

**COMMISSIE VAN TOEZICHT
BETREFFENDE
DE INLICHTINGEN- EN VEILIGHEIDSDIENSTEN**

REVIEW REPORT

on

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

CTIVD no. 31

11 April 2012

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 31

REVIEW REPORT

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

Table of Contents

Summary.....	i
1. Introduction.....	1
2. The Committee's investigation.....	1
3. General picture	4
3.1 Article 25 ISS Act 2002	4
3.2 Article 27 ISS Act 2002	4
4. Substantiation of the reasons for applying article 25 ISS Act 2002	6
5. Investigation of radicalisation trends.....	7
6. The power to tap or intercept and third parties.....	9
7. Consultation with DISS	10
8. Conclusions and recommendations.....	10

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 31

SUMMARY

Of the review report on the use by GISS of the power
to tap/intercept and the power to select Sigint

Summary

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

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

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

The Committee has established that when GISS investigates radicalisation trends, it is not always clear that the persons or organisations with respect to which the power to tap or intercept is used actually give cause for serious suspicion that they pose a threat to national security. The Committee recognizes the importance of investigating such trends, but emphasizes that in doing so GISS must continuously evaluate the use of special powers with respect to these persons or organisations. In one case the Committee established that GISS used special powers for several years without obtaining clarity about the threat emanating from the persons involved. It is the opinion of the Committee that particularly in the final period of this investigation the use of the power to tap or intercept approached the borderline of what is permitted by law. In one case GISS used special powers with respect to a person who wished to publish a certain message of which, so GISS believed, it could not be excluded that it might be taken as an incitement to activism or violence. The Committee considers this wording too broad, since the use of a special power must be based on a serious suspicion of threat.

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

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

REVIEW COMMITTEE
FOR THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 31

REVIEW REPORT

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

1. Introduction

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

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

This report has a secret appendix.

2. The Committee's investigation

In February 2009, the Committee reported to the Second Chamber of Parliament for the first time on its investigation of the application by GISS of articles 25 and 27 ISS Act 2002 (review report 19).¹ After the publication of this report the Committee continued monitoring the exercise of these powers on a quarterly basis. Monitoring serves as a means to keep a finger on the pulse and in principle does not result in a report to the Second Chamber. In September 2010 the Committee decided to convert the monitoring into an annual in-depth investigation. The reason for this decision was that by announcing an investigation and reporting on its findings the Committee would be able to give the Second Chamber a better understanding of the Committee's activities and findings regarding this important part of the work of GISