services, known as liaisons, who are stationed in the Netherlands. Liaisons have diplomatic status and are officially accredited with GISS. The code of conduct explains among other

---

[15] *Parliamentary Papers I* 2001/02, 25 577, no. 58a, p. 25.

[16] See for more information the letter from the Ministers of the Interior and Kingdom Relations and of Foreign Affairs to the Second Chamber about secret intelligence activities in the Netherlands, *Parliamentary Papers II,* 2008/09, 28 844, no. 25.

[17] CTIVD Review Report no. 14 on the investigation by GISS into unwanted interference by foreign powers (including espionage), *Parliamentary Papers II* 2006/07, 29 924, no. 18 (annex). Available at www.ctivd.nl.

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

things that under current Dutch law GISS is responsible for the activities of liaisons of foreign services who are in the Netherlands and that unmonitored activities of foreign liaisons may pose a threat to the national security of the Netherlands. The code also lays down rules for the conduct of liaisons and the performance of operational activities. Among other things liaisons are expected to inform GISS about their activities both on request and at their own initiative, to refrain from contacts which may result in a conflict of interests and to adhere to the instructions given by GISS and to Dutch law. Liaisons are issued with a copy of the Intelligence and Security Services Act 2002 (the ISS Act 2002). The code of conduct states explicitly that operational activities may only be performed on the condition that the head of GISS has been consulted and has given his permission and that the operational activities are performed in cooperation with and under the supervision of GISS. With regard to situations for which the code of conduct does not provide, a liaison must consult with the head of GISS. The Foreign Relations department of GISS is the primary contact for all foreign liaisons.

Accredited liaisons of foreign services are not the only persons who may be performing secret activities on Dutch territory. It does happen that employees of foreign services are active in the Netherlands but are not accredited with GISS. Also, foreign services sometimes try undertaking activities from outside the Netherlands which may result in violation of Dutch sovereignty.[19]

The Committee's investigation has shown that there is unwanted interference in the Netherlands by several foreign intelligence services, also by services with which GISS is cooperating more or less intensively. GISS regularly investigates indications of possible interference by foreign intelligence services and in certain cases conducts broad or in-depth investigations into unwanted activities. After identifying sovereignty violations by intelligence services of other countries, GISS usually takes timely action and appropriate measures tailored to the situation.

5. Criteria for cooperation

Article 59(1), ISS Act 2002, imposes on the head of GISS a duty to maintain contact with the appropriate intelligence and security services of other countries. Proper cooperative relations with foreign services are essential for the adequate performance of tasks by GISS. They are essential because the information obtained by such cooperation considerably extends the information position of GISS and thus increases its capability to assess national

[19] See also the Annual Reports for 2008 and 2007 of GISS, which are available at www. aivd.nl.

security risks and give the responsible authorities timely warning.[20] It is especially since the attacks of 11 September 2001 that the need for international cooperation of intelligence and security services has emerged more clearly and the willingness to cooperate increased accordingly.

Cooperative relations between GISS and foreign services differ from one counterpart service to the next and are often liable to change. Cooperation is usually largely a matter of exchanging information. In addition, joint operations are carried out with certain counterparts and technical and other forms of assistance rendered. In addition, meetings of experts are held, for example of lawyers, technicians and other experts. Besides, services cooperate in the field of personnel education and training. The intensity and the frequency of cooperation within the different bilateral relations of GISS vary widely. A distinction can be made, for example, between cooperative relations of a mainly formal, ad hoc, tactical or operational nature. GISS may also cooperates closely with a foreign service in one specific area of activity while in other areas it exercises restraint.

In some cases cooperative relations have been institutionalised in more or less formal cooperative groups, in which intelligence and security services of various countries participate. These institutionalised multilateral cooperative groups will be discussed in greater detail in section 11.

According to legislative history it is as a rule the responsibility of the head of GISS to decide with which foreign services GISS will cooperate and how closely. The Minister of the Interior and Kingdom Relations must be informed of any cooperation and in the case of high-risk counterparts the decision-making must be submitted to the Minister. According to the legislature the rationale for this rule is that in the light of Dutch foreign policy, in which human rights constitute an essential factor, cooperation with high-risk counterparts may acquire an extra dimension calling for explicit political decision-making.[21]

In 2005, in reply to questions from a member of Parliament, Van der Laan (D66), the Minister of the Interior and Kingdom Relations (when an amendment to the ISS Act 2002 was discussed in parliament) explained the general requirements for cooperation with a foreign intelligence or security service:

> "Cooperation takes place within the legal parameters and with due observance of Dutch foreign policy, including human rights policy. Prior to entering into a cooperative

[20] *Parliamentary Papers II* 1997/98, 25877, no. 3, pp. 73-74.
[21] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 102 and *Appendix to the Proceedings II (Aanhangsel Handelingen II)* 2004/05, no. 749.

relation with a foreign intelligence or security service a number of matters are investigated. Inquiries are made as to the service's democratic anchorage, its tasks, professionalism and reliability. It is examined whether international obligations make cooperation advisable and to what extent it may assist the Dutch services in the proper performance of their statutory tasks. These factors are assessed together and in context. Based on this assessment it is decided whether GISS is going to cooperate and if so, what will be the nature and intensity of the cooperation. As is usual in international dealings, the relationship may range from intensive cooperation at case level to contacts that are in principle purely formal."[22]

Earlier, in 1996, the issue of cooperating with foreign services was discussed in the Intelligence and Security Services Committee of the Second Chamber of Parliament (The ISS Committee).[23] It was stated then that the potential degree of reciprocity also played a role in the cooperation with foreign services. [24]

The various criteria for cooperation will now be discussed in greater detail.

5.1 Democratic anchorage and respect for human rights

Democratic anchorage and respect for human rights of a foreign service must play an essential role in decision-making about entering into and maintaining relations with that service. This follows naturally from article 59, ISS Act 2002, which provides among other things that cooperation with foreign intelligence and security services will only take place if the interests served by them are not incompatible with the interests to be served by GISS, which include the standards, and certainly also the fundamental and human rights standards, laid down in the Constitution and international conventions ratified by the Netherlands.

Whether or not a service has sufficient democratic anchorage depends on a number of factors. One can look, for example, at the general political system of the country in question and the position of the relevant service within the system, the statutory powers of and the (independent) oversight over the service. With regard to the criterion of respect for human rights it can be investigated whether the country in question has ratified

---

[22] *Appendix to the Proceedings II (Aanhangsel Handelingen II)* 2004/05, no. 749.

[23] The ISS Committee is currently constituted of the chairpersons of the political parties represented in the Lower House, with the exception of the chairpersons of breakaway groups that split off during the current parliament. The chairperson of the Socialist Party (SP) has also joined the IVD Committee from 1 May 2009.

[24] *Parliamentary Papers II* 1996/97, 25 418, no. 1, p. 2. The legislative history of the ISS Act refers to this document: see *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 63.

international human rights conventions and whether it observes these conventions in actual practice. It is also significant whether a foreign counterpart is being associated or has been associated with human rights violations. This can be investigated, for instance, by looking for mention of human rights violations in investigation surveys and reports of national and international human rights organisations.

In its report De AIVD in verandering [GISS in transition] the Committee for the Administrative Evaluation of GISS (Havermans Committee) made the following observation on how GISS applied the criteria of democratic anchorage and respect for human rights:

> "These criteria are not sacrosanct, though, and it is possible to distinguish between different levels of cooperation. In some cases obtaining certain information may be more important than adhering to such criteria. Due to the current threat of terrorism these principles have become less dominant. Sometimes, the present diffuse threat situation calls for contacts with services that do not meet all the requirements."[25]

It is the opinion of the Review Committee that GISS should exercise utmost restraint in cooperating with services of countries that have no or hardly any tradition of democracy and where human rights are violated (on a structural basis). In actual practice, however, precluding all and any cooperation with such services in advance could lead to undesirable and even disastrous situations. If such services possess information relating to a direct (terrorist) threat, it must be possible for GISS to apply to the services in question for information. Likewise, when GISS possesses indications of a concrete threat to another country, then for the purpose of preventing innocent victims it may be necessary to share information with the service or services concerned. This requires some degree of contact, albeit limited, between GISS and such services. The position that all cooperative relationships must be precluded in advance is indeed not supported by the ISS Act 2002 or its legislative history.

In his reply to Van der Laan's questions already cited above, the Minister discussed the use of information from foreign services that may have been obtained by torture. The Minister spoke of a differentiated approach to the issue of cooperating with foreign services: close cooperation with one service, while contacts with another service are purely formal. The Minister continues:

> "One of the reasons to opt for this differentiated approach is that in actual cases it is impossible to find out whether information received from a foreign intelligence and

[25] *Committee for the Administrative Evaluation of GISS, De AIVD in verandering,* November 2004, p. 113.

security service may perhaps have been obtained by torture. Intelligence and security services keep their sources and their methods secret, also in their mutual dealings. Moreover, a service will never say they obtained information by torture. This uncertainty, however, may not result in the absolute preclusion in advance of all forms of cooperation with certain services. In a situation in which such a service possesses information concerning an immediate threat of a terrorist attack, such a preclusion could have disastrous consequences. We must therefore always keep communication channels with the appropriate services open."

The Committee shares the view that in an actual case it is virtually impossible for GISS to find out whether information coming from a foreign intelligence or security service was obtained by torture. This makes it all the more important that GISS, before cooperating with a foreign intelligence or security service, assesses carefully to what extent the human rights situation in a country constitutes an obstacle to cooperation with the relevant service of that country. Besides, as the cooperative relation continues or changes, GISS will have to keep addressing the question up to which level it may cooperate with such a service and whether the intensity of the cooperative relation is not incompatible with the interests to be served by GISS. GISS must also be alert to possible side effects of cooperation, since it is not known how these services handle information obtained from GISS. If GISS suspects that a foreign service is using or will use information provided or to be provided by GISS for unlawful purposes, GISS must refrain from providing (further) information. Likewise, if GISS actually has concrete evidence that information obtained from a foreign service was obtained by torture, it will have to refrain from using this information. GISS will then have to terminate the substantive cooperation with the foreign service. It is only in highly exceptional emergencies that GISS may (or even must) depart from this rule. The Committee has not come across such a situation in its investigation.

The Committee has found that it is not always simple to assess whether an intelligence and/or security service of another country sufficiently satisfies the criteria of democratic anchorage and respect for human rights. It may happen that a foreign counterpart is careful about the rights of citizens, has clearly defined statutory powers and is at the same time controlled directly by and reports exclusively to the head of state in a country that has virtually no democracy. It may also happen that there are indications of human rights being violated in a country having a long-term democratic tradition. It is therefore not simply a matter of adding up a number of factors. For each foreign service GISS must make a well-considered assessment, not only when entering into a cooperative relation but also while an existing cooperative relation is intensified or changes in nature.

5.2 Tasks, professionalism and reliability

The duties and responsibilities assigned to a foreign counterpart are an important factor in the assessment whether or not to enter into or intensify a cooperative relationship with the service. It is important, for example, to examine whether the foreign counterpart is an intelligence service that is predominantly externally oriented (towards collecting (political) information), a security service that is more internally oriented (towards identifying threats to national security to enable measures to be taken), or a combination of the two. In this context the difference between defence services and civil services is also relevant. Other factors that must also be weighed are the actual powers of a service, e.g. operational and executive powers, and whether or not a service, in addition to intelligence and/or security tasks, has investigative tasks as well. These factors determine the working methods of a foreign counterpart and may for example have consequences for the manner in which it will handle information provided by GISS.

The degree to which a foreign counterpart may be considered professional and reliable depends largely on the experience gained by GISS during its cooperative relation with the service in question. At the time of entering into a cooperative relation this criterion will therefore be less useful and will be difficult to apply, although GISS does in this context exchange views and experiences with other (friendly) counterparts, which may be helpful when assessing whether a foreign service is professional and reliable. Professionalism and reliability of a counterpart service are also important factors in the decision process whether or not to intensify cooperation with the service. If there are indications that a counterpart operates unprofessionally, GISS cannot and may not count on this counterpart adhering to the agreements they have made. In that case their cooperation can be no more than superficial.

The Committee has found that the foreign services with which GISS maintains the closest cooperative relations are generally assessed to be highly professional and sufficiently reliable. The Committee draws attention to the fact that the assessment of the professionalism and reliability of a counterpart may be influenced by the person at GISS who does the assessment. In some cases intuitive factors, such as personal preferences, sympathies, recognisability and a sense of trust are more decisive than factual circumstances such as the expertise and technical capabilities of a service, the speed and carefulness with which information is exchanged et cetera. Furthermore, the person making the assessment does not always pay sufficient attention to the distinction between intelligence services and security services or to such tasks and responsibilities of a foreign service as can be objectively established. These observations of the Committee confirm a number of findings which, moreover, had already been made at GISS, too.

5.3 Advisability in the context of international obligations

According to the legislative history of the ISS Act 2002, Dutch foreign policy is one of the factors in assessing whether cooperation of GISS with a foreign intelligence or security service may involve a conflict of interests.[26] International obligations arising, for example, from membership of an international organisation or from international conventions ratified by the Netherlands must also be counted among the interests to be served by GISS. When entering into and maintaining contacts with foreign counterparts GISS must assess whether the international obligations of the Netherlands make it advisable to cooperate with the services in question.

The legislative history of the ISS Act 2002 shows that cooperation with foreign counterpart services of so-called 'high-risk countries' may, in the light of the foreign policy conducted by the Netherlands, have an additional dimension which calls for express political decision-making. According to the legislature it is evident that such a situation must be submitted for a decision to the responsible government member, in this case the Minister of the Interior and Kingdom Relations, and is not at the sole discretion of the head of GISS.[27]

The question arises whether cooperation of GISS with a counterpart service is possible if the Netherlands does not maintain diplomatic relations with the country in question, or if the international obligations of the Netherlands even preclude maintaining diplomatic relations with the country. The Committee considers that it may be in the interest of national security to keep the lines of communication with all foreign services open. In exceptional cases, moreover, when the usual diplomatic channels are closed, so-called 'silent diplomacy' may provide a solution. Usually, such 'silent diplomacy' is possible because of the contacts between intelligence and security services. One must not lose sight, however, of the fact that the services are bound by the parameters and restraints set by law. Keeping open the lines of communication with a specific foreign service does not mean that GISS may immediately start cooperating with it on a substantive level, for example by providing information in the context of the performance of its statutory tasks.

5.4 Enhancing the performance of its statutory tasks by GISS

According to the legislative history of the ISS Act 2002, the adequate performance of its statutory tasks by GISS requires it to cooperate with counterpart services where this is

[26] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 74.
[27] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 102.

possible.[28] When entering into or maintaining a cooperative relation with a foreign intelligence or security service GISS must therefore examine to what extent the cooperative relation benefits or may benefit the performance of its statutory tasks by GISS, as described in article 6(2), ISS Act 2002.

In principle GISS cooperates with a foreign intelligence and/or security service in the fields in which GISS and the foreign counterpart have interests in common. In his reply to questions from member of Parliament Van der Laan cited above in section 5, the Minister of the Interior and Kingdom Relations said:

> "Cooperation is different for each country and each service and is limited to fields in which the Dutch and the foreign services have common interests."[29]

It is the opinion of the Committee that the view, expressed by the Minister in this passage, that cooperation is limited to fields in which GISS and the foreign services have common interests, is contrary to the text and the purport of the Act. The fact is that in certain circumstances the Act allows GISS to provide information or render technical or other forms of assistance exclusively for the purposes of the interests to be served by the foreign counterpart, without the interests of GISS being served thereby. The guiding principle in this case is not the performance of tasks by GISS, but the interest that the foreign service has in cooperating. In this situation the cooperative relationship with the service in question and maintaining this relationship come first. Article 59 does, however, impose a restrictive condition, namely that the cooperation with a foreign intelligence and/or security service may only take place insofar as it is not incompatible with the interests to be served by GISS and the proper performance of its statutory tasks by GISS does not preclude the cooperation. These points will be discussed in greater detail in the sections on information exchange (section 7) and on technical and other forms of assistance (section 8).

5.5 Quid pro quo

GISS cooperates with foreign services on the basis of the principle of *quid pro quo* or reciprocity. The basic principle is, to put it briefly, 'one good turns deserves another' and this is a maxim that applies in the world of intelligence and security. In the course of the legislative history of the ISS Act 2002 it has been stated that requests for information from foreign services must in principle be met with a positive attitude, in order to remain sufficiently ensured that requests for information made by GISS to the foreign services will

[28] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.
[29] *Appendix to the Proceedings II* 2004/05, no. 749.

meet with a similar attitude.[30] Complying with the requests from a foreign service thus serves the own national security, albeit indirectly.[31] This is the background of the authority of GISS to provide information and render assistance exclusively for the purposes of the interests served by a foreign service. The principle of reciprocity thus constitutes the basis for good international cooperation. Insofar as and wherever this is possible, intelligence and security services will assist each other. For GISS, the limits to such assistance lie in any case there where rendering assistance would be incompatible with the interests to be served by GISS and the proper performance of its statutory tasks by GISS.

Within these statutory restraints GISS must nevertheless guard against going too far in meeting requests for information from foreign counterparts. The fact is that it could lead to GISS having little new information to offer, so that it will be unable to exchange information until it has built up its store of information again. Keeping track of the quid pro quo balance – the quantitative and qualitative proportion between information provided and information obtained - is therefore essential for GISS's ability to determine its own position relative to that of counterparts. The quid pro quo balance also enables GISS to assess the added value of a cooperative relation and the extent to which the cooperation must be adjusted in order to achieve the intended proportion in the cooperative relation.

Taking stock of and monitoring the *quid pro quo* balance is a difficult task. It is difficult to determine in a quantitative sense how much is provided to or obtained from a particular counterpart. GISS cooperates with foreign counterparts in many different fields and on different levels. In addition to a quantitative assessment, it must also make a qualitative assessment. In doing so, GISS must assess the content of the information provided or received and its reliability as well as the importance attached to it by GISS at the correct level.

The Committee's investigation has shown that GISS has perceived that the *quid pro quo* balance could be put to better internal use. It is advisable, for example, to use an unambiguous weighting and assessment system that would make it possible to determine the proportion between what has been provided and what has been obtained in a particular cooperative relation. It is difficult, however, to develop a practicable and comprehensive method for doing this. It is also advisable to make the *quid pro quo* balance clearer and more accessible for employees so that the different teams within GISS can make more targeted and deliberate choices in their cooperation with foreign services, which will not only serve the interest of the team but also the interest of the service as a whole. GISS' intended objective of making better use of the *quid pro quo* balance is to

[30] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 74.
[31] *Parliamentary Papers I* 2001/02, 25 877, no. 58a, p. 24.

make its cooperation and information exchange with foreign counterparts more purposive. GISS recently initiated some policy reforms to achieve this. The Committee applauds these initiatives. It notes that the initiatives underline the need for a central department, capable of keeping track of the cooperative relations and of adjusting them where necessary. GISS has allotted this role to the Foreign Relations department. The Committee will discuss this subject in greater detail in section 6.3.

6. Cooperation with foreign services

6.1 Policy and practice at GISS

Within GISS, the task arising from the responsibility of the head of GISS to maintain contact with intelligence and security services of other countries (article 59(1), ISS Act 2002) has been delegated to the Foreign Relations department. One of the tasks of this department is to make new contacts with foreign counterparts and maintain and develop existing bilateral cooperative relations. For this purpose it is important for the Foreign Relations department to have an overall picture of the cooperation with foreign counterparts so that it can, where necessary, adjust cooperative relations and monitor cooperation quality (see further section 6.3 below). The Foreign Relations department is not responsible for determining the policy of GISS in the field of international cooperation but it does make a contribution to this policy. For example, the department frequently develops policy proposals and takes other initiatives. On the other hand, the Foreign Relations department is (co-)responsible for the implementation of international cooperation policy.

The policy of GISS on cooperation with foreign intelligence and security services is for the most part prepared in the Foreign Relations Consultative Body *(Buitenland Beraad)*, a consultative body in which all directorates of GISS are represented. This service-wide consultative body advises the management of GISS on developments and incidents occurring in bilateral cooperative relations with foreign counterparts. It also shapes policies on developments taking place in the context of international policy talks and European cooperation and, where necessary, advises the service management in these fields. Ultimate decisions are taken by the management of GISS. In some cases the Minister of the Interior and Kingdom Relations is informed, for example about concrete cases of cooperation with services of which it is doubtful whether they satisfy the criteria for cooperation or about other cases that are politically sensitive.

Especially in the past few years many policy innovations or policy revisions in the field of international cooperation were initiated at GISS. In the course of the process GISS noticed

among other things that there is insufficient consistency, service-wide, in the cooperation with various foreign intelligence and security services. GISS devoted attention, among other things, to designing a more strategic and targeted international cooperation policy, aimed at tighter monitoring and control of the implementation of the policy. When the Committee closed its investigation the policy adjustment process at GISS had not been fully completed yet.

GISS has not developed a decision-making procedure for entering into or intensifying cooperative relations with foreign services.[32] There is, however, a recent internal manual – compiled by the Foreign Relations department and a number of legal experts to be used in training new operational staff – which among other things comprises assessments that must be made before entering into or intensifying a cooperative relation.[33] This internal manual states that ultimately the head of GISS decides whether or not GISS may cooperate with a foreign service or whether a relation may be further developed. The internal manual does not make it clear whether the Foreign Relations department or the Foreign Relations Consultative Body plays a role in the decision process.

The internal manual is based on the assumption that GISS must in principle always keep open the possibility of cooperating. Cooperation with a counterpart should never be precluded in advance. According to the internal manual it depends on a number of factors whether GISS will cooperate, on which conditions it will do so and whether a relation will be further developed. The factors mentioned by the Foreign Relations department and the legal experts are the same as the criteria for cooperation emerging from the legal history of the ISS Act 2002 that were discussed above in section 5 of this report.[34] The internal manual states that all of these factors must be assessed with each individual factor carrying more or less weight. This weighting then results in a decision to cooperate or not to cooperate with the foreign service concerned or a decision to intensify or not to intensify the cooperation.

According to the internal manual the first step of the process must be a balancing of interests. It must be assessed to what extent GISS and the foreign service have interests in common and whether a conflict of interests exists or major specifically Dutch interests are involved. The outcome of the balancing of interests, so the internal manual continues, must

[32] Such a decision procedure exists exclusively for cooperation in the field of security screenings. For this purpose GISS has compiled information files for eight countries, containing an assessment if and to what extent it is permissible to cooperate with the services of the eight countries in question in security screenings. See section 10 for details.

[33] The assessments mentioned in this manual are for the most part identical with an older policy document of GISS (then called National Security Service) in the field of international cooperation dating from 2000.

[34] The criteria are the democratic anchorage and respect for human rights of the foreign service concerned, the tasks, professionalism and reliability of the foreign service, the advisability of the cooperation in the context of international obligations, enhancement of the performance of tasks by GISS and the principle of *quid pro quo*.

then be weighted against the other cooperation criteria. These other criteria are *inter alia* the democratic anchorage, the respect for human rights and the tasks, professionalism and reliability of the foreign service concerned. The outcome of the balancing of interests weighted against the other criteria determines the possible scope of cooperation between GISS and the foreign service concerned, in other words in which different fields GISS might cooperate with the counterpart. According to the internal manual this outcome is also decisive for the intensity of the cooperative relation. Intensity means how closely GISS may cooperate with the foreign service and what forms of cooperation are permitted. Finally, the rule applies that there are no eternal allies and no perpetual enemies.[35]

The Committee has investigated how and on what grounds decisions to enter into a cooperative relation in general or decisions to further develop a cooperative relation were in practice taken at GISS. The Committee's investigation has shown that in practice GISS often does not make the general assessments for entering into a cooperative relation mentioned in the internal manual or does so only to a limited extent. Decisions regarding the possibilities of commencing cooperative relations with foreign services are not made on a structural basis and for each foreign service individually. With respect to the foreign services with which GISS has entered into a cooperative relation since 2001[36], GISS has insufficiently assessed the extent to which these services meet the criteria for cooperation and, consequently, the maximum scope and intensity permitted for the cooperation. With respect to cooperative relations that have been intensified since 2001, GISS likewise did only limited assessments using the weighting factors for cooperation. There is no overview of foreign services, accessible to GISS staff, giving information about the specific characteristics of the services concerned, the issues to be addressed regarding the possibility of cooperating with them and about how and on which conditions they may cooperate with these services. It is true that there are so-called information files for a number of countries and services which contain such information. But these were compiled with a view to cooperation for security screening purposes (see section 10) and are limited to a very small number of countries.

The Committee has found that in concrete operational cases GISS does assess whether a specific way of cooperating with a specific service in a particular situation is permissible. It does so, for example, when a target of GISS has contacts in another country and GISS wishes to obtain more information on these contacts. Another example is the situation that a target of GISS travels abroad and GISS wishes to keep track of the target's activities

---

[35] "*We have no eternal allies, and we have no perpetual enemies. Our interests are eternal, and it is our duty to follow them.*", Palmerston, Henry John Temple.

[36] The Committee mentions this year because of the influence which the events of 11 September 2001 had and still have on intelligence and security services and the cooperation between the services. The powers of the Committee came into effect from 29 May 2002, the date on which the ISS Act entered into force.

abroad. In such cases GISS usually assesses whether in the specific case it is permissible to request the foreign service of the country in question to provide information based on the personal data of the target. In some cases GISS also makes assessments regarding certain forms of cooperation, for example the possibility of starting joint operations with a particular foreign service. It is the opinion of the Committee that GISS rightly includes the circumstances of the specific case in its assessment whether cooperation is permissible in a particular situation. The Committee draws attention, however, to the fact that the procedure of exclusively making such *ad hoc* assessments is too limited and may have undesirable consequences.

With such an *ad hoc* assessment approach, decisions whether or not to cooperate or cooperate more closely with foreign services in a particular case are not taken consistently on the basis of the same assessments and are taken at different levels. In most cases the decision will be taken by a processor, analyst or team leader, in other cases the decision will be taken in consultation with the director concerned and in some cases the decision process will go all the way up to the management of GISS. This may result in differences between the various teams and directorates of GISS as to the extent to which cooperation or certain forms of cooperation with particular foreign services are considered permissible and will therefore take place. It may also mean that comparable foreign services are assessed differently. Furthermore, it may happen that assessments made by a team, for example about requesting a foreign service for assistance, are inconsistent with similar assessments made at a much higher level, for example about rendering assistance to the same foreign service (see also section 8).

The Committee's investigation has further shown that where the possibility of cooperating with a particular foreign service in a specific situation is assessed at team level, the direct operational interests of the team sometimes predominate too much over other factors that should also play an important role. In some cases teams pay hardly any attention to other aspects of the cooperation which should in fact be considered, such as the respect for human rights or the reliability of the service with which the team wishes to cooperate. In other words and returning to what is said in the internal manual of GISS, it seems that teams often do in fact balance the interests involved in a concrete case. But subsequently the result in the actual case is insufficiently examined against all the other, more general criteria for cooperation which include the democratic anchorage, respect for human rights and the tasks, professionalism and reliability of the foreign service concerned and the advisability of cooperating with it in the context of international obligations (see also section 5).

The Committee considers it possible to overcome most of the aforementioned problems in the decision-making process on entering into or intensifying a cooperation relation. It is

the opinion of the Committee that GISS must first make a fundamental assessment of the extent to which the criteria set for cooperation are satisfied and must do so at management level and for each individual foreign service separately. For each foreign service with which GISS cooperates it must be assessed to what extent the service may be considered professional and reliable, to what extent the service is democratically anchored, to what extent it respects human rights and so on and so forth. It must also be laid down, supported by reasons, which forms of cooperation are in principle permissible. In this way a careful and identical assessment is made for each of the different foreign services of the extent to which cooperation with them is permissible.

Subsequently, when a concrete (operational) case arises, the result of balancing the various interests involved can be examined against the general assessment of the foreign service. This method ensures that concrete operational interests are assessed in the context of the general assessment of the counterpart service already done previously on the basis of the cooperation criteria. At the same time this will have the result that teams deciding independently in an actual situation whether they may cooperate with a foreign service, for example by providing information or starting a joint operation, must ensure that their decisions are in keeping with the prior assessment of the extent to which cooperation with the service is in principle permissible. If a team wishes, for compelling reasons, to carry cooperation with a particular counterpart further than is in principle permitted, thus giving rise to an exceptional situation, a reasoned decision on the matter will have to be taken at management level.

It is the opinion of the Committee that this system will do justice to both the restraints on cooperation with foreign services set forth in the law and legislative history, and daily practice in which actually cooperating with a counterpart may be essential to the adequate performance of its statutory tasks by GISS. The Committee observes in this context that this is not and indeed should not be a static process. While a cooperative relation with a foreign service continues and develops, GISS may at any time adjust the assessment of the service in question. But it must do so on the basis of the generally applicable criteria for cooperation, supported by reasons and at the proper level.

The Committee is aware that GISS may find itself in a situation in which it has an opportunity to start cooperating (operationally) with a foreign service in a specific case at short notice. Such an opportunity may occur *ad hoc*, without involving any intention of structural cooperation. Great interests may be involved, moreover. If no cooperative relation with the foreign service in question exists yet at that moment, it may be difficult for GISS to make a thorough and full assessment, within a period of time that may sometimes be very short, of the extent to which the foreign service meets the applicable criteria for cooperation and consequently of the forms of cooperation that are permissible.

Nonetheless, the Committee takes the position that GISS must nevertheless make such an assessment. If it proves impossible in such a case to obtain an adequate picture of one or more aspects of the foreign service in question, these uncertainties must be identified and included in the assessment. If it appears that certain criteria for cooperation are not satisfied or if it is uncertain whether they are satisfied, this means in the opinion of the Committee that in principle certain forms of cooperation, such as providing personal data, rendering assistance and carrying out joint operations, are not permissible. If GISS wishes to carry the cooperation further than is in principle permitted in the specific case, the cooperation must in that specific case be founded on compelling (operational) interests that justify the cooperation and the Committee holds that it must be preceded by a reasoned decision of the service management. The Committee further holds the opinion that GISS should prevent such specific cooperation from setting a precedent and becoming the norm instead of the exception. Any future cooperation with the foreign service in question must again be examined against the general assessment of the criteria for cooperation and the forms of cooperation thus considered permissible.

The Committee recommends GISS to put in place a decision-making procedure for entering into or intensifying cooperative relations with foreign services that will ensure that the fundamental assessment of the extent to which the applicable criteria for cooperation are satisfied is carried out at management level for each foreign service individually.

6.2 In-depth investigation of a number of cooperative relations

In addition to the investigation by means of random checks of the cooperation of GISS with foreign intelligence and security services, the Committee conducted in-depth investigations of a number of cooperative relations maintained by GISS. For this purpose the Committee devoted attention to some close cooperative relationships existing of old, to a number of more recent close cooperative relationships and to relations with foreign services that were set up fairly recently. The Committee investigated the cooperation of GISS with both intelligence services and security services.

6.2.1 Close cooperative relationships existing of old

GISS cooperates with these counterparts in virtually all its working areas. It cooperates with the services at various levels, operational and analytical as well as more policy-oriented. In a number of fields or issues GISS cooperates very closely with these services.

Obviously these are fields or issues in which both services have concrete intelligence or security interests and with respect to which they usually apply similar methods or views and/or possess complementary (technical) capabilities.

The Committee has found that by its nature GISS cooperates more smoothly with security services than with intelligence services. Cooperation with security services often concerns security interests shared by the two services and there is usually a certain degree of interdependence. Partly for these reasons, in the practical sense the cooperation generally proceeds without serious problems and as a rule the cooperation balance is fairly stable. Few problems can be identified in the cooperation and the two counterparts take an open attitude towards each other.

Cooperation with intelligence services on the other hand shows more ups and downs. The *quid pro quo* principle[37] very much dominates these cooperative relations with the result that the possibility of achieving cooperation with another intelligence service is determined to a great extent by what GISS has in the offering, in other words by its own information position. In addition to the common interests the two services, other and sometimes conflicting interests may play a role which affect the cooperative relation. Maintaining a balanced cooperative relation with these services requires a more strategic approach on the part of GISS. The Committee's investigation shows that GISS is increasingly devoting attention to this aspect of its relations with certain foreign intelligence services.

6.2.2 Close cooperative relations of a more recent nature

The Committee investigated cooperative relationships with foreign services that are (or can be) very close in certain investigation areas, while there is no long-term tradition of cooperation with these services. Cooperation with these services takes place in a more limited number of fields and issues and consists mainly of operational and analytical cooperation.

In recent years the cooperation with these foreign services has increased considerably, both in intensity and in volume. Cooperation in this category is characterized, however, by a lower degree of trust and openness than in the category of foreign services discussed above. Partly as a result of this, problems or incidents that arise have a greater influence on the cooperative relation than in cooperative relations in which there is considerably greater trust and openness. For this reason it is all the more important to maintain a

[37] "One good turn deserves another", also known as the principle of reciprocity.

comprehensive overview of all aspects of cooperation throughout the service and to make adjustments where this is necessary.

The Committee considers that for some of these foreign services it may be open to doubt whether they satisfy one of the criteria for cooperation. For example, GISS may deem a foreign service less than reliable in some respects or hold that a counterpart has only limited democratic anchorage in the government system of its country. At the same time, however, it has no indications that it must be doubted whether these services meet the other criteria for cooperation. Moreover, the experience meanwhile gained by GISS in these cooperative relations has shown that these counterparts give effect to the cooperation in an adequate manner. In the fields in which GISS does cooperate with them it has a great interest in the cooperation.

6.2.3 Cooperative relations of relatively recent date

The Committee investigated a number of cooperative relations which recently showed quite considerable growth in a relatively short time. It is true that with some of these services GISS had already been in contact for some time, but cooperation with them never really got going in the past. It was particularly after the attacks in the United States in 2001 and after the Madrid attacks in 2004 that cooperation with these services was further developed. GISS increasingly cooperates operationally with these services and exchanges information or personal data with increasing frequency. Initially, cooperation with these services increased in the field of counterterrorism. This is indeed understandable since fighting cross-border terrorism entails a certain need for international cooperation. The Committee has found, however, that the cooperation of GISS with these foreign services is also increasing in other fields and areas of special attention.

As regards the cooperative relations investigated by the Committee, it is questionable to what extent the foreign services concerned meet the criteria for cooperation set out in legislative history. In particular there are doubts about the democratic anchorage of the foreign services concerned and doubts about the extent to which they respect human rights. As was discussed in section 6.1 above, the Committee considers it necessary that GISS makes a thorough assessment, for each of these cooperative relations, of the extent to which the criteria for cooperation set out in legislative history are satisfied.

6.3 The role of the Foreign Relations department

As stated above in section 6.1, within GISS the task arising from the responsibility of the head of GISS to maintain contact with foreign intelligence and security services has been delegated to the Foreign Relations department. This means that it is an important task of this department to (help) develop, maintain and safeguard the quality of these cooperative relations.

The Committee has established that in practice the role of the Foreign Relations department is chiefly a facilitating one. Among other things the department acts as point of contact for foreign liaisons stationed in the Netherlands and for GISS liaisons stationed abroad (see section 6.4). Teams and departments that cooperate with foreign services can ask the Foreign Relations department for further information on the services concerned or obtain advice. Where necessary, the Foreign Relations department consults the legal experts of the Legal Department. The Foreign Relations department has e.g. compiled so-called information files on a small number of services which can be used in connection with cooperation for security screening purposes, which contain supplementary information that employees can consult. Moreover, staff members of the Foreign Relations department are present at certain meetings with counterparts, and internal policy prescribes that the department must be informed about any other meetings held with counterparts. Messages and requests received at GISS or sent to foreign services are usually seen by the department. In this way the Foreign Relations department tries to keep informed of the different relationships maintained by GISS with counterparts.

In performing its tasks the Foreign Relations department depends partially on the provision of information by and the cooperation of others. The Committee's investigation has shown that the teams and departments at GISS which cooperate with foreign services do not or did not always proceed expeditiously in informing the Foreign Relations department of their cooperation activities. The Committee has noticed some improvement on this point, though. However, involving the Foreign Relations department in, or adequately informing it of cooperation activities is still not an automatism in all cases. It is the opinion of the Committee that doing so should be automatic procedure.

Following naturally from the task of discharging the responsibility to maintain cooperative relations, the Foreign Relations department also has an important responsibility, wherever this is necessary, in bringing cooperation relations with foreign services into line with the policy in this field as formulated at GISS. In order to be able to do so the department must on the one hand have a sufficiently clear picture of the intensity of and the balance in the cooperative relations with these services. On the other hand it is important that the Foreign Relations department provides the various teams and departments with sufficient

(proactive) steering and makes sure that the service-wide cooperation policy is implemented. A strong position of the Foreign Relations department in this matter can lead to uniformity in the cooperation of the teams and departments with foreign services. The Committee has found that in practice the steering role of the Foreign Relations department has not taken shape sufficiently.

The Committee points out that GISS recently prepared a number of rather critical policy documents which (among other things) addressed this subject. GISS noted e.g. that incoming and outgoing messages from and to foreign services should be subject to more supervision, that a need was felt for keeping a better overview of cooperative relations with foreign services and that better insight into the *quid pro quo* balance was advisable (see also section 5.5). A central and steering role of the Foreign Relations department is an important tool with respect to these problem areas. The Committee considers it advisable that GISS, for internal use, expressly lay down the different areas of responsibility of the Foreign Relations department insofar as this has not been done yet, and recommends GISS to ensure that internal policies are adequately implemented in practice.

6.4 Liaisons

In order to improve the efficiency and effectiveness of its cooperation with foreign intelligence and security services GISS has stationed liaisons in twelve countries. Each liaison has a number of countries in his portfolio. Liaisons maintain contact with the intelligence and security services of the countries within their operational area. Liaisons stationed abroad are attached to the respective Dutch embassies and accredited in that capacity with the authorities of the country concerned. An agreement has been concluded with the Ministry of Foreign Affairs which regulates the position of the liaisons in this context. GISS also has two travelling liaisons who maintain contacts with a large number of foreign counterparts while operating from the Netherlands.

The tasks of liaisons and the focal points within the positions vary between stations. Some stations are primarily political-strategic in nature while at other stations the emphasis is on operational cooperation with the foreign counterparts concerned. Liaisons act in the first place as intermediaries in the relations of GISS with counterparts. In addition, liaisons play a role in drawing attention to developments, threats and new opportunities in their respective operational areas.

Within the GISS organisation the liaisons are part of and functionally managed by the Foreign Relations department. Each liaison has a staff member at the department who acts as his or her contact. The operational activities of the liaisons are geared as much as

possible to the needs of the teams in the different directorates of GISS. Operationally, the liaisons are managed mainly by means of concrete questions and instructions from the teams. Here, too, the Foreign Relations department plays a role. It is the policy at GISS that the relevant staff member of the Foreign Relations department is always involved in contacts between a team and the liaison. At the same time liaisons have a steering role with respect to the teams and in the cooperative relation with the foreign counterparts. Among other things this can take the form of the liaison adjusting and streamlining mutual expectations, looking at requests from the respective teams to counterparts and taking part in determining the approach or strategy to be adopted in the cooperation.

There are also liaisons of foreign counterparts who are stationed in the Netherlands. The Foreign Relations department is the primary point of contact for liaisons of foreign services on Dutch territory. Each liaison stationed in the Netherlands is issued with a code of conduct that has been drawn up by GISS and DISS jointly. The code contains rules stating which activities a liaison is permitted to undertake on Dutch territory. If a liaison wishes to carry out operational activities, the permission and involvement of GISS are absolute requirements. Liaisons are also issued with an English translation of the Intelligence and Securities Services Act 2002 (the ISS Act 2002). Secret operations (without the permission of GISS) of foreign services on Dutch territory were discussed above in section 4.

7. The exchange of information

7.1 Legal framework

GISS has authority to provide information to intelligence and security services of other countries pursuant to article 36(1)(d) and article 59(2), ISS Act 2002, respectively. Information is provided pursuant to article 36(1)(d), ISS Act 2002, in the context of the proper performance of its statutory tasks by GISS, as laid down in article 6(2)(2), of the Act. The provision of information pursuant to article 59(2) ISS Act 2002 is a different matter. In this case the guiding principle is not the performance of its statutory tasks by GISS, but the interest which the foreign service has in being provided with the information. Maintaining a good cooperative relation with the relevant foreign service comes first here. If GISS possesses information which may be important to a foreign service, but may not be provided under article 36(1)(d) ISS Act 2002, it is nevertheless possible - under certain circumstances - to provide the information under article 59(2) ISS Act 2002.[38] An example is the situation where a foreign service requests GISS to provide

[38] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101.

information on a person or organisation whom or which GISS is not itself investigating. In such a case GISS may – under certain circumstances – provide the requested information to the foreign service even though this does not contribute to the performance of its statutory tasks by GISS. In most cases, however, GISS provides information to foreign services pursuant to article 36(1)(d), ISS Act 2002.

Information may only be provided to foreign intelligence and security services within all of the applicable legal parameters. The legislature has set further criteria for the provision of information under article 59(2), ISS Act 2002. The same article provides that information may be supplied provided (a) the interests to be served by the counterparts are not incompatible with the interests to be served by GISS and (b) the proper performance of its statutory tasks by GISS does not preclude it. GISS performs its tasks in subordination to the law. This means that the interests to be served by GISS must be deemed to include the standards, and certainly also the fundamental and human rights standards, that are laid down in the Constitution and in the international conventions ratified by the Netherlands.[39]

The legislature has included general provisions on information processing in the ISS Act 2002, namely in articles 12 to 16. These articles lay down a general system of standards for GISS that must be observed in information processing (information processing is defined to include the provision of information).[40] For example, article 12(2), ISS Act 2002, provides that information processing is only permitted for a specific purpose and insofar as necessary for the proper implementation of the ISS Act 2002 or the Security Screening Act. Article 12(3), ISS Act 2002, provides that information processing must be done with proper and due care. Article 12(4) provides that information processed by GISS must be accompanied by an indication of the degree of reliability or a reference to the document or source from which the information has been derived. So GISS must also observe these standards when providing information to foreign intelligence and security services.
The legislature has made a clear distinction between *personal* data[41] and other information. This emerges clearly *inter alia* in the general provisions on information processing, which e.g. impose additional requirements on the processing of personal data. Pursuant to article 13(1) , ISS Act 2002, GISS may only process personal data relating to an exhaustive list of categories of persons set out in the same article 13(1). The distinction between personal data and other information is also manifest in the special provisions of articles 40 to 42, ISS Act 2002, pertaining to the supply of personal data to third parties. The legislative history of the ISS Act 2002 shows that the rationale behind this distinction

[39] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 65.
[40] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 18-19
[41] Personal data is data relating to an identifiable or identified, individual natural person, article 1(e), ISS Act.

is that even more than is already the case when GISS provides information in general, due care must be the prime consideration where it concerns the provision of personal data. This is all the more cogent if GISS provides information in the context of performing its statutory tasks with the aim of removing or reducing a detected threat. If the threat originates from a specific person, the provision of data relating to him may in practice result in measures being taken against him.42 Pursuant to article [42], ISS Act 2002, GISS must keep records of every provision of personal data, known as the records protocol.

The legislative history of the ISS Act 2002 also makes a distinction between personal data and other information where it concerns the provision of information to foreign intelligence and security services. According to the legislative history special care must be exercised in providing personal data. Only a limited number of senior managers of the service are authorized to decide to provide personal data. If GISS wishes to provide personal data to a service of a country whose observance of human rights may be doubted, these personal data may be provided only if and to the extent that it is inevitable to do so in order to prevent innocent citizens from becoming victims of a terrorist attack.[43]

Compliance with the third party rule, as embodied in article 37 of the ISS Act 2002, likewise constitutes an important safeguard in the exchange of information between GISS and foreign intelligence and security services.

7.2 Third party rule

Information must be provided in conformity with what is known as the 'third party rule' which says that information obtained may only be provided to others if the service from which the information originates has given permission to do so. This requirement is laid down in article 37 of the ISS Act 2002. The legal history of the Act shows that this rule is an essential condition in international cooperative relations:

> "If a service cannot rely on the service in the addressee country keeping the information secret and using it exclusively for its own information, there can be no question of any real cooperation between the services in question. If a service gets the impression that the rule is not observed, it will stop or marginalize the exchange of information with the relevant counterpart."[44]

---

[42] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 59.
[43] *Parliamentary Papers II* 2000/01, 25 877, no. 59, p. 16.
[44] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 57.

Some intelligence and/or security services operate on the basis of the 'third *country* rule', giving a wider interpretation to the international principle. In principle the third country rule allows information originating from a foreign counterpart to be passed on between the intelligence and security services of the same country, unless the providing service has expressly precluded it. The ISS Act 2002 and the legislative history of the Act leave the Dutch intelligence and security services no scope for applying the third country rule.

Article 37(3), ISS Act 2002, provides that the relevant Minister or a person acting on his behalf may grant a foreign counterpart which has received information from GISS permission to pass on the information to others. It further provides that conditions may be attached to such permission, for example with respect to the nature and purpose of the use of the information.

Compliance with the third party rule constitutes an important safeguard in the cooperation between intelligence and security services. The rule contributes to source protection, the exchangeability of secret information and the mutual trust that forms the basis for a cooperative relation between intelligence and security services. In addition, the rule ensures control over the further distribution of information. This reduces the risk that information coming from one single source will find its way to several parties, each of them passing on the information in their turn, thus making it subsequently appear as if the information originated from several sources. The uncontrolled further provision of information may also result in the loss of comments about the reliability of the information from the service that initially provided it.

Where information is provided in the context of multilateral cooperative groups in which intelligence and security services of various countries participate, it is usually stated expressly with which (group of) intelligence and security services the information may be shared.

The Committee has established that GISS conducts a policy of strict compliance with the third party rule in regard to information received from foreign counterparts. GISS' practical implementation of the policy is also adequate. In practice, there are likewise very rarely found to be problems with the observance of the rule by foreign intelligence and security services with respect to information provided by GISS. The Committee notes that in nearly all cases the third party rule is stated in writing in messages sent to foreign counterparts. Occasionally, however, the rule is communicated orally to the counterpart by the liaison delivering the message. In a few other cases the person who prepared the message omitted to state the condition. For due care purposes the Committee considers it important that the third party rule is expressly included in writing in messages to foreign intelligence and security services and recommends GISS to make it standard procedure to state the rule.

7.3 Exchange of information in actual practice

GISS exchanges information with a large number of services on all kinds of subjects. The information exchanged may range from very general information on certain themes and more in-depth analyses of phenomena to very concrete information on particular matters or persons. The major part of information exchange takes place by messages being sent and received via secured connections. Another important channel is the (oral) exchange of information on the occasion, for example, of bilateral visits, contacts maintained by the liaisons with the various services under their responsibility and attendance at multilateral meetings. With respect to all these forms of information exchange GISS must each time ask itself whether it is permissible to provide this specific information to this specific service or services in this specific case. The opposite may also apply. In some cases GISS must ask itself whether it can afford not to provide certain information.

GISS has formulated a number of basic principles for the provision of information to foreign counterparts, thus elaborating the concrete details of *inter alia* the general statutory provisions pertaining to the processing of information. In principle, for example, information is provided in writing, so that it is subsequently possible to verify who provided which information to which counterpart and at what time this happened. If information is provided at oral consultations, a report must subsequently be prepared of the meeting. Purpose limitation is also an important instrument when information is provided. GISS states what is the context of the information provided and the reason for providing it. It imposes the condition on the receiving service that the information may be used exclusively for the (intelligence) purpose for which it was provided. Where there is an indication that the information in question will be used for another purpose, GISS' internal policy prescribes that the information may not be provided. Moreover, the receiving service must observe the third party rule discussed above. When providing information, GISS must, in addition to the third party rule, also mention the reliability of the information.

Internal policy imposes the above basic principles as conditions for the provision of personal data to foreign services. Moreover, additional conditions have been formulated that are equivalent to the criteria for cooperation mentioned above. The principle of reciprocity (*quid pro quo*), for example, and the nature of the activities of a foreign service play a role in the decision whether or not to provide personal data. Yet another condition is that the interests of a foreign service may not be incompatible with the interests of GISS, which must be deemed to include observance of fundamental and human rights standards, and that the proper performance of its statutory tasks by GISS may not preclude the provision of personal data. Moreover, if there are indications that the provision of the personal data may lead to the violation of human rights, GISS may in principle not provide

the information. Merely the country to which the foreign service concerned belongs may already constitute an indication. According to internal policy the conditions formulated by GISS may only be set aside *by way of rare exception*. This requires the existence of an unacceptable risk to society and its citizens that calls for prompt action. And it requires an urgent necessity to provide the personal data to the foreign service in question.

The internal policy of GISS further requires a proper assessment in each individual case – regardless of the service to which personal data are to be provided – whether it is permissible to provide the personal data. In its assessments concerning the provision of personal data GISS distinguishes between two categories of foreign intelligence and security services.[45] The first category comprises services from countries having a long democratic tradition, including a number of EU and NATO countries, and services of countries that do not have a (long) democratic tradition but do satisfy the criteria of professionalism, reliability and respect for human rights. According GISS policy, the second category consists of services for which there are clear indications that they do not satisfy one or more of the criteria of observance of human rights standards, reliability and sufficient professionalism. It is the opinion of the Committee that this category therefore covers all other foreign services – those which cannot be placed in the first category – of which it is questionable whether they satisfy the criteria for cooperation.

In principle, according to the policy of GISS providing personal data to foreign services in the first category does not pose a problem. The Committee shares the view that providing personal data to services falling in the first category is in principle permitted, provided all applicable statutory requirements are met including the requirements of necessity, appropriateness and due care. According to the policy of GISS, great restraint must be exercised in providing personal data to services falling in the second category. The Committee thinks this means that in principle no personal data are provided *unless* the rare exception occurs that is mentioned above. After all, if it is suspected that the foreign service in question does not observe human rights, is not reliable and/or operates unprofessionally, the conditions applying to the provision of personal data will not be satisfied either. Under current GISS policy these conditions may only be set aside by way of rare exception. This refers to cases involving an *urgent necessity* to provide the personal data to the relevant foreign service. The policy of GISS thus follows the statutory requirements applying to information processing and what is stated in the legislative history about the provision of personal data to services of countries whose respect of human rights is open to doubt.[46]

---

[45] It is not always clear to the Committee, though, in which category certain services are placed by GISS (see also section 6.1).

[46] *Parliamentary Papers II* 2000/01, 25 877, no. 59, p. 16.

When a team within GISS is conducting an investigation and wishes to share certain information (personal data or other information) with a foreign counterpart, the responsibility and power of decision lie in principle with the team leader. Under GISS policy the closeness of the cooperation with the foreign service concerned determines the nature and extent of the information exchange. As a rule GISS will provide information to foreign services with which it has a very close and intense cooperative relation more frequently and of a more substantive and sensitive nature than to counterparts with which GISS cooperates only occasionally. If the team has doubts about providing certain information to a specific counterpart, it must consult the Foreign Relations department and/or a legal expert before it may provide the information.

With respect to the provision of *personal* data, GISS also makes a distinction between the two categories of foreign services where it concerns the decision-making level. Decisions whether or not to provide personal data to services in the first category are taken by the team leader. In the case of the second category the internal rule is that the decision to provide personal data is in principle taken at director level. In rare exceptional cases – urgent necessity to provide personal data because of an unacceptable risk to society and its citizens that calls for prompt action – the internal policy prescribes that the decision to provide personal data be taken by the head of GISS. It is the opinion of the Committee that the provision of personal data to a foreign service in the second category always constitutes a rare exception.

The Committee's investigation has shown that in daily practice a processor or analyst in a team usually decides on his own whether or not personal data or other information will be provided to a foreign service. It depends on the appraisal and experience of the staff member concerned whether and in which cases the team leader is consulted. In cases that are (obviously) open to question the team leader is usually consulted. The Committee holds the opinion, however, that this practice does not do sufficient justice to the requirements imposed by the legislature on information processing, namely that it must be done with proper and due care (article 12(3), ISS Act 2002). The requirement of due care applies with even greater force in the case of the provision of personal data. It is the opinion of the Committee that decisions about providing personal data to counterparts should be taken at least at team leader level in *all cases* and not only when a processor or analyst is in doubt. This has meanwhile become adopted policy at GISS. The Committee further holds the opinion that in the case of personal data being provided on the basis of the aforementioned rare exception - urgent necessity to provide personal data because of an unacceptable risk to society and its citizens that calls for prompt action – the decision to do so must always be taken at service management level. The reason for this is that said exception, entailing disregard of individual human rights, applies only under exceptional circumstances. From a due care perspective it is advisable that in these circumstances

decisions be taken at service management level. The Committee recommends GISS to bring its internal rules and practice regarding the provision of personal data to foreign services into line with this finding.

The Committee has established that GISS increasingly exchanges (personal) data with foreign intelligence and security services of which it is doubtful whether they satisfy the prescribed criteria for cooperation. This can be explained by the growing international (terrorism) threat, which has the result that from GISS' point of view it has become more advisable to exchange information with foreign counterparts, in certain cases even with services of which it is doubtful whether they satisfy the prescribed criteria for cooperation. In this context GISS is sometimes confronted with the question whether in a specific case it can afford not to provide (personal) data to a certain foreign service. At the same time, however, GISS must always consider to what limits the provision of (personal) data is lawful. The Committee points out that in a certain field the assessments made by GISS on this issue are in practice increasingly stretching the limits. For the purposes of fighting terrorism, for example, it is sometimes deemed almost an automatism that (personal) data may be provided to foreign services of which it is doubtful whether they satisfy all the criteria for cooperation.

The Committee has established that in some cases GISS acted unlawfully[47] when it provided personal data to foreign intelligence and security services. In three of the cases which the Committee came across, GISS provided personal data to counterparts of which it is doubtful whether they satisfy the criteria for cooperation without the requirement of (urgent) necessity being satisfied. The Committee further came across two cases in which GISS sent along personal data of a person other than the person to whom the provision of data primarily related (third parties) without this being necessary. In one single case personal data was provided without the subsidiarity principle being satisfied and GISS could have used a less infringing means. Finally, the Committee came across one case in which personal data was provided to a foreign service of which it is doubtful whether it satisfies the prescribed criteria for cooperation, while GISS is no longer able to retrieve the reasons for providing the personal data.

The Committee holds the opinion that in some cases the assessment underlying decisions to provide personal data to foreign services of which it may be doubted whether they satisfy the prescribed criteria for cooperation is very limited in scope. In these cases little attention is paid to the possible risks and other adverse effects which the provision of

[47] In the cases referred to here, the Committee reviewed whether GISS could reasonably have come to the decision to provide the personal data to the foreign service(s); GISS has a certain margin of discretion in this matter. The cases that the Committee considered unlawful are cases in which this margin was exceeded.

personal data to a foreign service of which it may be doubted whether it satisfies the prescribed criteria for cooperation may entail for the person concerned. The Committee has established that in many cases the reasons for providing personal data to a foreign service are not laid down in writing.

The Committee has established that in seven cases personal data was provided to foreign services of which it may be doubted whether they satisfy the prescribed criteria for cooperation while no permission to do so had been given at the appropriate level. The Committee noticed that in many cases the permission to provide personal data to a foreign service is not laid down in writing. From a due care perspective the Committee considers it proper procedure for GISS to record the permission granted in writing.

The Committee has further found that in many cases when GISS provides information to foreign services it does not give any indication of the degree of reliability or a reference to the document or the source from which the information is derived. GISS thus does not comply with the provision of article 12(4), ISS Act 2002.

The Committee has found that in some cases it proved difficult for GISS to retrieve fully to which foreign services a message was provided. In this regard the Committee draws attention to the obligation imposed on GISS by article 42, ISS Act 2002, to keep records of the provision of personal data.

The Committee recommends GISS to exercise greater care in providing personal data to foreign services and to act in accordance with all the applicable statutory provisions as well as its own internal rules. The Committee also recommends that GISS, for due care purposes, keep written records of the thorough assessments that are or should be made prior to providing personal data to a foreign service of which it may be doubted whether it satisfies the prescribed criteria for cooperation. The Committee further recommends GISS to keep records of all permissions to provide personal data to a foreign service.

The Committee reflects that article 43, paragraphs (2) and (3), ISS Act 2002, provide, if information proves to be incorrect or is being processed wrongfully, that it must be corrected or removed. The relevant Minister must as soon as possible notify this fact to the persons to whom the information has been provided. The information removed must be destroyed, unless statutory provisions on the retention of information preclude it. Implementation of these provisions in the cases referred to above means that all personal data wrongfully provided to foreign services must be destroyed. The Committee points out, however, that the information wrongfully provided is not in the possession of GISS but of the foreign service(s) concerned. A recommendation to GISS will not lead to the intended objective of article 43, paragraphs (2) and (3), ISS Act 2002, namely the removal of the

information wrongfully processed. For this reason the Committee in this case refrains from making a recommendation to such effect.

8. Technical and other forms of assistance

8.1 Legal framework

Pursuant to article 59(4), ISS Act 2002, GISS may, for the purposes of maintaining relations with foreign intelligence and security services, render technical and other forms of assistance to foreign services for the benefit of the interests to be served by these services. The legislative history of the Act shows that this provision was created because it was considered advisable to regulate not only the provision of information, but also other forms of cooperation with foreign services.[48] Rendering technical and other forms of assistance is made subject to similar conditions as those applying to the provision of information. Assistance for the benefit of the interests of a foreign service may only be rendered insofar as the interests to be served by the foreign service are not incompatible with the interests to be served by GISS (article 59(4)(a), ISS Act 2002) and insofar as the proper performance of its statutory tasks by GISS does not preclude rendering assistance (article 59(4)(b), ISS Act 2002). A distinction must be made between rendering assistance to a foreign service for the benefit of the interests served by the foreign service on the one hand and carrying out joint operations undertaken (partly) for the performance of its statutory tasks by GISS on the other hand.

An example mentioned in the legislative history of a situation in which the proper performance of its statutory tasks by the Dutch service is incompatible with assisting a foreign service is the frustration of ongoing operations of GISS itself. It is also observed that the kind of assistance that is requested is significant, too. It must, among other things, fit within the legal parameters to be observed by GISS. If a certain form of assistance is incompatible with those parameters, rendering the assistance nevertheless would be contrary to the proper performance of its statutory tasks by GISS.[49]

Assistance to foreign services often concerns the exercise of special powers, such as tailing and surveillance operations. GISS must fully observe the statutory regulations applying to the exercise of these powers, also when they are exercised to meet a request for assistance. This means that GISS must among other things satisfy the criterion of necessity laid down in article 18, ISS Act 2002.[50] In all cases, therefore, the exercise of a

[48] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 37.
[49] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 64.
[50] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 38.

special power to assist a foreign service must always (also) be necessary for the proper performance of its statutory tasks by GISS as referred to in article 6(2), at a and d, ISS Act 2002 (the a-task and the d-task). The necessity referred to here is stricter than the necessity required for the processing of information by article 12(2), ISS Act 2002, which concerns necessity for the purposes of properly implementing the ISS Act 2002 or the Security Screening Act. When GISS renders assistance by exercising special powers it must, in addition, meet the requirements of proportionality and subsidiarity, as embodied in articles 31 and 32, ISS Act 2002. Foreign services rendering assistance to GISS will have to observe the rules applying to them in their respective countries, so the legislative history of the Act shows. Foreign services using means of intelligence in their own territory must observe the legal parameters applying to them.[51]

It must therefore be assessed for each individual request for assistance whether the requested assistance fits within the prescribed parameters. That is why rendering assistance must be preceded by a written request from the foreign service concerned to GISS. Article 59(5), ISS Act 2002, provides that a request for assistance must be signed by the competent authority of the requesting foreign service and must give a detailed description of the desired form of assistance and the reason(s) why the assistance is requested.

Pursuant to article 59(5) and (6), ISS Act 2002, assistance may only be rendered with the permission of the Minister concerned. The Minister may only give the head of the service a mandate to give such permission with respect to requests of an urgent nature (for example cross-border tailing and surveillance activities), subject to the condition that the Minister be immediately informed of any permission granted. The power to give permission to render technical and other forms of assistance has been vested at this (high) level because of the potential political aspects which rendering assistance may entail.[52] If the Minister has given permission to assist a foreign service, the assistance is rendered under the responsibility of the Minister.[53]

8.2 Rendering assistance in actual practice

In the course of its investigation the Committee came across only a few cases of assistance rendered by GISS to a foreign service in which the permission of the Minister of the Interior and Kingdom Relations was expressly requested and granted. Each of these cases

[51] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62.
[52] *Parliamentary Papers II* 1999/2000, 25 877, no. 8, p. 101 and no. 9, p. 37.
[53] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 38.

involved assistance to a service with which GISS had a close cooperative relation in situations that could be ranged under the a-task or the d-task of GISS but which had no connection with any assignment of one of the teams of GISS. The Committee has found evidence that the assistance by GISS was partly rendered in the form of exercising special powers. As was explained above, article 18, ISS Act 2002, provides that the exercise of a special power must (also) be necessary for the proper performance of the a-task or the d-task of GISS. It is the opinion of the Committee that in the cases mentioned above this necessity requirement was met. The Committee has also established that the forms of assistance rendered for the benefit of the foreign service concerned were not incompatible with the interests to be served by GISS (article 59(4)(a), ISS Act 2002) and that the proper performance of its statutory tasks by GISS did not preclude them (article 59(4)(b), ISS Act 2002).

The Committee has found that GISS only rarely considers certain forms of cooperation to be assistance within the meaning of article 59(4), ISS Act 2002, which requires the prior permission of the Minister of the Interior and Kingdom Relations. Assistance rendered independently of any specific team assignment is deemed to be assistance in this sense. Usually, GISS does not consider supporting forms of cooperation that may be ranged (whether or not indirectly) under a team assignment to be assistance within the meaning of article 59(4), ISS Act 2002. Examples are tailing and surveillance activities carried out at the request or instigation of a foreign service which have aspects in common with an investigation conducted by GISS in the performance of its own statutory tasks. GISS holds the view that these supporting forms of cooperation are also in the interest of GISS and for this reason it does not classify such activities as assistance within the meaning of article 59(4), ISS Act 2002. The Committee holds the opinion that the interpretation given by GISS to the term assistance pursuant to article 59(4), ISS Act 2002, is too narrow. In the opinion of the Committee the decisive criterion should not be whether a supporting activity may be ranged under a team assignment, but whether the supportive form of cooperation can actually contribute to an ongoing investigation by GISS. If, for example, a foreign service requests GISS to render assistance by exercising a special power with regard to a target of the foreign service, it is the responsibility of GISS to examine whether the information that may be obtained by rendering the requested assistance can contribute to an investigation being conducted by GISS itself. This will e.g. be the case if GISS is also investigating the person concerned or if the person can be linked to persons or organisations being investigated by GISS. It is the opinion of the Committee that in such cases the supporting form of cooperation need not be regarded as assistance within the meaning of article 59(4), ISS Act 2002, but rather as part of a joint operation. If the supporting activities can make no contribution to an ongoing investigation of GISS, the activities will have to be regarded as assistance. GISS will then require the prior permission of the Minister before it may assist the foreign service (article 59(5), ISS Act 2002). The Committee has established

that in the cases in which GISS rendered assistance to a foreign service within the meaning of article 59(4), ISS Act 2002, but did not regard it as such, it wrongly omitted to request the Minister of the Interior and Kingdom Relations for permission to render the assistance.

The Committee has established that GISS also does not range under article 59(4), ISS Act 2002, assistance rendered to foreign services not involving the exercise of special powers. An example is assistance in the form of a course or training or transfer of technical knowledge, rendered in the interest of the foreign service. Such forms of assistance, which are to be distinguished from the provision of information, are rendered by GISS with a view to continuing or intensifying a cooperative relation. It is the opinion of the Committee that formally these forms of assistance must be deemed to fall under article 59(4), ISS Act 2002, too. According to the legislative history of the Act, assistance usually involves the exercise of special powers.[54] This means that assistance may also involve the performance of activities other than the exercise of special powers by GISS. The examples given above expressly concern activities that serve to assist the foreign service in question and are performed in its interest. GISS has no interest whatsoever in performing these supporting activities other than its cooperation with the foreign service in itself. These cases are covered by article 59(4), ISS Act 2002.

The Committee takes the ground that in actual practice the above interpretation of the term assistance as used in article 59(4), ISS Act 2002, may lead to situations that are difficult to defend. The Committee does not hold the opinion, for example that the mere fact that a special power is exercised in the interest of and to assist a foreign service necessitates in all cases that the required permission be raised to ministerial level. If for example GISS performs (cross-border) tailing and surveillance activities for the benefit of foreign services – a power for which normally permission from a team leader will suffice – it is the opinion of the Committee that permission from the Minister is a disproportionately severe requirement. The Committee also takes the ground that the severity of the permission requirement of article 59(5) and (6), ISS Act 2002, may also not be proportionate to forms of assistance which do not involve the exercise of special powers, have hardly any politically sensitive aspects and do not violate any fundamental rights. In spite of the disproportion between these forms of assistance and the level at which permission is required to be given, the Committee holds the opinion that article 59(4), ISS Act 2002, and what is said in the legislative history of the Act about rendering assistance to foreign services leave insufficient scope for the interpretation given to the term assistance by GISS. The Committee recommends GISS to give a stricter interpretation to the term assistance within the meaning of article 59(4), ISS Act 2002, and to bring the internal (permission) procedures into line with that interpretation.

---

[54] *Parliamentary Papers II* 1999/2000, 25 877, no. 9, p. 38.

8.3 Requests for assistance made by GISS

GISS also makes requests for assistance to foreign intelligence and security services. It may, for example, request a foreign service to tail and/or keep under surveillance a GISS target when the target travels to the country of that service, or to tap his telephone. The ISS Act 2002 does not lay down rules for making requests for assistance to foreign services. According to the legislative history of the Act it is the responsibility of the foreign service and the other appropriate authorities in the country concerned to decide whether or not to comply with a request from GISS. If the foreign services render assistance to GISS, they will have to observe the statutory and regulatory provisions applying to them.[55] This does not mean that GISS may simply request all kinds of assistance provided the assistance is compatible with the rules applying to the foreign service. It is the opinion of the Committee that GISS may exclusively request a foreign service to exercise special powers which GISS itself is authorised to exercise, with due observance of the statutory requirements of necessity, proportionality and subsidiarity attached to the exercise of these powers. This is so because assistance by a foreign service at the request of GISS is rendered for the purposes of the proper performance of its statutory tasks by GISS. And GISS is bound to perform its tasks in accordance with the law (article 2, ISS Act 2002). It is the opinion of the Committee that a request from GISS to a foreign service to render assistance for the purposes of the performance of GISS' own tasks by exercising powers which GISS itself is not authorized to exercise or which does not satisfy the requirements of necessity, proportionality and subsidiarity, is unlawful.

No permission requirement for making a request for assistance has been embodied in either the law or an internal rule of GISS. It is usually a team leader who decides whether a foreign service will be requested to render assistance. In some cases the relevant director is involved in the decision making or the Foreign Relations department is consulted. In actual practice it proves to depend mainly on the team wishing to make the request whether this happens and in which cases. The Committee considers it advisable that the requirement of permission for making requests for assistance to foreign services be laid down expressly and recommends GISS to ensure that this is done. The requirement can be linked to the permission which normally speaking is required for exercising the power to which the request relates. For example, if the request is for assistance by tailing a person and/or keeping a person under surveillance, a team leader's permission to make the request will suffice. A request to a foreign service to tap a person's telephone will require permission from the Minister. Because of the required due care, permission to request the assistance of a foreign service of which it is doubtful whether it satisfies one or more criteria for cooperation will have to be granted at a higher level than permission to request

[55] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 62.

the assistance of a foreign service with respect to which no doubts exists. The Foreign Relations department should be informed of such requests in advance.

The Committee has established that a number of requests for assistance in the form of exercising special powers made to foreign services of which it is doubtful whether they satisfy the prescribed criteria for cooperation did not satisfy the requirements of necessity, proportionality and/or subsidiarity. In three cases the request for assistance made to the foreign service could have such harmful consequences for the person(s) concerned as to be disproportionate to the intended purpose of GISS. In two of these cases, moreover, it would have been sufficient for GISS to use a means less injurious to the person(s) concerned, for example not requesting the assistance of the foreign service but performing activities itself. It is the opinion of the Committee that GISS should not have requested the assistance of these foreign services of which it was doubtful whether they satisfied the prescribed criteria for cooperation.

The Committee has further established that some requests for assistance from GISS to foreign services are worded in a way that leaves the foreign service much scope for deciding how to act in meeting the request. The Committee also noticed that GISS does not always stipulate additional guarantees from the foreign services in question that may limit the potential detriment to the person(s) concerned. From a due care perspective the Committee believes that it would be better if GISS makes its requests for assistance to foreign services as explicit as possible and where possible states the limits of the requested assistance. The liaison who has the service in question in his portfolio can play a prominent role here. This will require that the arrangements made with the foreign service are recorded in detail.

The Committee recommends that GISS, prior to asking a foreign service for assistance by exercising special powers, makes a thorough assessment of the necessity, proportionality and subsidiarity of the request to be made and record the assessment in writing. The Committee deems it advisable that the obligation to state reasons in writing is expressly included in the permission procedure for requests to foreign services recommended by the Committee.

9. Joint operations

9.1 Legal framework

Joint operations with foreign counterparts are carried out on Dutch territory as well as abroad. In both cases GISS may only operate to the extent the current legal parameters

permit. Legislative history shows that foreign service agents may only be deployed on Dutch territory if the head of GISS has given permission and subject to the conditions attached to the permission. If the (politically sensitive) nature of an operation and the accompanying potential risk factor so require, permission must be given in consultation with the responsible Minister. If permission to deploy an agent of a foreign service on Dutch territory is granted, the agent will operate under the responsibility of the Minister and under the direction of GISS.[56] Such an operation must always be considered a joint operation, with the foreign service acting as an equal partner. In addition, it is the responsibility of GISS to monitor the operational activities of the foreign service agent and check whether they are in accordance with the conditions set.[57]

Joint operations on Dutch territory may therefore only be carried out under the direct direction and actual control of GISS. GISS is responsible for ensuring that foreign counterparts operate in the Netherlands in accordance with the applicable rules. This means that GISS must ensure that the activities carried out by the services in joint operations are consistent with the interests to be served by GISS and besides are no impediment to the proper performance of its statutory tasks by GISS.

In a previous review report the Committee observed on this point that a certain degree of supervision by GISS over joint operations with foreign services is required so that GISS can monitor whether the operation is being carried out within the applicable legal parameters. The Committee further observed that under certain specific circumstances a more far-reaching form of supervision by GISS over such operations is needed. The Committee mentioned as examples of specific circumstances the deployment of foreign service agents on Dutch territory, or the involvement of human sources of GISS in a joint operation.[58]

9.2 Joint operations in actual practice

GISS carries out joint operations mainly with counterparts with which it has a long-term cooperative relation. In a few cases GISS started one or more joint operations with foreign services with which it has been cooperating only since fairly recently. For GISS, the reliability, professionalism and operational methods of a counterpart are important distinctive criteria for operational cooperation.

---

[56] With respect to activities in places in use by the Ministry of Defence these are *mutatis mutandis* the Minister of Defence and the Director of DISS.

[57] *Parliamentary Papers II* 2000/01, 25 877, no. 14, p. 64.

[58] CTIVD Review report no. 5B on the investigation by the Review Committee of the legitimacy of the investigation by GISS into the proliferation of weapons of mass destruction and means of delivery, *Parliamentary Papers II* 2005/06, 29 924, no. 5 (appendix). Available at www.ctivd.nl.

The Committee has investigated joint operations of GISS in the Netherlands as well as abroad. It has not emerged from the Committee's investigation that GISS, when carrying out joint operations with counterparts, failed to satisfy the conditions imposed on such operations by law and legislative history. All the joint operations that were investigated satisfied the permission requirement and the Minister of the Interior and Kingdom Relations was consulted where necessary. The investigation also has not produced any indications that the activities of foreign counterparts in joint operations with GISS on Dutch territory conflicted with the interests to be served by GISS or with the proper performance of its statutory tasks by GISS. The subject of secret operations of foreign services on Dutch territory without the knowledge of GISS was discussed in section 4.

With regard to the period covered by the present investigation the Committee has not found any indications that GISS takes insufficient charge of or gives insufficient direction to joint operations with foreign services taking place (partly) on Dutch territory. In 2002, in an internal evaluation of its cooperation with a particular foreign service, GISS formulated a number of basic conditions for successful operational cooperation that could apply to all GISS operations. These conditions were elaborated into internal rules for joint operations, called *Joint Operations Guidelines*, which were approved by the GISS service management in 2007. The Guidelines include a number of items that must be considered when preparing for, entering into, carrying out or terminating operations performed in cooperation with foreign services. It is the opinion of the Committee that if the operational teams follow the Guidelines, this will help improve the supervision of joint operations with foreign services.

One of the items for consideration included in the Guidelines is the principle that the team or department carrying out a joint operation must always keep the Foreign Relations department informed. If there are reasons to depart from this principle, the head of the operation must contact the head of the Foreign Relations department. As was already noted above in section 6.3, the Foreign Relations department is not (sufficiently) informed in all cases. It is the opinion of the Committee that the (head of the) Foreign Relations department must in all cases be informed and kept informed of the operational cooperation with the foreign services, even in the case of a highly sensitive operational cooperation. It concerns not so much information about the substantive operational details but rather about things like the arrangements made with the counterpart, the reasons why the services cooperate and the interests involved, any problems encountered during the cooperation and the quality and quantity of the information obtained from or provided to the counterpart.

10. Cooperation for security screening purposes

GISS also cooperates with foreign intelligence and security services for security screening purposes. Security screening precedes the issue or refusal of a declaration of no objection which is required for persons who are to hold a position involving confidentiality. If a person to be screened spent (a considerable) time abroad in the period before the screening, GISS depends to a large extent on information from foreign counterparts for its investigation of that period. GISS has a duty to make reasonable efforts to obtain the information necessary for a proper assessment.[59] If it proves impossible for GISS to obtain the necessary information by making a reasonable effort, it follows that the security screening has not produced sufficient information to enable GISS to make an assessment. The person concerned will then be refused a declaration of no objection. So it also serves the interest of the person involved in a screening that GISS cooperates properly with foreign services for security screening purposes. Pursuant to article 36(1)(d), ISS Act 2002, GISS may provide information on a person to be screened to a foreign counterpart which can then perform an administrative check based on this information. At the request of a foreign service GISS may also, pursuant to article 59(2), ISS Act 2002, provide information about a person involved in a security screening conducted by that service.

With a number of foreign counterparts GISS exchanges information for security screening purposes on the basis of existing treaties on security issues. Examples are the WEU Security Agreement and the NATO Treaty.[60] In addition, information is exchanged for security screening purposes with foreign counterparts without an underlying treaty. Usually, however, GISS and the relevant counterpart lay down arrangements made between them in this regard in a memorandum of understanding or agreement. GISS does not maintain relations with every foreign intelligence and/or security service based on which it may provide and request information on parties involved in security screening. The reason for this is that personal data may only be provided with due care and sufficient safeguards (see also section 7). Before entering into a cooperative relation for security screening purposes GISS must therefore assess whether the counterpart concerned qualifies for such cooperation.

In January 2004 a procedure was included in the internal Manual of GISS for decision-making whether or not to cooperate with counterparts with which GISS does not or not

[59] See also CTIVD Review Report no. 11b on the investigation of the Committee into the implementation of the Security Screening Act by GISS, *Parliamentary Papers II* 2006/07, 29 876, no. 21 (annex). Can be consulted at www.ctivd.nl.

[60] See also the explanatory memorandum to the Policy Rule for insufficient information in security screenings at civil airports *(Beleidsregel onvoldoende gegevens bij veiligheidsonderzoeken op de burgerluchthavens)*, Government Gazette 2001, no. 59.

yet have a security screening relationship. The Foreign Relations department compiles a country information file in which are recorded among other things background information on the country, an assessment of the criteria for cooperation, items for consideration (if any) and a cooperation recommendation to the service management. After being discussed in the Foreign Relations Consultative Body, the country information file is submitted to the service management of GISS for approval. After approval by the service management, GISS may cooperate with the service(s) of the country concerned for security screening purposes. In addition to this procedure the Manual of GISS also contains a list of countries with which GISS is cooperating for security screening purposes.

According to this internal procedure, GISS may only cooperate for security screening purposes with services giving the required priority to the observance of human rights and whose professionalism, reliability and democratic anchorage are not subject to doubts (see section 5 for a detailed discussion of these criteria). The principle of *quid pro quo* is also relevant here. If GISS cannot provide personal data for security screening purposes to a specific foreign counterpart, it will likewise not comply with requests for an administrative check for security screening purposes received from that foreign service. The procedure further provides that if doubts exist whether a foreign counterpart satisfies one of the aforementioned criteria, GISS should not request this service to provide information for security screening purposes. In such cases the nature of the cooperative relation is not so close that GISS can and may rely on the information provided by the security service in question. It may even be irresponsible, also with regard to the interest of the person concerned, to disclose in certain countries that a person is being considered for a position involving confidentiality.

In the course of its investigation the Committee examined all country information files. The Committee has found indications that in some cases the interest of GISS in cooperating with a specific service for security screening purposes carries more weight than the requirements of reliability, democratic anchorage and observance of human rights. The specific joint interest of fighting terrorism in civil aviation is often mentioned in assessments leading to decisions to cooperate with services having limited democratic anchorage or of which it is questionable whether they observe human rights or provide information that is reliable in all cases. In some country information files, moreover, GISS takes the ground that it is possible to minimize the risks to the persons whose personal data is provided to the service in question by taking strict (procedural) precautionary measures. In some country information files, for example, GISS states that a request to the foreign service must state expressly that the request is exclusively for an administrative check of the person investigated and that the service may not do any field research. Since May 2007 the rule applies at GISS that all requests to foreign services must state that the addressee service should exclusively perform an administrative check. The country

information files further state that it must also be stated expressly that the information provided in the request may not be used for purposes other than doing an administrative check and that the information may not be furnished to third parties without the prior permission of GISS. One important safeguard is the fact that the person being screened must sign a declaration of consent in which he gives permission to provide his personal data to the addressee service. The country information files also state that it will be examined in each individual case whether there are special circumstances making it inadvisable to provide information about the person being screened to the foreign service. No information will be provided about relatives of a person concerned. Initially, moreover, GISS will only cooperate in security screenings in the context of civil aviation because there the interests of GISS and the foreign services are synchronous. If experiences are positive, the cooperation can be extended to other kinds of security screenings.

It is the opinion of the Committee, when GISS cooperates in security screenings with foreign counterparts of which it is questionable whether they satisfy the prescribed criteria, that the protection of the person screened requires that GISS takes precautionary measures (as mentioned above) and applies them strictly. The Committee has established, however, that in actual practice the precautionary measures mentioned in the country information files were not always applied or applied strictly. Requests to foreign services with respect to which these precautionary measures are applicable do not always state that the foreign service may do an administrative check only and no field research. In one case the foreign service did in fact do field research. GISS called that foreign service to account for it. Since mid-2007 GISS applies the rule that all requests to foreign services must include a statement that the service may only do an administrative check. The Committee came across one case from a later date in which the statement was not included. The Committee recommends that GISS strictly apply the prescribed precautionary measures aimed at protecting persons involved in security screening and in all cases expressly include the conditions laid down with respect to foreign services subject to doubts in the written request.

The Committee's investigation has shown that GISS also cooperates for security screening purposes with services of which it may be doubted whether they satisfy the prescribed criteria, without the service management having given permission for the cooperation after following through a decision procedure. No precautionary measures have been laid down in a country information file with respect to these services. The Committee has also established that GISS already was or is cooperating with some services while the decision procedure had or has not been followed through yet. The Committee considers this improper and holds the opinion that GISS must always first follow through the decision procedure before it may start cooperating. The purpose of the procedure is precisely to arrive at a decision, assessed at service management level and supported by the Foreign

Relations department and the Foreign Relations Consultative Body, whether or not to cooperate with a foreign service for security screening purposes. The procedure provides that if the intended cooperation partner does not satisfy the criteria for cooperation, additional precautionary measures must be adopted to protect the persons whose personal data is furnished to the service concerned. It is the opinion of the Committee that this procedure does justice to the requirements set by the legislature on the provision of personal data, namely that the provision of such data must take place with due care and sufficient safeguards. The Committee recommends that GISS, before starting to cooperate with a foreign service for security screening purposes, first assess in accordance with the internal decision procedure whether the service qualifies for cooperation and if so, subject to which conditions.

The Committee has established that persons involved in a security screening who resided abroad for a certain period are not in all cases informed of the fact that their personal data may be provided to a foreign service. It is true that this possibility is mentioned in the explanatory notes to the (digital) Personal Information Form that persons subject to security screening must fill out.[61] But this fact is only expressly pointed out to them if GISS is going to make inquiries with foreign services of which it is doubted whether they satisfy the prescribed criteria for cooperation and with respect to which GISS has decided that additional safeguards must be provided. This is due to the fact that the approved country information files for these foreign services prescribe that GISS requires the consent of the person concerned before it may request the foreign service to provide information. No such requirement of consent from the person concerned applies to requests to foreign services about which no doubts exist. The Committee holds that it is in the interest of the persons concerned that they are expressly informed in all cases that GISS will possibly make inquiries with a foreign counterpart if they resided abroad for some time. The Committee recommends that GISS include a passage to this effect in the Personal Information Form which a person involved in screening must fill out and sign before GISS may start a security screening investigation.

The manual of GISS contains a list of countries with which GISS cooperates for security screening purposes, whether or not subject to conditions. The Committee notes that this list is outdated. The Committee has found that not all countries with which GISS actually cooperates are included in the list. For some countries it is expressly stated that GISS does not cooperate with them for security screening purposes while in actual fact it does. The Committee knows that the Security Screening department has an accurate and updated

[61] In the digital Personal Information Form each question is accompanied by an icon (a question mark) which, when clicked, leads to the explanatory note to the question. The text referred to here is found under the icon next to the question "Did you reside at another address at any time in the past [x number of] years?", stating that this includes addresses abroad.

list. The Committee recommends, with a view to due care, that the list of the Manual, which is accessible to GISS employees, be brought into line and kept identical with the list at the Security Screening department.

The Committee remarks that sometimes GISS has to wait a long time before a foreign service replies to a request from GISS. Every request sent to a foreign service expressly states the time limit within which GISS would like to receive a reply. If the foreign service does not respond within the time limit stated, GISS sends a reminder and if necessary a second reminder at a later date. GISS evaluates cooperative relations on this point and in some cases it calls the foreign services to account on the matter. In this way GISS tries as far as possible to reduce the prolonged time that security screenings sometimes take to the statutory time limit of eight weeks.

11. Cooperation in an institutionalized multilateral context

GISS also cooperates with intelligence and security services of other countries in more or less formalised cooperative groups. Such multilateral cooperation exists with European countries and has in a few cases been set up in an EU context. GISS also cooperates in the context of the North Atlantic Treaty Organisation (NATO). GISS participates in the NATO Special Committee, where the heads of the security services of the NATO member states discuss security-related issues. In addition, GISS in its capacity as National Security Authority plays a role within the Dutch delegation to the NATO Security Committee, the security body of NATO which develops the policy for securing classified NATO information. Multilateral cooperation also takes place in the context of the United Nations (UN). For example, GISS assists organisations within the UN (focusing on counterterrorism) by providing them with relevant information.

The Committee's investigation has shown that GISS makes an active contribution to several multilateral fora. These more or less institutionalized cooperative groups are particularly suitable for exchanging information and views between member services, and for coordinating policy choices in the field of national and international security in a broad sense. Operational cooperation is usually more often a bilateral matter. The Committee has noticed, however, that GISS is increasingly participating in ad hoc operational cooperation in (limited) multilateral context, in particular in the field of fighting terrorism. The interests of GISS in this field coincide with the interests of various other intelligence and security services, making the determination and implementation of a joint strategy an obvious course of action.

The following paragraphs contain a brief discussion of a number of European cooperative groups.

11.1 Joint Situation Centre (SitCen)

SitCen, established in 2002, is a part of the EU Council Secretariat in which twenty European intelligence and security services cooperate and falls under the responsibility of the Secretary-General of the EU Council. SitCen functions as an alert mechanism for international crisis situations and provides (information) support for international operations. In addition, SitCen makes information and threat analyses to support EU policy-making, in particular the common foreign and security policy in the second pillar. SitCen provides information to various policy-makers both within the EU and in the Member States. The analyses of SitCen are used inter alia in various Council bodies such as the Political and Security Committee (PSC), the Terrorism Committee (COTER) and the Working Group on Terrorism (WGT). To a large extent, moreover, SitCen shares its terrorism reports with Europol. SitCen is (partly) dependent on the supply of information from the intelligence and security services involved. SitCen has the capability to combine information, compare perspectives and use the specialisms of the various intelligence and security services. This also has advantages in providing insight into transnational phenomena.

11.2 Counter Terrorist Group (CTG)

The CTG was established by the heads of a number of European security services after the attacks of 11 September 2001. The CTG has grown into an informal cooperation group made up of the security services of the EU countries plus Norway and Switzerland. Europol and the services of the United States have observer status at the CTG. The objective of the CTG is to intensify cooperation and information exchange in the field of counterterrorism between the security services of the participating countries. Within the CTG participants exchange information in the field of counterterrorism, prepare (threat) analyses - including a joint European threat assessment – and undertake operational cooperation. There were also frequent exchanges of information on the (foiled) attacks in the United Kingdom, Germany and Denmark. In CTG context the heads of the security services meet every six months. Meetings of directors responsible for counterterrorism are more frequent. The CTG was deliberately kept outside the EU system of council working groups and set up in a more informal setting. This allows the CTG to function as an independent forum at the level of service heads and directors responsible for counterterrorism and facilitates cooperation between the security services. A recurring question is how the European services can give greater visibility to the cooperation in the CTG without abandoning its independence and informal nature. At present, the analyses produced by the CTG are partially contributed to the working groups of the European Council. In addition, the CTG regularly gives presentations in the Permanent Representatives Committee (COREPER) at

Brussels. In 2004 a link was set up between CTG and SitCen. The CTG supplies collective information on specific subjects and has a representative at SitCen, rotating every six months.

11.3 Club de Berne (CdB)

The CdB is an informal cooperative group of the heads of a large number of European security services and was established in 1965. Meetings of the CdB are held every six months. Security services of countries that are not (yet) part of the CdB may be admitted if all members agree. Decisions of the CdB are likewise taken unanimously. In addition to meetings of the heads of the services other events such as working groups, training sessions and expert meetings are organised in the context of the CdB. In principle, members cooperate in all the working areas of the security services. In a CdB context GISS initiated discussions on the future of security services. Developments in society such as growing interest if the public in security issues, concerns about privacy rights, increasing overlap between intelligence and investigation work and increasing EU regulation of security matters, all viewed in the light of the global terrorist threat, place greater emphasis on the visibility of and cooperation between security services. This demands the necessary adjustments of security services, both organisational adjustments and in the field of security.

11.4 Middle European Conference (MEC)

The MEC is a multilateral cooperative group of a number of West and Middle European intelligence and security services. The MEC was established after the Berlin Wall fell in 1989 for the purpose of providing support and assistance to the services of the Central European countries. The MEC functions as a platform for consultation and information exchange and contributes to the mutual trust between the affiliated intelligence and security services. In the past three years GISS was actively - though to a decreasing extent - involved with the MEC. With most of the services affiliated with the forum GISS also cooperates in the context of other informal groups.

12. Cooperation within the Kingdom of the Netherlands

Based on a long tradition, GISS cooperates with the Netherlands Antilles Security Service (NASS) and the Aruba Security Service (ASS). This cooperation for national security purposes has not been laid down by law. The Charter for the Kingdom of the

Netherlands[62] (further referred to as the Charter) contains an exhaustive list of the affairs of the Kingdom (Articles 3 and 43(2) of the Charter). National security is not included in the list and must therefore be deemed to be a domestic affair of each of the individual countries of the Kingdom which autonomously manage their internal affairs, so Article 41(1) of the Charter provides. The intelligence and security services of the countries of the Kingdom therefore cooperate on an entirely voluntary basis. For this purpose GISS, NASS and ASS have concluded a cooperation agreement.

After the events of 11 September 2001 the countries of the Kingdom declared themselves in favour of intensifying cooperation between the countries in the field of international counterterrorism and adopted a joint declaration to this effect.[63] The closer cooperation is focused mainly on strengthening legislation and regulations in the field of fighting terrorism, intensifying police and judicial cooperation, building and maintaining an adequate store of information by the security services and enhancing monitoring and supervision of the financial sector. With regard to the third item the declaration states that an agreement will be concluded between the security services. This agreement, which *inter alia* lays down the countries' fundamental willingness to conduct joint investigations and exchange relevant information, was signed in March 2005. The agreement also provides a framework for cooperation in the field of security screening. The agreement is being put into effect among other things by the organisation of expert meetings and regular contacts between the heads of the services. The declaration further states that the countries may decide to set up ad hoc cooperation arrangements with a view to conducting specific investigations and that GISS will provide technical assistance to NASS and ASS. For example, GISS assisted NASS in a reorganisation process aimed at enabling NASS to improve its contribution to counterterrorism activities within the Kingdom. GISS also arranges training and traineeships in consultation with NASS and ASS.

The intelligence and security structure within the Kingdom will change on a number of points due to constitutional reforms. The country of the Netherlands Antilles will cease to exist. The islands St. Maarten and Curaçao will acquire country status within the Kingdom and in that capacity will become responsible for their own national security. The Netherlands Antilles Security Service (NASS), which has its head office on Curaçao, will be transformed into the Curaçao Security Service. St. Maarten wishes to establish a security service of its own. Bonaire, St. Eustatius and Saba, also known as the BES islands, will have a special position giving them a direct tie with the Netherlands. Within the Netherlands form of government the BES Islands will each be set up as a public body and will thus come to fall under the full responsibility of the Netherlands. The Final Declaration on the

[62] *Bulletin of Acts and Decrees* 1995, 233.
[63] *Government Gazette* 2002, no. 10, p. 7.

future political position of the BES island[64] does not include agreements on national security or the intelligence and security structure in the new situation. It was agreed, though, that upon the introduction of the new government structure the Antillean laws currently in force on the islands will be gradually superseded by Dutch law, with or without adjustment to the specific situation on the islands. In this context the Intelligence and Security Services Act 2002 (the ISS Act 2002) will obviously enter into effect on the BES islands as well. The tasks and responsibilities of GISS and the oversight over this service will then also extend to include the BES islands. This means that the Committee's reviews will cover a wider territory as well. A proposal amending the ISS Act 2002 in connection with the constitutional changes is currently being prepared.

13. Coordination between GISS and DISS

It is stated in legislative history that it has been agreed that GISS will maintain contacts with civil intelligence and security services and DISS with defence intelligence and security services and with liaison intelligence services. Where the performance of the services' tasks so requires, the heads of GISS and DISS inform each other when it has to contract defence or civil services, respectively.[65]

The Agreement laying down further rules for the cooperation between GISS and DISS includes an article on international cooperation. [66] It provides *inter alia*:

> 'GISS and DISS maintain international contacts, each on the basis of its own mandate. The head of GISS and the director of DISS inform each other periodically about their international contacts to safeguard that the interests to be served by the services are not harmed.

In actual practice it is sometimes difficult to distinguish between civil and defence intelligence and security services. Not all countries have an exclusively civil and an exclusively defence intelligence and/or security service. Often there is an internally oriented security service and an externally oriented intelligence service. Where these foreign services employ both civilian and military personnel, it is difficult to determine which service must be deemed to be a civil service and which one a defence service.

On the whole, GISS and DISS each have a different network of counterparts with which they cooperate. In practice, however, it is not the case that GISS cooperates exclusively

[64] Annex to *Parliamentary Papers II* 2006/07, 30 800 IV, no. 5.
[65] *Parliamentary Papers II* 1997/98, 25 877, no. 3, p. 73.
[66] *Government Gazette* 2006, no. 35, p.11.

with civil services and DISS maintains contacts exclusively with defence services. The Committee endorses the view that such a strict separation of the services' contacts is indeed not feasible in practice. Even where it is possible to distinguish between civil and defence services in another country, it may still be important for the performance of their respective tasks that GISS and DISS maintain contact or cooperate with that country's defence service or civil service, respectively.
In order to safeguard that the interests to be served by GISS and DISS are not affected and that the services are not hampered in the proper performance of their tasks, a certain degree of coordination between GISS and DISS is necessary. It is particularly important in this context that the services inform each other of the contacts they are maintaining with counterparts in other countries with which both of them cooperate. This is not only necessary to prevent GISS and DISS from unintentionally hindering each other but also to present a united face to the outside world and avoid a situation in which foreign counterparts can play them off against each other and unintended rivalry can arise at the expense of the cooperation. The need for cooperation with foreign counterparts is all the more important where GISS and DISS jointly carry out operations in cooperation with foreign services.

In this investigation the Committee has not found any indications thatn in practice, the cooperation of GISS and DISS with foreign services was insufficiently coordinated or that this led to problems.[67] Contacts between GISS and DISS are frequent, both at management level and between employees at the operational level. The two services cooperate to a greater or lesser extent in all areas of attention and operational areas that the services have in common. This makes it fairly feasible for the two services to achieve a certain degree of coordination. GISS and DISS regularly consult with each other about their international contacts and how they deal with their foreign relations. Insofar as the third-party rule permits, GISS and DISS share information obtained from counterparts that may be relevant to the other service and do so actively, i.e. on their own initiative. GISS and DISS also coordinate operations in which the two services operate jointly in cooperation with foreign services. In this regard, too, the Committee has not found any evidence that in actual practice the coordination between the two services created obstacles in the cooperation or otherwise led to problems.

[67] See also, however: CTIVD Review Report no. 5B on the Review Committee's investigation into the legitimacy of the investigation by GISS into the proliferation of weapons of mass destruction and means of delivery, *Parliamentary Papers II* 2005/06, 29 924, no. 5 (annex). To be consulted at www.ctivd.nl.

14. Conclusions and recommendations

14.1 The Committee's investigation has shown that there is unwanted interference in the Netherlands by several foreign intelligence services, also by services with which GISS is cooperating more or less intensively. After identifying sovereignty violations by intelligence services of other countries, GISS usually takes timely action and appropriate measures tailored to the situation. (section 4)

14.2 It is the opinion of the Committee that GISS should exercise utmost restraint in cooperating with services of countries that have no or hardly any tradition of democracy and where human rights are violated (on a structural basis). The position that all cooperation should be precluded is not supported by the ISS Act 2002 and the legislative history of the Act and could, in practice, lead to undesirable and even disastrous situations.

The Committee shares the view that in an actual case it is virtually impossible for GISS to find out whether information coming from a foreign intelligence or security service was obtained by torture. This makes it all the more important that GISS, before and while it cooperates with a foreign intelligence or security service, assesses carefully to what extent the human rights situation in a country constitutes an obstacle to cooperation with the relevant service of that country.

It is the opinion of the Committee that if GISS suspects that a foreign service is using or will use information provided or to be provided by GISS for unlawful purposes, GISS must refrain from providing (further) information. Likewise, if GISS actually has concrete evidence that information obtained from a foreign service was obtained by torture, it will have to refrain from using this information. GISS will then have to terminate the targeted cooperation with the foreign service. It is only in highly exceptional emergencies that GISS may (or even must) depart from this rule. The Committee has not come across such a situation in its investigation. (section 5.1)

14.3 The Committee has found that the foreign services with which GISS maintains the closest cooperative relations are generally assessed to be highly professional and sufficiently reliable. (section 5.2)

14.4 The Committee considers that it may be in the interest of national security to keep the lines of communication with all foreign services open. Keeping open the lines of communication with a specific foreign service does not mean that GISS may immediately start cooperating with it on a substantive level. (section 5.3)

14.5 The Committee has found that taking stock of the quid pro quo balance and keeping it up to date is a difficult task. GISS recently initiated some policy reforms to make

better internal use of the *quid pro quo* balance. The Committee applauds these initiatives. The Committee notes that the initiatives underline the need for a central department, which is capable of keeping track of the cooperative relations and, where necessary, adjusting them. (section 5.5)

14.6 The Committee has established that in practice GISS often does not make the general assessments whether or not to enter into a cooperative relation or does so only to a limited extent. There is no structured decision making for each individual foreign service separately on the possibilities of entering into a cooperative relation with the foreign service.

The Committee has established that in concrete operational cases GISS does assess whether a specific way of cooperating with a specific service in a particular situation is permissible. It is the opinion of the Committee that GISS rightly includes the circumstances of the specific case in its assessment whether cooperation is permissible in a particular situation. The Committee draws attention, however, to the fact that the procedure of exclusively making such ad hoc assessments is too limited and may have undesirable consequences.

It is the opinion of the Committee that GISS must first make a fundamental assessment of the extent to which the criteria set for cooperation are satisfied and must do so at management level and for each individual foreign service separately. Subsequently, in a concrete (operational) case the result of balancing the various interests involved can be examined against the general assessment of the foreign service. It is the opinion of the Committee that this system will do justice to both the restraints on cooperation with foreign services set forth in the law and legislative history, and daily practice in which actually cooperating with a counterpart may be essential to the adequate performance of its statutory tasks by GISS.

The Committee observes in this context that this is not and should not be a static process. While the cooperative relation with a foreign service continues and develops, GISS may at any time adjust the assessment of the service in question. But it must do so on the basis of the generally applicable criteria for cooperation, supported by reasons and at the proper level.

The Committee recommends GISS to put in place a decision-making procedure for entering into or intensifying cooperative relations with foreign services which will ensure that the fundamental assessment of the extent to which the applicable criteria for cooperation are satisfied is carried out at management level for each foreign service individually. (section 6.1)

14.7 The Committee has found that by its nature GISS cooperates more smoothly with security services than with intelligence services. (section 6.2.1)

14.8 In recent years the cooperation with foreign services with which GISS has no long-term tradition of cooperation but does cooperate intensively in certain investigation areas has increased considerably, both in intensity and in volume. (section 6.2.2)

14.9 Relations with services of which it can be doubted whether they satisfy the criteria for cooperation were further developed, in particular after the attacks in the United States in 2001 and after the attacks in Madrid in 2004. Initially, cooperation with these services increased in the field of counterterrorism. (section 6.2.3)

14.10 The Committee has found that in actual practice the Foreign Relations department plays a role that is chiefly facilitating.

The Committee's investigation has shown that the teams and departments within GISS which cooperate with foreign services do not or did not always proceed expeditiously in informing the Foreign Relations department of their cooperation activities.

Committee has found that in practice the steering role of the Foreign Relations department has not taken shape sufficiently.

The Committee considers it advisable that GISS, for internal use, expressly lay down the different areas of responsibility of the Foreign Relations department insofar as this has not been done yet, and recommends GISS to ensure that internal policies are adequately implemented in practice. (section 6.3)

14.11 The Committee has established that GISS conducts a policy of strict compliance with the third party rule in regard to information received from foreign counterparts. GISS' practical implementation of the policy is also adequate. For due care purposes the Committee considers it important that the third party rule is expressly included in writing in messages to foreign intelligence and security services and recommends GISS to make it standard procedure to state the rule. (section 7.2)

14.12 It is the opinion of the Committee that decisions about providing personal data to counterparts should at least be taken at team leader level in all cases. This has meanwhile become adopted policy at GISS. The Committee further holds the opinion that in the case of personal data being provided by way of rare exception - urgent necessity to provide personal data because of an unacceptable risk to society and its citizens that calls for prompt action – the decision to do so must always be taken at service management level. The Committee recommends GISS to bring its internal rules and practice regarding the provision of personal data to foreign services into line with this. (section 7.3)

14.13 The Committee has established that GISS increasingly exchanges (personal) information with foreign intelligence and security services of which it is doubtful whether they satisfy the prescribed criteria for cooperation. The Committee points out that in a certain field the assessments made by GISS on this issue are in practice increasingly stretching the limits. (section 7.3)

14.14 The Committee has established that in some cases GISS acted unlawfully when it provided personal data to foreign intelligence and security services. In three cases GISS provided personal data to counterparts of which it is doubtful whether they satisfy the criteria for cooperation without the requirement of (urgent) necessity being satisfied. In two cases, moreover, GISS sent along personal data of a person other than the person to whom the provision of data primarily related (third parties) without this being necessary. In one single case personal data was provided without the subsidiarity principle being satisfied and GISS could have used a less infringing means. Finally, the Committee came across one case in which personal data was provided to a foreign service of which it is doubtful whether it satisfies the prescribed criteria for cooperation, while GISS is no longer able to retrieve the reasons for providing the personal data.
The Committee recommends GISS to exercise greater care in providing personal data to foreign services and to act in accordance with all the applicable statutory provisions as well as its own internal rules. (section 7.3)

14.15 The Committee holds the opinion that in some cases the assessment underlying decisions to provide personal data is very limited in scope and has established that in many cases the assessment has not been laid down in writing. The Committee recommends that GISS, for due care purposes, keep written records of the thorough assessments that are or should be made prior to providing personal data to a foreign service of which it may be doubted whether it satisfies the prescribed criteria for cooperation.

14.16 The Committee has established that in seven cases personal data was provided to foreign services of which it may be doubted whether they satisfy the prescribed criteria for cooperation while no permission to do so had been given at the appropriate level. The Committee has further established that in many cases the permission to provide personal data has not been laid down in writing. The Committee recommends that GISS, for due care purposes, record in writing any permission given to provide personal data to a foreign service (section 7.3)

14.17 The Committee has found that in many cases when GISS provides information to foreign services it does not give any indication of the degree of reliability or a

reference to the document or the source from which the information is derived. GISS thus fails to comply with the provision of section 12(4), ISS Act 2002. (section 7.3)

14.18 The Committee has found that in some cases it proved difficult for GISS to retrieve fully to which foreign services a message was provided. In this regard the Committee draws attention to the obligation imposed on GISS by article 42, ISS Act 2002, to keep records of the provision of personal data. (section 7.3)

14.19 The Committee has found that GISS only rarely considers certain forms of cooperation to be assistance within the meaning of article 59(4), ISS Act 2002, which requires the prior permission of the Minister of the Interior and Kingdom Relations. The Committee holds the opinion that the interpretation given by GISS to the concept of assistance pursuant to article 59(4), ISS Act 2002, is too narrow. In the opinion of the Committee the decisive criterion should not be whether a supporting activity may be ranged under a team assignment or may have aspects in common with an investigation, but whether the supportive form of cooperation can actually contribute to an ongoing investigation by GISS.
The Committee has established that GISS also does not range under article 59(4), ISS Act 2002, assistance rendered to foreign services without involving the exercise of special powers. It is the opinion of the Committee that these forms of assistance must formally be deemed to fall under article 59(4), ISS Act 2002, too.
The Committee has established that in the cases in which GISS rendered assistance within the meaning of article 59(4), ISS Act 2002, to a foreign service but did not regard it as such, it wrongly omitted to request the Minister of the Interior and Kingdom Relations for permission to render the assistance.
The Committee recommends GISS to give a more stringent interpretation to the term assistance within the meaning of article 59(4), ISS Act 2002, and to bring the internal (permission) procedures into line with the stricter interpretation. (section 8.2)

14.20 The Committee has found that the requirement of permission to request a foreign service to render assistance has not been embodied in the law or an internal rule of GISS. The Committee considers it advisable that the requirement of permission for making requests for assistance to foreign services be laid down expressly and recommends GISS to ensure that this is done. The requirement can be linked to the permission which is normally required for exercising the power to which the request relates. (section 8.3)

14.21 The Committee has established that a number of requests for assistance involving the exercise of special powers made to foreign services of which it is doubtful

whether they satisfy the prescribed criteria for cooperation did not satisfy the requirements of necessity, proportionality and/or subsidiarity. In three cases the request for assistance made to the foreign service could have such harmful consequences for the person(s) concerned as to be disproportionate to the intended purpose of GISS. In two of these cases, moreover, it would have been sufficient for GISS to use a means less injurious to the person(s) concerned, for example not requesting the assistance of the foreign service but performing activities itself. It is the opinion of the Committee that GISS should not have requested the assistance of the foreign services of which it was doubtful whether they satisfied the prescribed criteria for cooperation.

The Committee has established that some requests for assistance from GISS to foreign services are worded in a way that leaves the foreign service much scope for deciding how to act in meeting the request. The Committee also noticed that GISS does not always stipulate additional guarantees from the foreign services in question that may limit the potential detriment to the person(s) concerned. From a due care perspective the Committee believes that it would be better for GISS to make its requests for assistance to foreign services as explicit as possible and where possible state the limits of the requested assistance.

The Committee recommends that GISS, prior to asking a foreign service for assistance involving the exercise of special powers, make a thorough assessment of the necessity, proportionality and subsidiarity of the request to be made and record the assessment in writing. The Committee thinks it advisable that the obligation to state reasons in writing be expressly included in the permission procedure for requests to foreign services recommended by the Committee. (section 8.3)

14.22 It has not emerged from the Committee's investigation that GISS, when carrying out joint operations with counterparts, failed to satisfy the conditions imposed on such operations by law and legislative history. (section 9.2)

14.23 It is the opinion of the Committee, when GISS cooperates in security screenings with foreign counterparts of which it is questionable whether they satisfy the prescribed criteria, that the protection of the person screened requires that GISS takes precautionary measures (as mentioned above) and applies them strictly. The Committee has established, however, that in actual practice the precautionary measures were not always applied or not applied strictly. The Committee recommends that GISS strictly apply the prescribed precautionary measures aimed at protecting persons involved in a security screening and in all cases expressly include the conditions laid down with respect to foreign services subject to doubts in the written request. (section 10)

14.24 The Committee's investigation has shown that GISS also cooperates for security screening purposes with services of which it may be doubted whether they satisfy the prescribed criteria, without the service management having given permission for the cooperation after following through a decision procedure. No precautionary measures have been laid down in a country information file with respect to these services. The Committee has also established that GISS already was or is cooperating with some services while the decision procedure had or has not been followed through yet. The Committee considers this improper and holds the opinion that GISS must always first follow through the decision procedure before it may start cooperating. The Committee recommends that GISS, before starting to cooperate with a foreign service for security screening purposes, first assess in accordance with the internal decision procedure whether the service qualifies for cooperation and if so, subject to which conditions. (section 10)

14.25 The Committee holds that it is in the interest of the persons involved in a security screening that they are expressly informed in all cases that GISS may make inquiries with a foreign counterpart. The Committee recommends that GISS include a passage to this effect in the Personal Information Form which a person concerned must fill out and sign before GISS may start a security screening investigation. (section 10)

14.26 The Committee has found that the list in the Manual of GISS of countries with which GISS cooperates for security screening purposes is outdated. The Committee recommends, with a view to due care, that the list of the Manual, which is accessible to GISS employees, be brought into line and kept identical with the list at the Security Screening department. (section 10)

14.27 The Committee's investigation has shown that GISS is actively involved with several multilateral fora. (section 11)

14.27 In this investigation the Committee has not found any evidence that the cooperation of GISS and DISS with foreign services was insufficiently coordinated or that this led to actual problems. (section 13)

Thus adopted at the meeting of the Committee held on 12 August 2009.

Review Report CTIVD no. 24

On the lawfulness of the performance by GISS of its obligation to notify

Table of contents

Review Report CTIVD no. 24

On the lawfulness of the performance by GISS of its obligation to notify

SUMMARY

When the General Intelligence and Security Service (GISS) exercises certain special powers that are listed exhaustively in the Intelligence and Security Services Act 2002 (further referred to as the ISS Act 2002), this creates an obligation to notify, so Article 34 of the Act provides. Special powers that are subject to the obligation to notify are, for example, telephone tapping and forced entry into a home. The obligation to notify means that five years after a special power has been exercised GISS must examine whether a report of the exercise of the special power can be submitted to the person with regard to whom the power was exercised. The purpose of the obligation to notify is to (better) enable individuals to effectuate their fundamental rights.

It is not possible in all cases to notify the person concerned. The obligation to notify may lapse, be suspended or be cancelled. The examination preceding notification may lead to the conclusion that the person concerned cannot be traced or has died. In these cases the obligation to notify lapses. If the notification examination shows that the special power is relevant to the current information level of GISS, the obligation to notify will be suspended until the relevance has ceased. Furthermore, the notification examination may lead to the conclusion that the obligation to notify must be (permanently) cancelled if – briefly stated – notification can reasonably be expected to result in a source of GISS being disclosed, in relations with other countries being seriously damaged, or in a specific use of a GISS method being disclosed. These are the grounds for cancellation.

In forty-three per cent of the cases the notification examination resulted in the conclusion that the person concerned could not be traced. Twenty-five per cent of the notification decisions were decisions to suspend the obligation to notify and in twenty-seven per cent it was decided that a ground for cancellation applied. In the remaining five per cent of the cases the person concerned had died, or a special power had been used in regard of an organisation, or the special power was not exercised after all even though permission to do so had been obtained.

Although no person has been notified so far, the Committee has established that as a rule GISS performed its obligation to notify in conformity with the statutory requirements. In the course of its investigation the Committee encountered a number of exceptional cases.

The Committee has established that in one case GISS did not act in conformity with the statutory requirements when tracing the person concerned. It is the opinion of the Committee that in one case GISS wrongfully decided to suspend the obligation to notify. In addition, it is the opinion of the Committee that in two cases GISS wrongfully decided to invoke source protection as a ground for cancellation. The Committee recommends that GISS reconsider these notification decisions. This does not mean to say, however, that reconsideration would result in notification, because there may be other grounds for deciding not to notify.

The Committee further holds the opinion that there are two points on which the policy adopted by GISS is too narrow. When tracing persons concerned, GISS confines its efforts to an administrative check of its own information system and of the municipal personal records database, in the sense that GISS checks its own information systems to collect identity data in order to be able to do a successful search in the municipal personal records database. It is the opinion of the Committee that GISS' own information systems can also play an independent role and should not be used only as a supplement to the municipal personal records database. It is the opinion of the Committee that GISS may be expected to enquire from the local Regional Intelligence Service or another relevant body within the meaning of section 60 of the ISS Act 2002 whether they happen to have information of their own about the actual abode of a person concerned if the file available to GISS contains indications that such an enquiry may lead to some result. The Committee recommends that GISS adjust its tracing policy on this point. The Committee has no indication that in the cases it investigated the persons concerned could in fact have been traced if GISS had done such a further search, but cannot exclude it, either.
The Committee has established that GISS gives a broad interpretation to the notion of 'ongoing investigation', linking it to threats emanating from certain phenomena in society. The Committee recommends linking the notion as much as possible to actual investigations rather than to societal phenomena. The Committee has established, though, that in practice GISS does indeed seek a link with actual investigations and decided on good grounds to suspend notification, with the exception of the one case mentioned above.

See section 5 of the review report for a detailed overview of the conclusions and recommendations of the Committee.

Review Report CTIVD no. 24

On the lawfulness of the performance by GISS of its obligation to notify

1 Introduction

1.1 The obligation to notify

When the General Intelligence and Security Service (GISS) exercises certain special powers that are listed exhaustively in the Intelligence and Security Services Act 2002 (further referred to as the ISS Act 2002), this creates an obligation to notify, so Article 34 of the Act provides.[1] Examples of special powers subject to the obligation to notify are telephone tapping and forcing entry into a home. The obligation to notify means that five years after a special power has been exercised GISS must examine whether it is possible to inform the person with regard to whom the power was exercised. The purpose of the obligation to notify is to (better) enable individuals to effectuate their fundamental rights. It is not possible in all cases to notify the person concerned. The obligation to notify may lapse, be suspended or cancelled. The examination preceding notification may lead to the conclusion that the person concerned cannot be traced or has died. In these cases the obligation to notify lapses. If the notification examination shows that the special power is relevant to the current information level of GISS, the obligation to notify will be suspended until the information is no longer relevant. In addition, the notification examination may lead to the conclusion that the obligation to notify must be (permanently) cancelled if – briefly stated – notification can reasonably be expected to result in a source of GISS being disclosed, in relations with other countries being seriously damaged, or in a specific use of a GISS method being disclosed.

The *de facto* effective date of the obligation to notify was 29 May 2007, five years after the ISS Act 2002 entered into effect. A letter dated 4 December 2008 regarding an evaluation of the obligation to notify sent by the minister of Internal Affairs and Kingdom Relations (further referred to as: the minister) to the Second Chamber states that there should be no taboo about debating the benefits and necessity of the obligation to notify.[2] The minister thought it too early, however, to conduct the debate at the time. The minister stated that the findings of the Review Committee for the Intelligence and Security Services (further

[1] The ISS Act 2002 uses the term 'submitting a report'. In the legislative history of the Act, however, the term notify is used consistently. This review report will mostly follow the terminology of legislative history..
[2] *Parliamentary Papers II* 2008/09, 30 977, no. 18, p. 7.

to be called: the Committee) would have to be "included in this discussion". The Committee has found that the Second Chamber is amazed that nobody has been notified so far.[3] With the present review report the Committee aims at providing a clear overview of the parameters and the performance of the obligation to notify. In this context it points out that in conformity with the powers assigned by the legislator to the Committee, the present report deals only with the question whether the obligation to notify has been performed lawfully by GISS. Efficiency considerations are not discussed in this review report.

1.2 The Committee's investigation

Pursuant to its review task under Article 64 of the ISS Act 2002, the Committee investigated whether GISS performed its obligation to notify lawfully. Pursuant to Article 78(3) of the ISS Act 2002, the Committee informed the Minister of the Interior and Kingdom Relations and the Presidents of the two Chambers of the Dutch parliament of its intention to conduct this investigation on 23 April 2009. In the course of its investigation the Committee examined the notification decisions – together with the underlying files - that were taken in the period from 29 May 2007 to 11 November 2009, inspected the documents pertaining to the obligation to notify (establishing the parameters) and interviewed various employees of GISS involved in performing the obligation to notify.

One element of the Committee's review task is to monitor whether GISS performed its obligation to notify lawfully. The Committee has been monitoring how the obligation to notify is being performed since the *de facto* entry into force of this obligation. For the purposes of better enabling the Committee to perform this review task, Article 34(2) of the ISS Act 2002 provides that the Committee must be informed if it is not possible to submit a report to the person concerned. The notice to the Committee must state the reasons why the report cannot be submitted.

While it is true that the existence of a ground for suspension does not make notification permanently impossible, the ISS Act 2002 does not preclude the possibility of the Committee being informed in those cases, too. With a view to the Committee's monitoring task the Committee considered it advisable that it should also be actively and periodically informed of the cases in which a ground for suspension applied. By now, GISS is indeed putting this principle into practice.[4] It is the opinion of the Committee that this does justice to the legislator's intention of reinforcing the monitoring task of the Committee.[5]

---

[3] See e.g.: *Parliamentary Papers II* 2008/09, 30 977 and 29 924, no. 22, pp. 6, 8 and 11.
[4] *Parliamentary Papers II* 2008/09, 30 977, no. 18, p. 2.
[5] *Parliamentary Papers II* 2000/01, 25 877, no. 18.

Section 2 discusses the theoretical framework underlying the obligation to notify. Section 3 contains the findings of the Committee. The Committee's concluding observations are laid down in section 4. Section 5 presents the conclusions and recommendations of the Committee.

This review report includes a classified appendix.

1.3 Background of the development of the notification rules

Initially, the obligation to notify the exercise of certain special powers was not included in the legislative proposal for a new law regulating the intelligence and security services (eventually enacted as the ISS Act 2002). The obligation to notify was expressly linked to the obligation to notify arising from Articles 12 and 13 of the Constitution.[6] In the period when the ISS Act 2002 was being drafted, a proposed amendment to Article 13 of the Constitution was pending, which provided that violations of the secrecy of the mail and communications would create an obligation to notify. Article 12 of the Constitution already provided for an obligation to notify of entry into a house against the will of the occupant. The legislator took the position that an obligation to notify already ensued from the provisions of Article 12 and (the new) Article 13 of the Constitution by themselves, and not from any provision of the ECHR. The idea was therefore to link the obligation to notify in the ISS Act 2002 to the entry into force of the pending amended Article 13 of the Constitution. This would mean that the details of the obligation to notify in the new law on the intelligence and security services would not be elaborated until after the amended Article 13 of the Constitution had entered into force. During the legislative process for the new law on the intelligence and security services, however, it was decided, on the insistence of several political groups in parliament, to have the obligation to notify enter into force simultaneously with the original bill.[7]

2 Theoretical framework

2.1 The obligation to notify in relation to the European Convention on Human Rights

In the legislative history of the ISS Act 2002 there are several instances where the government observes that an obligation to notify cannot be derived from the European

[6] See for example: *Parliamentary papers II* 2000/01, 25 877, no. 59, p. 13.
[7] *Parliamentary papers II* 1998/99, 25 877 and 26 158, no. 6, p. 1.

Convention on Human Rights (ECHR).[8] The 1978 judgment *Klass v. Germany* of the European Court for Human Rights (ECtHR) is cited in substantiation of this position.[9] In this judgment the ECtHR examined among other things what is the relation between the obligation to notify and Articles 8 and 13 of the ECHR. Initially, the Council of State, in its opinion on the original legislative proposal for what was to become the ISS Act 2002, explicitly took the position that an obligation to notify could in fact be derived from *Klass v. Germany.*[10] In its opinion on the amended bill, which did include an obligation to notify, the Council of State merely stated that Article 12 of the Constitution in any case imposed an obligation to notify of the forced entry into homes and did not further discuss the case law of the ECtHR in this context.[11]

The issue under consideration in the judgment was the German system of active notification. German law imposes an obligation of active notification. In the German system the obligation to notify lapses, however, if notification is incompatible with the interests of national security. The ECtHR ruled that this did not constitute a violation of Article 8 read with Article 13 ECHR. But the ECtHR emphatically placed the right to being actively notified within the framework of the complex of adequate and effective safeguards from violations of an individual's fundamental rights. The obligation to notify can contribute to such safeguards.

The nature of the *Klass* judgment is, however, casuistic and the ECtHR only examined the question whether, in the circumstances of the actual case, an existing obligation to notify might be restricted because of national security interests. The judgment therefore does not deal with the situation that the national law does not provide at all for an obligation of (active) notification. But the ECtHR did make the following observation regarding the possibility for individuals to subject the legality of the exercise of certain special powers to review a posteriori:

> "As regards review a posteriori, it is necessary to determine whether judicial control, in particular with the individual's participation, should continue to be excluded even after surveillance has ceased. Inextricably linked to this issue is the question of subsequent notification, since there is little scope for recourse to the courts by the individual concerned unless he is advised of the measures taken without his knowledge and thus able retrospectively to challenge their legality."[12]

---

[8] See e.g.: *Parliamentary papers II* 1999/00, 25 877, no. 9, p. 29 and *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 52.

[9] ECtHR 6 September 1978, no. 5029/71 *(Klass. v. Germany)*.

[10] *Parliamentary papers II* 1997/98, 25 877, no. A, p. 2-3.

[11] *Parliamentary papers II* 1997/98, 25 877, no. A, p. 7.

[12] ECtHR 6 September 1978, no. 5029/71, §57 *(Klass. v. Germany)*. The ECtHR again confirmed this position in ECtHR 29 June 2006, no. 54934/00, §135 *(Weber and Saravia v. Germany)*.

The ECtHR goes on to say that notification is not possible in all cases. Notification may not jeopardise the long-term objectives of the investigation that were the reason for exercising a special power. Neither may notification jeopardise the lawful interests of the intelligence service, such as keeping secret sources, methods and current level of information. The above is known as the *jeopardise* criterion.[13] The ECtHR then states that active notification is obligatory:

> "[…] as soon as notification can be made without jeopardising the purpose of the restriction."

In a more recent judgment concerning the obligation to notify (*Association for European Integration and Human rights and Ekimdzhiev v. Bulgaria*) the ECtHR scrutinizes the Bulgarian legal system, which does not have any obligation to notify at all.[14] The ECtHR takes the following grounds.

> "Finally, the Court notes that under Bulgarian law the persons subjected to secret surveillance are not notified of this fact at any point in time and under any circumstances. According to the Court's case law, the fact that persons concerned by such measures are not apprised of them while the surveillance is in progress or even after it has ceased cannot by itself warrant the conclusion that the interference was not justified under the terms of paragraph 2 of Article 8, as it is the very unawareness of the surveillance which ensures its efficacy. However, as soon as notification can be made without jeopardising the purpose of the surveillance after its termination, information should be provided to the persons concerned. By contrast, the SSMA does not provide for notification of persons subjected to surreptitious monitoring under any circumstances and at any point in time. On the contrary, section 33 of the SSMA, as construed by the Supreme Administrative Court, [*CTIVD: The relevant Bulgarian legislation*] expressly prohibits the disclosure of information whether a person has been subjected to surveillance, or even whether warrants have been issued for this purpose. Indeed, such information is considered classified […]. The result of this is that unless they are subsequently prosecuted on the basis of the material gathered through covert surveillance, or unless there has been a leak of information, the persons concerned cannot learn whether they have ever been monitored and are accordingly unable to seek redress for unlawful interferences with their Article 8 rights. Bulgarian law thus eschews an important safeguard against the improper use of special means of surveillance."[15]

---

[13] See for example: *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 86 and *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 53.

[14] ECtHR 28 June 2007, no. 62540/00, §90 *(Association for European Integration and Human rights and Ekimdzhiev v. Bulgaria)*.

[15] *Association for European Integration and Human rights and Ekimdzhiev v. Bulgaria,* §90-91.

In this judgment the ECtHR further takes the ground that in that case, in the given circumstances of the relevant (Bulgarian) law, the fact that there will be no notification constitutes violation of Article 13 ECHR:

> "It thus appears, that, unless criminal proceedings have subsequently been instituted or unless there has been a leak of information, a person is never and under no circumstances apprised of the fact that his or her communications have been monitored. The result of this lack of information is that those concerned are unable to seek any redress in respect of the use of secret surveillance measures against them. Moreover, the Government have not provided any information on remedies – such as an application for a declaratory judgment or an action for damages – which could become available to the persons concerned if they find out about any measures against them […]. In *Klass and Others* the existence of such remedies was not open to doubt."[16]

One cannot simply draw general conclusions from this case law of the ECtHR. These ECtHR judgments are strongly tailored to the actual circumstances of the case. The ECtHR does not prescribe an established system of legal protection but merely requires that the complex of safeguards be adequate and effective. The ECtHR considers notification to be one of the means that may contribute to this complex of actual and effective safeguards. With regard to the Dutch system it is therefore relevant to examine the structure of the complex of safeguards. It is a fact, however, that none of the other safeguards provide for an active obligation to inform an individual that special powers have been exercised in regard to him.[17] *In Association for European Integration and Human rights and Ekimdzhiev v. Bulgaria* the ECtHR states expressly that it considers notification to be an important safeguard against abuse of special powers. It follows from the legislative history that the obligation to notify serves the purpose of informing an individual that special powers have been exercised in regard to him in order to enable him thus to expose allegedly unlawful acts by the services.[18] But the Committee can only infer from the case law of the ECtHR that it attaches value to a system of active notification and that it gives active notification its place within the complex of legal safeguards. In the opinion of the Committee, however, the obligation to notify cannot be considered an obligation ensuing automatically from the ECHR.

---

[16] *Association for European Integration and Human rights and Ekimdzhiev v. Bulgaria,* §101.

[17] What is meant here is legal protection by way of the courts, the Review Committee for the Intelligence and Security Services, the Parliamentary Committee for the Intelligence and Security Services, the complaints procedure before the National Ombudsman and the regulations concerning applications for inspection of files including review of these remedies by the courts and the Committee.

[18] *Parliamentary papers I* 2001/02, 25 877, no. 58a, p. 17.

2.2 The obligation to examine whether notification is possible

2.2.1 Link to certain special powers

As was already briefly mentioned above, the obligation to notify is linked to the exercise of a number of special powers that are listed exhaustively in Article 34(1) of the ISS Act 2002. These are the power to open letters and other addressed consignments pursuant to Article 23(1) of the ISS Act 2002, the power to use a technical device for tapping, receiving, recording and intercepting any form of conversation, telecommunication or data transfer by means of an automated work, irrespective of where this takes place (for example telephone or e-mail tapping) pursuant to Article 25(1) of the ISS Act 2002, the power to select non-specific non-cable-bound telecommunication on the basis of identity or any technical characteristic (for example intercepting and listening in to satellite communications) pursuant to Article 27(3)(a) and (b), and the power to enter a home without the consent of the occupant pursuant to Article 30(1) of the ISS Act 2002. It follows from the above that the exercise of special powers not included in Article 34(1) of the ISS Act 2002 is not subject to the obligation to notify.[19] The obligation to notify comes into existence by the actual exercise of a special power regardless of whether the exercise has yielded any data.

2.2.2 Possible results of the examination whether notification is possible

Five years after a special power has been exercised the relevant minister is required to examine whether the person concerned can be notified of this fact. Pursuant to Article 4.1 read with Article 4.11 of the Decree of 2008 of the Ministry of the Interior and Kingdom Relations concerning mandates (further referred to as the Ministerial Mandate Decree 2008) the minister's obligation to examine whether notification is possible is mandated to the (substitute) head of GISS.[20] This examination can have four possible results. First of all an examination pursuant to Article 34(5) of the ISS Act 2002 may have the result that there will be no notification because notification is not reasonably possible. It follows from the legislative history that this is the case if the person concerned cannot be traced or has died (the obligation to notify lapses).[21] In the second place it is possible that notification must

[19] Examples are access to places not being homes (businesses) pursuant to Article 30(1) of the ISS ACT 2002, surveillance and shadowing persons pursuant to Article 20(1) ISS ACT 2002, infiltration of organisations by an agent of GISS pursuant to Article 21(1)(a) of the ISS ACT 2002 and requesting traffic data pursuant to Article 28(1) of the ISS ACT 2002.

[20] Decree of 2 February 2009, Government Gazette 2009, 20.

[21] *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 55.

definitely never take place on the basis of one of the grounds for cancellation mentioned in Article 34(7) of the ISS Act 2002 (the obligation to notify is cancelled). If any of these grounds for cancellation applies, this causes the obligation to notify to lapse. A third possible result is that the examination shows that notification would disclose the current level of information of the service as provided in Article 34(6) read with Article 53(1) of the ISS Act 2002 (the obligation to notify is suspended). In this case notification will be suspended for a period of one year each time. The obligation to examine whether notification is possible will revive annually as long as the minister holds the opinion that notification is not yet possible in view of the provision of Article 34(6) of the ISS Act 2002. Finally, the result may be that there are no statutory impediments to performing the obligation to notify and that the service must therefore proceed to send notification to the person concerned.

The Committee has found that it is not possible to deduce a prescribed order of examination from the ISS Act 2002 or from its legislative history. Moreover, GISS is not required to examine all possible grounds for not notifying. If, for example, the person concerned cannot be traced, GISS need not examine whether a ground for cancellation of the obligation to notify applies as well.

2.2.3 Reasonable term

If notification is possible, it should be effected as soon as possible. In the opinion of the Committee this means that the examination preceding the actual performance of the obligation to notify must also be carried out fairly expeditiously. It is the opinion of the Committee that GISS must have completed the entire procedure from the moment when the obligation to examine whether notification is possible arises until the eventual issue of the notification report to the person concerned within a reasonable period. It depends on the specific circumstances of the case what may be considered a reasonable term.

2.2.4 The person to be notified

One of the most elementary questions that must be answered is the question who is to be notified. With regard to this question the law says that the obligation to notify exists with respect to persons in regard to whom one of the special powers enumerated in Article 34(1) of the ISS Act 2002 has been exercised. The Committee distinguishes four categories.

In the first place there are special powers exercised in regard to persons who, because of the goals they are pursuing or because of their activities, give cause for a serious suspicion

that they pose a threat to the democratic legal system or to the security or other vital interests of the state (Article 6(2)(a) read with Article 13(1) of the ISS Act 2002). These persons are called targets. The exercise of a special power by virtue of Article 34(1) of the ISS Act 2002 in regard to a target is subject to the obligation to notify.

The service may also exercise a special power in regard to a person who cannot be considered a target but in whose case the exercise of the special power may result in a considerable improvement of the information level regarding a target. An example is the situation where a target is very security-minded and information on the target can only be obtained through a person in the target's environment. In this exceptional case the law permits the service to exercise special powers in regard to a *non-target*, as they are called.[22] It is the opinion of the Committee that the obligation to notify is fully applicable in regard to such a non-target as well, since this case, too, concerns the purposeful invasion of privacy. And the purpose of the obligation to notify is to protect the rights of persons whose privacy is invaded.

On the basis of the service's intelligence task abroad, moreover, special powers are also exercised in regard to persons concerning whom data must be processed as part of an investigation regarding other countries (Article 6(1)(d) read with Article 13(1)(c) of the ISS Act 2002.[23] Whenever there is a purposeful invasion of privacy, the obligation to notify applies in regard to those persons as well.

A distinction must be made between the above and cases involving third parties. A third party is any person who cannot be put in either the category of targets or the category of non-targets. This may, for example, be any person with whom the person in regard to whom the special power is exercised, communicates. Another example is a person making sporadic use of the telephone of the person whose telephone is being tapped. Like GISS, the Committee holds the opinion that there is no obligation to notify third parties, since there is no purposeful invasion of their privacy. This issue was explicitly raised and discussed in the legislative history of the ISS Act 2002.[24]

---

[22] Article 6(2)(a) ISS Act 2002 reads "conducting investigations regarding organisations and persons […]". In this context, however, Article 13(1)(e) of the ISS Act 2002 requires that the data to be processed "[…] is necessary to support the proper performance by the service of its statutory tasks".

[23] These persons are not called targets because the investigation is not primarily aimed at them but at the activities of the countries mentioned in the foreign intelligence task designation order.

[24] *Parliamentary papers I* 2001/02, 25 877, no. 58a, p. 22-23.

2.2.5 Exercise of a special power in regard to an organisation

The above centred on the exercise of a special power in regard to a natural person. It is also possible, however, for special powers to be exercised in regard to an organisation. But the law only imposes an obligation to notify natural persons. Nonetheless, the exercise of a special power in regard to an organisation frequently involves the invasion of the private life of natural persons as well. It is relevant to examine in which cases the exercise of special powers in regard to an organisation may give cause to notify a natural person.

When assessing this matter, GISS will consider two factors. The first regards the nature of the information the service wishes to gather. A relevant aspect is whether it concerns the organisation as a whole, or specific members of the organisation as well. The second factor regards the domain within which the power is exercised. For this purpose it must be examined whether the power is aimed primarily at communications within the scope of work or at communications within the scope of an individual member's private life. It is the opinion of GISS that a person only qualifies for notification if the investigation is wholly or partly aimed at an individual member of the organisation or if the communications take place within the scope of this member's private life.
The Committee points out that the case law of the ECtHR shows that a person's work environment may also fall within his private life within the meaning of Article 8 ECHR.[25] In the opinion of the Committee a person should therefore qualify for notification if special powers have been exercised in regard to him in the context of an investigation which, though primarily targeting an organisation, also aimed at gathering information originating from this person. In this case the question whether tapped communications took place in the context of work or of the person's private life does not play a significant role.

2.2.6 Submitting a notification report

If it follows from the examination that a report can be submitted, this should be done as soon as possible. Article 34(3) of the ISS Act 2002 contains a limitative list of what the report must contain. It also follows from this paragraph that the report must be in writing. It is a concise report. It only states the identity of the person concerned, the special power that was exercised, the person or body who ordered the exercise of the power including the date of the order and the period during which the special power was exercised (Article 34(3), (a) through (e), of the ISS Act 2002).

[25] See e.g.: ECtHR 25 October 2007, no. 38258/03, §48 *(Vondel v. The Netherlands)*.

The person concerned is not informed of the investigation in the context of which the special power was exercised nor of the reasons for exercising the special power. If the person concerned wishes to try and place the special power in a specific context, he may, pursuant to Article 47(1) of the ISS Act 2002, request GISS to allow him to inspect the personal data relating to his person that are in the possession of the service.

2.3 Lapsing of the obligation to notify

2.3.1 Possibility of tracing the person concerned

Pursuant to Article 34(5) of the ISS Act 2002 the obligation to submit a report (i.e. the obligation to notify) lapses at the moment when it has been established that it is not reasonably possible to do so. Notifying the person concerned is not reasonably possible if this person cannot be traced or has died.[26] In order to be able to perform the obligation to notify, GISS must reasonably be able to trace the place of abode of the person concerned. When the person concerned dies, the obligation to notify applying in regard to him does not devolve on a surviving dependant.

2.3.2 Reasonable effort

Legislative history shows that GISS may be expected to make a reasonable effort in its attempts to trace the person concerned.[27] It is the opinion of the Committee that a reasonable effort comprises in any case checking GISS' own information systems and searching the municipal personal records database.[28] The fact that a person concerned is meanwhile no longer in the Netherlands will as a rule result in the person concerned no longer being traceable by reasonable effort, since it would go too far to approach foreign authorities for the purposes of an extensive search. If, however, the place of abode abroad of the person concerned can be traced by simple means, this person must be notified.[29] This may be the case, for example, for a person living abroad whose place of abode is generally known.

The Committee has established that GISS, when tracing a person concerned, usually confines its efforts to searching its own information systems and the municipal personal

[26] *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 55.
[27] *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 92.
[28] Pursuant to the Municipal Database (Personal Records) Act, GISS has direct access to the municipal personal records database.
[29] *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 92.

records database, in the sense that GISS' search of its own information systems serves to collect identity data in order to enable GISS to do a successful search in the municipal personal records database. It is the opinion of the Committee that GISS' own information systems can also play an independent role and should not be used only as a supplement to the municipal personal records database. Legislative history shows that if this search does not yield results, the obligation to notify lapses only if the person concerned also cannot be traced otherwise with a reasonable effort. It is the opinion of the Committee that GISS may be expected to enquire of the local Regional Intelligence Service (*RID*) or another relevant body within the meaning of section 60 of the ISS Act 2002 whether they happen to have information of their own about the actual abode of a person concerned, if the file available to GISS contains indications that such an enquiry may lead to a result.[31] Upon the entry into force of the post-Madrid measures, so the Committee holds, these efforts will include consulting the Immigration and Naturalisation Service (*IND*) of the Ministry of Justice.[32] There is close cooperation in particular with the *RID* and by virtue of Article 60 of the ISS Act 2002 intelligence information at the disposal of the *RID* forms part of GISS' own systems.[33] Information at the disposal of the *RID* in the context of its public order task can also contain data that are relevant to the traceability of a person concerned. Mention of the actual abode in the file on the person concerned, for example in a subsequent official report, may be an indication that it may be useful to do a check at the *RID*.

GISS holds the opinion that consulting other databases than the municipal personal records database has no added value. If such a database yields an indication of the abode of the person concerned, this will still not give absolute certainty. GISS has pointed out that the integrity of such databases is not an established fact.
The Committee has established, however, that the processing of data in the municipal personal records database is likewise dependent on the information provided by individuals about their place of abode. It cannot be excluded that an individual does not really live at the address stated in the municipal personal records database. In this respect the Committee finds that it is also not possible to obtain absolute certainty about the abode of the person concerned by checking the municipal personal records database. It is the opinion of the Committee that sending the notification by registered mail constitutes sufficient safeguard against issuing the notification letter to the wrong person.

---

[30] *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 55.

[31] Sources within the meaning of Article 60 of the ISS Act 2002 are the chief officer of a police force, the commander of the Royal Military Constabulary and the director-general of the tax and customs administration of the ministry of Finance.

[32] The post-Madrid measures include a proposal also to bring the chief director of the Immigration and Naturalisation Service (IND) within the scope of operation of Article 60(1) of the ISS Act 2002. See: *Parliamentary papers II* 2005/06, 30 553, no. 2, p. 9 and 32.

[33] See on this subject CTIVD Review Report no. 16 on the investigation of the cooperation between GISS and the Regional Intelligence Services and the Royal Military Constabulary, respectively, *Parliamentary papers II* 2008/09, 29 924, no. 22 (appendix), available [in Dutch] at www.ctivd.nl.

The Committee and GISS have discussed this issue, but so far GISS has not adopted the recommendation of the Committee. In response to the Committee's recommendation, however, GISS tried, in random cases, to trace a number of persons by checking the police registers. This did not yield useful results that could lead to a person concerned being traced. If a result was obtained, so GISS said, it had to be checked again against the municipal personal records database in order to obtain certainty about the person's abode. The same applied with regard to checking data available at the Tax and Customs Administration, the social insurance bank *SVB* and the Government Road Transport Agency *RDW*. The lack of any concrete results confirmed GISS in its conviction that consulting these registers is neither advisable nor useful.
The Committee points out, however, that this was merely an isolated test involving only a small number of cases. It is the opinion of the Committee that it is scarcely possible to draw general conclusions about the usefulness of such searches from this test. It is quite possible that in some cases searching police registers in particular can indeed lead to some result, for example if the actual abode of the person concerned is mentioned in a statement made to the police.
The Committee further stated that agencies within the meaning of Article 60 of the ISS Act 2002 should only be consulted if there are *indications* that this will be of some use. This principle was not included in the random test done by GISS. The Committee therefore maintains its recommendation to adjust the tracing policy on this point.

However, as will be described below in section 3.3, the Committee has found no indication that in the cases it investigated the persons concerned could have been traced if GISS had made this further search, but cannot exclude it either.

2.4 Suspension of the obligation to notify

2.4.1 Protection of current level of information

Article 34(6) of the ISS Act 2002 provides that the obligation to notify is suspended if submitting a notification report would disclose the current level of information of the service.[34] In determining when it is appropriate to postpone notification, the legislator has sought a link with the ground for suspension laid down in Article 53(1) of the ISS Act 2002 which applies in the context of the rules pertaining to applications for inspection of files.[35] Article 53(1) of the ISS Act 2002 provides as follows.

[34] *Parliamentary papers II* 2000/01, 25 877, no. 58, p. 38.
[35] These are applications within the meaning of Article 46 of the ISS Act 2002.

"1. An application as referred to in Article 47 will in any case be refused if:
a. data relating to the person making the application has been processed for the purposes of any investigation, unless:
1°. the data was processed more than five years ago,
2°. since then, no new data relating to the person making the application has been processed for the purposes of the investigation for the purposes of which the original data was processed, and
3°. the data is not relevant to any ongoing investigation;
b. no data relating to the person making the application has been processed."

If an application for inspection of files must be refused pursuant to Article 53(1) of the ISS Act 2002, the obligation to submit a notification report will be suspended, too. Where the point is to prevent disclosing the current level of information, it is irrelevant whether this happens on GISS' own initiative or in response to an application for disclosure from the person concerned. Moreover, notification may in practice lead to an application for inspection of files. The legislative history shows that it would be inconsistent if the two sets of rules would not use the same assessment framework as regards the term.[36]

Article 34(6) of the ISS Act 2002 should be read together with paragraph (1) of the same Article. If a ground for suspension exists, this ground for suspension applies for one year at a time. After the expiry of one year, GISS must again examine whether the ground for suspension is still valid. Suspension emphatically cannot lead to cancellation.[37] Each time it is examined on an annual basis whether the case still involves current data. This annual examination continues until it is possible to notify.

2.4.2 Link with Article 53(1) of the ISS Act 2002

In assessing whether a ground for suspension applies, two scenarios can be recognized. On the one hand it is possible that since the exercise of the special power to be notified, new data relating to the person concerned has been processed in connection with the investigation for the purposes of which the special power was exercised (Article 53(1)(a)(2) of the ISS Act 2002). In this case it can be said that the person concerned is currently still under surveillance. On the other hand it is possible that the data in question is still relevant to an ongoing investigation (Article 53(1)(a), at 3, of the ISS Act 2002). If for example the results of a certain telephone tap are still relevant to an ongoing investigation, this level of information should not be revealed by submitting a report on the exercise of the telephone tapping power in question.

[36] *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 90.
[37] *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 58.

The ground for suspension specifically focusing on the fact that the person concerned is currently still under surveillance will not easily give rise to discussion. If the person concerned is still drawing the attention of GISS in connection with the relevant investigation, notifying this person may lead to a deterioration of the possibility to collect data on this person.

2.4.3 Ongoing investigation

The provision of Article 53(1)(a), at 3, is open to several interpretations, with the term 'ongoing investigation' in particular giving rise to discussion. The Committee has established that GISS rightly proceeds on the basis of the principle that it must always be determined on a case by case basis whether there still is an ongoing investigation.
It is important, however, to state how broadly this term may be interpreted. The Committee has found that GISS uses a fairly broad definition of the term 'ongoing investigation'. An internal policy document of GISS shows that with respect to the a-task (within the meaning of Article 6(2)(a) of the ISS Act 2002) the term ongoing investigation is understood to mean "the complex of activities of a service aimed at making visible the threat posed by phenomena in society to one or more of the vital interests of the state as mentioned in the law". In connection with the d-task (within the meaning of Article 6(2)(d) of the ISS Act 2002), an ongoing investigation is understood to mean "the complex of activities performed on the grounds of a designation within the meaning of the designation order of the prime minister, in which he designates the matters to be investigated by GISS pursuant to Article 6(2)(d) of the ISS Act 2002."

The Committee particularly draws attention to the broad interpretation given to the term 'ongoing investigation' in connection with the a-task. GISS has chosen to link this to the threat posed by certain phenomena in society. Examples of such phenomena are 'islamic terrorism', 'radicalisation' and 'violent political activism'. This policy may have the result that as long as islamic terrorism is being investigated, it will not be possible to notify the persons in regard to whom a special power has been exercised for the purposes of this investigation. For instance, a person operating on his own (sometimes called a "self igniter") and an international jihad network may both be investigated for the purposes of investigating islamic terrorism without there being any connection between the two. The link with such a wide field of investigation may have the result that there will be no notification as long as the other (sub)investigation is still ongoing. It is not to be expected, moreover, that any of the aforementioned phenomena will cease to be an area of responsibility for GISS. The ground for suspension may thus come to acquire a permanent nature, which the Committee considers to be not in accordance with the intention of the legislator, nor with the requirement of relevance laid down in Article 53(1)(a), at 3, of the

ISS Act 2002. The information in question must be relevant to an ongoing investigation. Such a broad definition of the term investigations does not do justice to the requirement of relevance. The Committee recommends that GISS link the definition to concrete investigations instead of phenomena in society. Ongoing investigation may be defined, for example, as a concrete investigation of a network or an organisation or in some cases even an individual person. This would do greater justice to the wording of Article 53 of the ISS Act 2002 and the intention of the legislator, which aimed at making a clear distinction between suspension and cancellation.

The Committee has established, however, as can also be read in section 3.4, that in practice GISS does in fact make this link with concrete investigations and decided to suspend notification on good grounds, with the exception of one case that is mentioned in that section.

GISS has pointed out the possibility of cross-connections. Cross-connections are more than superficial contacts between different networks, one of which is still being investigated by GISS.
If there are indications of relevant connections between certain networks while one of these networks is still being investigated by GISS, then it is the opinion of the Committee that this may be an impediment to notifying persons belonging to the network that is not or no longer being investigated, since notification must not result in harming the operational position of the service. The fact that these connections have not yet been recognized by GISS in all cases does not mean that the ground for suspension does not apply. However, in such cases GISS will have to state reasons why it holds that the data to be released by notification is relevant to an ongoing investigation. It is GISS that must make a plausible case that in the relevant area of responsibility there is a significant risk of non-recognized connections.
The Committee comments in this context that not every contact between two networks or organisations can without further reasons result in suspension of notification. There must be contact that is relevant in connection with the risk of interfering with any ongoing investigation. It is impossible to give general rules in this matter and all the circumstances of the case must be taken into consideration in assessing this issue.
The Committee endorses the principle applied by GISS that it must be determined on a case by case basis whether the information to be notified is relevant to any ongoing investigation.

The answer to the question whether there is an ongoing investigation does not depend on the exercise of special powers. Monitoring a specific investigation issue by investigating open sources can also mean that there is an ongoing investigation.

2.5 Cancellation of the obligation to notify

2.5.1 General observations regarding cancellation

Article 34(7) of the ISS Act 2002 provides for the possibility that the obligation to notify referred to in the first paragraph of this Article will lapse altogether if one of the grounds mentioned in paragraph 7 applies. Pursuant to paragraph 7 the obligation to notify lapses if submitting the report can reasonably be expected to result in sources of a service (including intelligence and security services of other countries) being disclosed, in relations with other countries and international organisations being seriously damaged or in a specific use of a method of a service or the identity of a person who assisted the relevant service in using the method, being disclosed. The foregoing is an elaboration of the jeopardise criterion laid down by the ECtHR that was discussed in section 1.3 above. GISS can only perform its statutory task with a certain measure of secrecy, which effectually means that GISS must be able to keep secret its sources, methods and current level of information.[38] Although the term used in the ISS Act 2002 is that the obligation to notify lapses, the term cancellation of notification is also used in this context.[39] Before considering the individual grounds for cancellation, the Committee will first discuss the cancellation rules generally.

The aforementioned obligation to examine whether notification is possible refers to the provision of the first paragraph of the Article under consideration. This obligation to examine pertains to the possibility that the ground for suspension embodied in Article 34(6) of the ISS Act 2002 is applicable. If a ground for cancellation applies, the service is not required to examine whether submitting a report is relevant to any ongoing investigation, and the obligation to examine will not revive annually.

Establishing that one of the grounds for cancellation applies is a final decision. The nature of the grounds for cancellation is generally such that they will continue to apply once they have been established to exist. Annual revision, as in the case of the ground for suspension, is therefore not logical. Because of the final nature of the grounds for cancellation GISS will, for reasons of efficiency, examine as early as at the time of exercising the special power whether a ground for cancellation applies; this procedure is supported by the legislative history of the ISS Act 2002.[40] At the instigation of the Committee this initial establishment of the applicable ground for cancellation when the special power is first being exercised has been converted into a provisional establishment, which is examined

[38] *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 86.
[39] *Parliamentary papers II* 2008/09, 30 977, no. 18, p. 4.
[40] *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 91 and *Parliamentary papers II* 2000/01, 25 877, no. 14, p. 55.

five years later to see whether the original reason is still valid.[41] In case of doubt this may lead to further investigation of the underlying file. Attention may be drawn in this context to e.g. the provisional invocation of the ground for cancellation "disclosure of a specific method of a service". The fact that GISS has a specific advanced technique at its disposal may be considered secret at the time when the power is exercised, but five years later the existence of this technique may be a generally known fact. Making this assessment five years later will prevent a ground for cancellation from being established under the influence of passing fads.

The obligation to examine only lapses if submitting a report can reasonably be expected to result in the occurrence of one of the situations mentioned under (a) to (c) of Article 34(7) of the ISS Act 2002. The criterion of reasonable expectation implies on the one hand that it is not required that one of the situations mentioned in the grounds for cancellation will occur. A reasonable expectation that it may occur is sufficient. On the other hand the requirement that the expectation must be reasonable implies in the opinion of the Committee that the expectation must be based on certain facts or empirical rules and must be capable of being objectified. The position that notification can be reasonably expected to result in one of the situations mentioned will therefore have to be based on sound reasons that can be tested by the Committee.

2.5.2 Source protection

It follows from Article 34(7)(a) of the ISS Act 2002 that the obligation to examine lapses if notification can be reasonably expected to result in disclosure of sources of the service, including those of intelligence and security services of other countries. Protecting the service's sources is one of the basic principles of the ISS Act 2002 and is embodied *inter alia* in the duty of care in regard to its sources that Article 15 of the Act imposes on the service.[42] It is vital to the effective functioning of the service and to the safety of sources that these sources are assured that their identity will remain secret. Moreover, foreign services will be considerably less willing to provide information to GISS if the origin of the information cannot be kept secret.[43]

Source protection as a ground for cancellation is interpreted very strictly by the service. A recent letter from the minister of the Interior and Kingdom Relations shows that the service must examine in each individual case whether it is certain that submitting a

[41] *Parliamentary papers II* 2008/09, 30 977, no. 18, p. 5.
[42] Inter alia: *Parliamentary papers II* 1997/98, 25 877, no. 3, p. 68; *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 42.
[43] *Parliamentary papers I* 1997/98, 25 442, no. 231b, p. 8.

notification report will not lead to disclosure of the identity of a source.[44] In case of doubt, it will be decided not to notify. The Committee points out that notifying only if it is certain that there will be no disclosure of any of the service's sources deviates from the criterion mentioned in the ISS Act 2002. Although the Committee recognizes the great importance of source protection, in practice it is virtually impossible to obtain certainty on this matter. The Committee holds that the resulting stringent restriction of notification is not in keeping with the original intention of the legislator. The criterion of reasonable expectation implies that more is required than the purely theoretical possibility of a source of the service being disclosed. In actual practice, so it will be shown in section 3.5.1 below, this has not led to situations in which the Committee and GISS arrived at different outcomes.

Moreover, source protection as a ground for cancellation should not be put forward too easily. It is the opinion of the Committee that this ground for cancellation pertains primarily to the protection of human sources and not to the deployment of a specific technical device (telephone tapping, for example) as a source of the service. The background to source protection lies in particular in the service's duty of care in regard to sources to ensure their safety, and furthermore in a need to prevent a decreasing willingness on the part of sources to provide information to the service.[45] Such aspects do not play a role in the use of technical sources. In the case of intelligence and security services of other countries, the ground for cancellation applies to sources of these foreign services as well as to information supplied by these services generally. A decreasing willingness to share information may cause the information position of GISS to deteriorate as far as its ability to gather information is concerned and will thus affect national security.

The Committee has established that GISS takes the position that the law does not require a causal connection between the information provided by a source and the power exercised. If at the same time a source of the service is present in the circle of the acquaintances of the person to be notified, the service will very rarely decide to notify regardless of whether the service's source influenced the decision to exercise the special power. Apart from rare exceptions, it is the opinion of the Committee that this is not in conformity with the intention of the legislator. The Committee recommends GISS to practice restraint in this respect. The criterion set by the ISS Act 2002 is the reasonable expectation that a source of the service will be disclosed. In the opinion of the Committee this implies that there must in principle be a plausible relation between the information supplied by the source and the exercise of the special power. The Committee has further found, as follows from section 3.5.1, that in actual cases GISS does in fact use the presence of a causal connection as a guideline.

---

[44] *Parliamentary papers II* 2008/09, 30 977, no. 18, p. 5.
[45] *Parliamentary papers II* 1997/98, 25 877, no. 3, p. 68.

2.5.3 Causing serious damage to relations with other countries and international organisations

The obligation to examine whether notification is possible lapses if notification can reasonably be expected to result in relations with other countries and international organisations being seriously damaged (Article 34(7)(b) of the ISS Act 2002). This ground for cancellation is based on the principle that notification of the person concerned should not result in deterioration of diplomatic relations of the Netherlands with other countries. This ground for cancellation is likewise given a broad interpretation by GISS and is not restricted to serious damage to diplomatic relations only. GISS takes the position that serious damage may be considered to exist if international contacts will proceed less smoothly or if notification results in decreasing willingness to provide certain information. In addition, the place where the special power is exercised may be relevant, for example if a special power is exercised on the territory of another country.

The Committee here points in particular to the criterion that there must be serious damage. It is the opinion of the Committee that this implies that not every form of contact with another country or an international organisation will have the effect of causing the ground for cancellation to apply. Although the criterion is that there must be serious damage, the Committee is aware that this may be readily assumed, since international relationships are delicate by nature; a good relationship comes on foot and goes on horseback. The Committee holds the opinion, however, that here, too, GISS must assess on a case by case basis whether the ground for cancellation applies and it has established that this is indeed the policy of GISS.

2.5.4 Disclosure of a specific use of a method of the service or of the identity of "assistants"

Article 34(7)(c) of the ISS Act 2002 provides that the obligation to examine whether notification is possible lapses if notification will lead to disclosure of the specific use of a method of the service or disclosure of the identity of a person who assisted the service in using the method. This ground concerns the use of methods that fit within one of the special powers described in the Act. It follows from the legislative history that the ground for cancellation is primarily included in order to prevent disclosure of GISS' level of technical knowledge.[46] The service may, for example, have used a specific way of entry and may have required the assistance of a third party to do so. If knowledge of the technical possibilities is made public, targets of the service may subsequently adapt their behaviour

[46] *Parliamentary papers II* 1999/2000, 25 877, no. 8, p. 93.

which may impair the effective performance by the service of its statutory tasks. Another example is the situation that the physical safety of the person who assisted GISS in using the method is endangered.

The Committee points out that the ground for cancellation applies only if it relates to a method of the service that is not generally known. The mere fact that the service has used a directional microphone, for example, cannot have the standard effect of cancellation. It follows from the law that GISS has this power and furthermore the notification letter will only describe the exercise of the special power in general terms. It is the opinion of the Committee that cancellation will only be in order if the specific characteristics of how the special power was exercised give cause for cancellation.

2.6 Making the obligation to notify part of the organisational structure

GISS has opted to centralize performance of the obligation to notify. This task has been entrusted to the legal department of GISS. Examinations whether notification is possible are assigned to a processor of this department. If necessary, the processor will obtain information about specific notification proposals from the directorate at whose instigation the special power was exercised. An applicant for permission to exercise a special power will state as early as in his proposal to exercise a special power whether there is reason to decide not to notify. What is said on the subject in the proposal constitutes a provisional indication of the subsequent final decision.

When performing the obligation to notify, GISS makes use of what is called Powers Chart (*Bevoegdhedenkaart*), an application specifically developed for the purpose. Powers Chart provides a largely automated system in which records are kept of all permissions to exercise special powers. In addition, entries are made in the system whether and when a special power has actually been exercised. Powers Chart is used to generate a clear overview showing when the exercise of a power subject to notification creates an obligation to examine whether notification is possible. Powers Chart automatically suspends the obligation to examine until the expiry of the five-year term applying to the exercise of the last special power in regard to the person concerned. On the expiry of this term the Power Chart system generates a report that an obligation to examine whether notification is possible has come into existence.

After this initial period of automatic suspension it must be assessed on a case by case basis whether there are indications calling for an extension of the suspension period by another year. The assessment can be processed in Powers Chart, which one year later creates a new

obligation to examine whether notification is possible. When the obligation to examine arises, moreover, the system generates a final proposal as to whether or not a ground for cancellation applies. The Power Chart system thus provides for reassessment of the validity of a ground for cancellation five years after the initial proposal on this issue.

One element of the examination whether notification is possible is that of tracing the person concerned. This tracing is done in collaboration with the GISS department responsible for searching open sources, which has direct access to the Online Municipal Personal Records. The processor provides the department concerned with as many identifiable data as possible from the file on the person concerned. If necessary, a further search in GISS' own systems may be done if checking the Online Municipal Personal Records has not yielded clear results. In addition, the processor assesses whether the processed data are relevant to any ongoing investigation and whether a ground for cancellation applies. Eventually, the examination whether notification is possible will result in a notification proposal, which may be that a notification letter will be sent, that notification will be suspended for one year, that the obligation to notify lapses because the person concerned cannot be traced or has died, or that the obligation to examine whether notification is possible lapses because a ground for cancellation applies. At the end of the chain the notification proposals are submitted to the (deputy) head of GISS for signature.

3 Findings of the Committee

3.1 Introductory remarks

The investigation of the Committee covered all notification decisions since the actual entry into force of the obligation to notify on 29 May 2007 until 11 November 2009. The Committee has established that in the review period GISS did not decide in any of the cases to actually submit a notification report. In 43 per cent of the cases the outcome of the examination whether notification was possible was that the person concerned could not be traced. In 25 per cent of the notification decisions the obligation to notify was suspended and in 27 per cent of the notification decisions it was concluded that a ground for cancellation applied. In the remaining cases the person concerned had died, a special power was exercised in regard to an organisation or it was eventually decided not to exercise the special power although permission to do so had been obtained.

3.2 The obligation to examine whether notification is possible

3.2.1 Reasonable term

The Committee has established that in a number of cases a considerable time elapsed between the moment when the obligation to notify came into existence and the moment of taking a decision whether or not the person concerned would be notified. Four times a year a series of notification proposals are presented to the (deputy) head of GISS. This means that the decision-making procedure has the effect that examinations whether notification is possible which are completed early in such a period are kept, at least until the next time a series of notification decisions will be signed. It is the opinion of the Committee that this period must be counted when assessing whether the statutory requirement of a reasonable term is satisfied. Although no persons have been notified so far, the Committee has established that the decision-making procedure would not have been different if there had been cases in which it would have been decided to submit a notification report.

The Committee can appreciate the policy of clustering notification proposals so that decisions on these proposals can be taken periodically and in batches. The Committee has established that the examinations whether notification is possible, which result in the preparation of a notification proposal, were carried out within a reasonable term.
In the opinion of the Committee, however, it is in principle contrary to the reasonable term requirement if there is a considerable interval between the preparation of a notification proposal and the subsequent notification decision. The Committee observes in this connection that it may happen that a notification proposal is further scrutinized in response to facts or circumstances that have subsequently emerged. In the absence of such facts or circumstances a notification proposal should in principle be dealt with in the following round of decisions. The Committee has established that this did not happen in all cases.
The Committee has established that notification decisions are generally taken within a reasonable term. In a few cases the Committee established that there was a long period between the examination whether notification was possible and the subsequent notification proposal on the one hand and the final notification decision on the other hand. The Committee recommends that GISS exercise due care to ensure that the last phase is completed as soon as possible.

3.2.2 Exercise of a special power in regard to an organisation

The Committee has established that in a number of cases GISS exercised a special power with the objective of gathering information on an organisation. It follows from the ISS Act 2002 that exercising a special power in regard to an organisation is not subject to the obligation to notify. The Committee has established that in the cases in question GISS decided with due care and on rightful grounds that the special power was exercised in regard to an organisation and not in regard to a natural person.

3.3 Lapse of the obligation to notify

The Committee has established that in tracing the person concerned GISS usually confines its efforts to searching its own information systems and the municipal personal records database, in the sense that GISS searches its own information systems to collect identity data in order to be able to do a successful search in the municipal personal records database. GISS' own information systems are consulted to find out which potential identification data are known at GISS. These are e.g. date of birth, address, name and, if applicable, aliases. The results of this search are provided to the department at GISS that is charged, among other things, with doing checks in the municipal personal records database. If the search in this database leads to uncertainties, the department gets back to the processor and asks for additional information. This leads to another check in GISS' own information systems in order to get hold of the missing data.

The Committee has established that in a number of cases the search in the municipal personal records database produced the town of residence but no address details. Enquiry at GISS showed that this may mean that the person concerned has gone abroad. The last municipality of registration is required to maintain the person's registration in this municipality so that his personal data remain clearly known should he return to the Netherlands. Another possibility is that a municipal inspection showed that the person in question did not actually reside at the address stated by him. If this is the case, the address will be removed from the registration entry. The person concerned will, however, continue to be registered in the municipality as his place of residence for the purpose of keeping the personal data.

In a single case the result of a tap showed that the tapped number did not belong to the person in regard to whom the telephone tap had been executed, but, so it emerged later, to an unrelated third party. The Committee holds the opinion that in this case it should have been examined whether notification of this person was possible. The Committee has established that GISS purposefully infringed the privacy of the person concerned, since

GISS purposefully continued tapping his telephone for some time to investigate whether the person concerned belonged to the network of the true target. In the opinion of the Committee this means that this person was not a third party as defined in section 2.2.4 of this review report. This is not changed by the fact that subsequently it emerged that this person was not related to the target.
The Committee has established that GISS did try to trace the true target. GISS did a check using the name of the true target in combination with the unrelated third party. The Committee holds, however, that this check clearly could not have led to the true target being traced, since the search terms used by GISS were based on an address where the true target did not live, as GISS itself had proved.

The Committee has found that in one case GISS was unable to trace a person who should have been known to be in a penal institution at the time. The Committee has established that the data of the place of abode of the person concerned were present in GISS' own information system, but that GISS did not use these data when tracing the person. This issue is discussed in greater detail in the secret appendix to the present review report. The Committee recommends that the relevant notification decision be reconsidered taking the foregoing into account.

The Committee has established that GISS, when tracing persons concerned, acted in accordance with the statutory requirements, except for the case mentioned above concerning a person who was in a penal institution. The Committee recommends that the notification decision in that case be reconsidered. This does not mean to say, however, that such reconsideration would lead to notification, since there may be other grounds for deciding not to notify.

The Committee calls to mind the recommendation stated in section 2.3.2 to include other sources than the municipal personal records database in the process of tracing a person concerned. The Committee does not have any indication, though, that in the cases it investigated GISS would have been able to trace the persons concerned if it had done such a wider search, but it cannot exclude it either.

3.4 Suspension of the obligation to notify

Suspending notification is prescribed if the special power was exercised in regard to the person concerned less than five years ago or if data relating to this person was processed in this period for the purposes of the investigation in question. The data must also not be relevant to any ongoing investigation. The Committee has established that in the large majority of notification cases where a ground for suspension applied, the suspension was

based on the fact that new data relating to the person concerned had been processed in the past five years. This may mean, for example, that the person concerned was observed in a surveillance action, that the person concerned was mentioned in a report from a human source or that tapping reports show that the person concerned was still maintaining contacts with persons recently investigated by GISS. In one single case it was decided to suspend notification on the grounds that the data in question was relevant to an ongoing investigation without the person concerned being part of this investigation. The Committee has established that GISS generally proceeds with due care when determining whether a ground for suspension applies. It is the opinion of the Committee that the conclusion that notification must be suspended is always supported by the underlying documents. The Committee has established that GISS links its decisions as much as possible to individual investigations. It is the opinion of the Committee that this approach does justice to the casuistic approach that should be typical of such assessments. Nonetheless, the Committee wishes to discuss one case in which the decision to suspend notification was, in its opinion, not taken on valid grounds.

The Committee has established that in one specific examination whether notification was possible it was established that GISS had decided more than five years ago that it would no longer investigate a certain group, to which the person concerned belonged. For the purposes of that investigation special powers had been exercised at the time in regard to the person concerned. Less than five years ago, in response to a request for information about the matter from a counterpart service, GISS confirmed that it had ceased investigating the group in question. It is the opinion of the Committee that in this case GISS' invocation of a ground for suspension within the meaning of Article 53(10(a) of the ISS Act 2002 was not made on valid grounds. In the opinion of the Committee, confirmation of a prior decision no longer to investigate a certain group cannot be considered a new fact within the meaning of Article 53(1)(a), at 2, of the ISS Act 2002. Moreover, in the margin of the examination report belonging to the relevant notification decision GISS had noted that it must always be possible to take up a case again ad hoc if there was reason to do so. However this may be, the Committee holds the opinion that such a marginal note does not constitute sufficient grounds for deeming an investigation to be an ongoing investigation. The Committee recommends that GISS reconsider the notification decision in question.

The Committee has established that in a number of cases some time elapsed between the initial processing of the results of a special power and the further utilisation of the results in subsequent intelligence products. In connection with the moment the term of suspension begins to run it is relevant to examine under which circumstances it can be said that new data are being processed. The Committee holds the opinion that processing of new data can be said to occur if data that has already been processed is examined in a

different context, for example because of the availability of subsequent information. For example, the results of the exercise of a special power can be put in a different light when they are compared with intelligence that has subsequently become available. If this is the case, the five-year period should begin to run at a later date. If, however, the initial examination results are subsequently merely cited and do not or cannot lead to new knowledge, the date of the initial processing should mark the commencement of the five-year period. The Committee has not come across any cases in which it was wrongly decided to suspend the obligation to notify on the grounds of intelligence already available at the time but not used until a later date.

The Committee has established that GISS holds the opinion that suspension of notification is prescribed if the person concerned had contacts in the past five years or still is in contact with a person who is still being investigated. The Committee has established that GISS could reasonably hold that the contacts in these cases were relevant and more than merely superficial contacts.

In a number of examinations whether notification was possible GISS established that the person concerned formed part of a relatively small network. In such cases GISS stated that it would not notify until there was no longer any ground for suspension applicable to any of the persons in the network. If certain persons from the network should be notified and others not, this could lead to the conclusion that certain persons had recently been, or were still being investigated by GISS. This could lead to disclosure of the current level of knowledge of GISS. The Committee appreciates the position taken by GISS.

The Committee has established that most examinations whether notification was possible involved the exercise of a special power based on the a-task of GISS. A number of cases, however, concerned a special power based on the d-task. In such notification examinations GISS decided that notification must be suspended if the special powers were exercised for the purposes of an investigation in a country which under the current Designation Order was designated as a special-attention country. The Committee considers this to be in accordance with the law.

The Committee has established that GISS, when assessing whether a ground for suspension applied, acted in accordance with the statutory requirements, with the exception of one single case that was discussed above. The Committee recommends that GISS reconsider this case. This does not mean to say, though, that reconsideration would result in notification, because there may be other grounds for deciding not to notify.

3.5 Cancellation of the obligation to notify

3.5.1 Source protection

If notifying the person concerned can reasonably be expected to result in sources of GISS, including those of intelligence and security services of other countries, being disclosed, the obligation to notify is cancelled on the ground of source protection. In section 2.4.2 the Committee has taken the position that a technical source, such as a telephone tap, is not a source within the meaning of Article 34(7)(a) of the ISS Act 2002. The Committee has established that GISS took this position in a recent examination report accompanying a notification decision. The Committee has established, however, that with respect to a notification decision of an earlier date GISS decided to cancel notification on the ground of source protection because the telephone number had been obtained by telephone tapping. The Committee holds that this is not in keeping with the intention of the ISS Act 2002. The Committee recommends that GISS reassess the decision in question taking account of the Committee's opinion.

The Committee has established that GISS considers this ground for cancellation applicable if the exercise of a special power can be traced back to information about the person concerned that was obtained from a source of GISS. However, the mere fact that information was obtained from a source does not suffice to make the ground for cancellation applicable. For this to happen it is required that notification can be reasonably expected to lead to the identity of the source being disclosed. The Committee has established that GISS interpreted this requirement by expressing in the notification report that the person concerned had communicated the information to the source of GISS confidentially.

The Committee has established that in some cases an official report on the person concerned was sent to the National Public Prosecutor for Counterterrorism. The Committee has established that one of these official reports contained the telephone number of the person concerned. By acting thus GISS disclosed its knowledge of this telephone number, since the official report might subsequently be added to the case file and be seen by the person concerned. It is the opinion of the Committee that in this situation GISS may no longer decide to cancel the obligation to notify on the mere grounds that the telephone number in question had been communicated to a source of GISS confidentially. This would be different only if notification of the person concerned would provide the person concerned with additional data which would help to disclose the source of GISS. The Committee has in mind the situation that the date on which telephone tapping started makes it clear to the person concerned that there is a connection with his giving the telephone number to the source of GISS.

In a number of cases the underlying file shows that several telephones were tapped in regard to the person concerned. The Committee has established that in cases where one of the telephone numbers had been provided confidentially to a source, GISS also invoked source protection as a ground for cancellation with respect to the other telephone numbers that had been tapped. The reason GISS stated for this was that the notification letter, if sent, would not show which telephone number was tapped and the person concerned might therefore assume that his unlisted number had been tapped.[47] GISS stated that experience had shown that in such a case the person concerned will seek the person who leaked the information in his immediate surroundings. The Committee subscribes to this position of GISS but holds at the same time that source protection requires the actual exercise of a special power with respect to an unlisted telephone number. In other words, the Committee holds that the source in the surroundings of the person concerned must actually have supplied information about the person concerned on the basis of which a special power was exercised. The mere fact that a source is active in the surroundings of the person concerned does not by itself have the effect that the ground for cancellation of source protection applies.

In one specific case GISS decided to cancel notification on the grounds of source protection because a telephone number had both been obtained from a human source and become known to GISS by the use of a technical means. Since the person concerned was not aware of the use of the technical means, and could only guess at this, the Committee agrees to the position taken by GISS that the ground for cancellation of source protection applied in this case.

The Committee has established that in a number of cases GISS communicated with foreign counterpart services about the person concerned. In this context the Committee distinguishes between two situations.
On the one hand the Committee recognizes the situation where there is a direct connection between information obtained from the counterpart service and the exercise of the special power. The Committee has established that in a number of cases the provision of information by the counterpart service led directly to the exercise of special powers in regard to a specific person. It is possible that the information resulted in an investigation of a person who previously was unknown to GISS. It is also possible, however, that the information obtained resulted in the exercise of a specific special power in regard to a person who was already known to GISS. This is the case, for example, where GISS obtained a telephone number of the person concerned that so far had remained

[47] Article 34(3), first sentence and at (b), of the ISS Act 2002 says on this subject: "The report will be in writing and contain exclusively: […] an indication of the special power as referred to in the first paragraph that has been exercised with regard to the person in question."

unknown to GISS from a counterpart service, which resulted in a telephone tap on this telephone number. The Committee has established that in a number of cases the counterpart service, when providing the information, stated at the same time that the information came from a sensitive (human) source.
On the other hand the Committee recognizes the situation where there have been general communications between GISS and a counterpart service about a person qualifying for notification, for example in the context of an investigation of a specific organisation to which the person in question belongs. But the information from the counterpart service did not result in a more intensive personal investigation of the person concerned. The communications may, for example, have consisted of an exchange of general information about the organisation in question.
The Committee has established that it was only in the former situation that GISS cancelled notification on the ground of Article 34(7)(a) of the ISS Act 2002, which the Committee considers to be in agreement with the objective of the Act.

The Committee has established that GISS acted in accordance with the statutory requirements when determining whether the ground for cancellation of source protection applied, with the exception of two cases that were discussed above. In one case a technical source was wrongly deemed to be a source within the meaning of Article 34(7)(a) and in the other case the telephone number that had been provided confidentially had already been disclosed in an official report. The Committee recommends that GISS reconsider these notification decisions. This does not mean to say, however that reconsideration would lead to notification, since there may be other grounds for not notifying.

3.5.2 Serious damage to relations with other countries and international organisations

The Committee has established that in a number of cases GISS decided to cancel notification because notifying the person concerned could be reasonably expected to have the effect of seriously damaging relations with other countries and with international organisations (Article 34(7)(b) of the ISS Act 2002).

The Committee has established that the exercise of the power to select data obtained by using the technical device of receiving and recording non-specific non-cable-bound telecommunications pursuant to Article 27(3)(a) and (b) of the ISS Act 2002 ("Sigint") results without exception in cancellation on the grounds of serious damage to relations with other countries and international organisations. The Committee has established that as a rule the exercise of Sigint goes hand in hand with tapping non-cable-bound telecommunications coming from another country. This violates the sovereignty of the

country involved and disclosure of the fact that GISS has exercised this power may cause serious damage to relations with other countries.

The Committee has established that GISS, for the purposes of its a-task, among other things investigates espionage activities of foreign powers. Such investigations may entail the exercise of special powers that are subject to the obligation to notify. The Committee has established that in such cases GISS holds the opinion that the ground for cancellation under consideration here applies. In view of the extremely sensitive nature of such investigations and the far-reaching consequences they may have for relations with other countries, the Committee holds that in these cases the invocation of this ground for cancellation is in agreement with the ISS Act 2002. The Committee has established that GISS is increasingly open about intelligence activities of other countries in the Netherlands, as emerges *inter alia* from recent annual reports of GISS. However, GISS' statements on the subject cannot be traced to individual cases and neither do these reports state expressly that in actual cases the investigations into such activities were carried out by exercising special powers.

The files on a number of notification decisions show that an investigation of the person concerned was started on the basis of information obtained from counterpart services. In these cases the ground for cancellation under discussion here was considered applicable, whether or not in combination with other grounds. Like GISS, the Committee holds that notification might lead to serious damage to relations with other countries or international organisations. The Committee refers to the criteria for applicability of the ground for cancellation of source protection that were set out in the preceding section. In the opinion of the Committee the decisive factor for the applicability of the ground for cancellation under consideration here is the fact that notification of the person concerned can be reasonably expected to be traceable to the information provided by the counterpart service.

The Committee has established that GISS acted in accordance with the statutory requirements when determining whether the ground for cancellation of serious damage to relations with other countries or international organisations applied.

3.5.3 Disclosing a specific use of a method of the service or the identity of "assistants"

The Committee has established that in some cases GISS decided to cancel notification on the cancellation ground that notification would disclose a specific use of a method of GISS or the identity of the person who assisted GISS in using the method (Article 34(7)(c) of

the ISS Act 2002). The Committee has found that these decisions were taken in accordance with the Act.

The Committee is aware that the decision that this cancellation ground applies is a final decision. It points out, however, that in the opinion of the Committee this cancellation ground does not have the same permanent nature as the other two cancellation grounds. The Committee calls to mind that in principle a specific use of a method of GISS concerns the specific technical possibilities at the disposal of GISS.[48] The Committee has established that the current state of the (technical) art plays an important role in this context. In one case, for example, the Committee found that five year after a – previously unknown - technical capacity of GISS was used, it had become generally known. It is the opinion of the Committee that GISS, when reassessing the cancellation ground, rightly decided that the cancellation ground did not apply, in spite of the fact that it had been put forward at the time on good grounds.

The Committee has established that GISS acted in conformity with the statutory requirements when determining whether the cancellation ground that notification would disclose a specific use of a method of GISS applied.

4 Concluding observations

The Committee has established that apart from a few exceptions, GISS performed the obligation to notify in accordance with the statutory requirements. Possibly, some of the observations made in the foregoing will lead to a notification letter being sent to the person concerned after all. In the majority of the investigated notification decisions GISS decided on good grounds that the obligation to notify would be suspended or cancelled. The Committee thinks it probable, moreover, that the decisions that will be reconsidered will subsequently lead to a decision not to notify on other grounds. The Committee takes the position that this justifies the conclusion that so far the obligation to notify has not made an actual contribution to the possibilities for individuals to challenge an allegedly unlawful exercise of special powers by GISS. There is, however, no simple answer to the question whether this will be different in the (near) future.

The obligation to notify shows strong similarity to the rules on applications for inspection of files. The grounds for cancellation and suspension are even largely identical. The Committee has established that actual practice with regard to applications for inspection of files shows that data are released to a fairly large extent, while so far not one single

[48] See section 2.5.4 above for a more detailed interpretation of the term "specific use of a method".

notification letter has been sent. The main reason for this is the fact that applications for inspection of files may relate to any and all data in the possession of GISS. On the one hand this means that an application may relate to data from a more distant period. For example: a substantial part of applications for inspection of files relates to data collected during the Cold War. On the other hand applications for inspection of files are not limited to data in the possession of GISS that were obtained by the exercise of a select number of powers. In practice, moreover, applications for inspection of files do not involve problems with tracing the person concerned, since this person himself or herself states where he lives. The notification procedure is frustrated by the failure to trace the person concerned in nearly half of the cases.

It is the opinion of the Committee that it cannot be said that the grounds for cancellation as such are formulated too broadly. The grounds for cancellation do justice to the lawful interests to be protected by GISS. It is a fact that the nature of the special powers that are subject to the obligation to notify is such, that they often go hand in hand with the applicability of a ground for cancellation. Examples are the exercise of Sigint and the virtually inevitable connection with the ground for cancellation of serious damage to relations with other countries.

It is true that on the subject of traceability there is some difference of opinion between the Committee and GISS about the interpretation to be given to the term reasonable effort. The Committee has established, however, that it will not be possible to trace a substantial part of persons concerned without making far-reaching, disproportional tracing efforts. This is partly due to the mere lapse of time between the termination of the investigation of a person concerned and the start of the examination whether notification is possible.

The Committee has established that only a small number of the operational investigations started since 2002 are deemed or can be deemed to have been completed. As a rule, investigations of GISS are long-term affairs. This is true, for example, for investigations of terrorist or jihadist networks. These networks are typically rather fluid. GISS will for a long time keep a finger on the pulse in regard to persons investigated at some point in the course of such investigations. In addition, the exercise of special powers is not the final piece of an investigation but usually rather the reason for undertaking further investigative activities. This does not change the fact that investigations must come to an end and that this will eventually cause the grounds for suspension which are currently applicable to lapse. This means that in the long term more notifications will be effected. It is not inconceivable that with the lapse of time the value of notification will decline for the person concerned.

The Committee has established that the performance of the obligation to notify takes up a considerable part of GISS' capacity and that this will only increase in the future. The Committee also has established that even though GISS generally performs the obligation to notify in a lawful manner, no notification letters have been sent so far. It is the opinion of the Committee that it is not possible to explicitly infer an active obligation to notify from the ECHR and the relevant case law of the ECtHR on the subject, and that the weight of such an obligation must be balanced against the complex of other existing legal safeguards. In this context the Committee draws attention to the means of redress already available to individuals, such as filing a complaint in reaction to allegedly improper conduct by GISS and the possibility of filing an application for inspection of the personal data that have been processed by GISS. In this context the Committee comments that such applications must be dealt with on the basis of the same principles that underlie the obligation to notify. The point, therefore, is the added value of the obligation to notify for the Dutch system of legal protection. In this connection one may also raise the question whether the costs of performing the obligation to notify are justified by the benefits. This involves a balancing of interests, however, which is not the responsibility of the Committee but of the legislator.

5 Conclusions and recommendations

5.1 The Committee has established that apart from a few exceptions, GISS performed the obligation to notify in accordance with the statutory requirements (section 4).

5.2 The Committee has established that GISS, when tracing a person concerned, usually confines its efforts to searching its own information systems and the municipal personal records database, in the sense that GISS' search of its own information systems serves to collect identity data in order to enable GISS to do a successful search in the municipal personal records database. It is the opinion of the Committee that GISS' own information systems can also play an independent role and should not be used only as a supplement to the municipal personal records database. It is the opinion of the Committee that GISS may be expected to enquire from the local Regional Intelligence Service (*RID*)) or another relevant body within the meaning of section 60 of the ISS Act 2002 whether they happen to have information of their own about the actual abode of a person concerned if the file available to GISS contains indications that such an enquiry may lead to some result. The Committee recommends that GISS adjust its tracing policy on this point. It has no indication that in the cases it investigated the persons concerned could have been traced if GISS had made this further search, but cannot exclude it either (section 2.3.2).

5.3 The Committee has established that GISS gives a broad interpretation to the notion of 'ongoing investigation', linking it to the threat emanating from certain phenomena in society. The link with such a wide field of investigation may have the result that there will be no notification of one person as long as there is still a related, if only remotely, ongoing (sub)investigation. It is not to be expected, moreover, that any of the aforementioned phenomena will cease to be an area of responsibility for GISS. The ground for suspension may thus come to acquire a permanent nature, which the Committee considers not to be in accordance with the intention of the legislator, nor with the relevance requirement of Article 53(1)(a), at 3, of the ISS Act 2002. The Committee recommends that GISS link the definition as much as possible to concrete investigations instead of phenomena in society. The Committee has established, however, that in practice GISS does indeed make this link with concrete investigations and decided to suspend notification on good grounds, with the exception of one case mentioned in conclusion 5.5 (section 2.4.3).

5.4 The Committee has established that GISS, when tracing persons concerned, acted in accordance with the statutory requirements, with the exception of one single case. The Committee recommends that the notification decision in that case be reconsidered. This does not mean to say, however, that such reconsideration would lead to notification, since there may be other grounds for deciding not to notify (section 3.3).

5.5 The Committee has established that GISS, when assessing whether a ground for suspension applied, acted in accordance with the statutory requirements, with the exception of one single case. The Committee recommends that GISS reconsider the notification decision taken in this case. This does not mean to say, though, that such a reconsideration would lead to notification, because there may be other grounds for deciding not to notify (section 3.4).

5.6 The Committee has established that with the exception of two cases GISS acted in accordance with the statutory requirements when determining whether the ground for cancellation of source protection applied. In one of these two cases a technical source was wrongly deemed to be a source within the meaning of Article 34(7)(a) and in the other the telephone number that had been provided confidentially had already been disclosed in an official report. The Committee recommends that GISS reconsider these notification decisions. This does not mean to say, however, that such reconsideration would lead to notification, since there may be other grounds for deciding not to notify (section 3.5.1).

5.7 The Committee has established that GISS acted in accordance with the statutory requirements when determining whether the ground for cancellation of serious damage to relations with other countries or international organisations applied (section 3.5.2).

5.8 The Committee has established that GISS acted in conformity with the statutory requirements when determining whether the cancellation ground that notification would disclose a specific use of a method of GISS applied (section 3.5.3).

Adopted at the meeting of the Committee of 24 February 2010.

Review Committee on the Intelligence and Security Services

Anna van Saksenlaan 50

2593 HT The Hague

Internet: www.ctivd.nl

E-mail: info@ctivd.nl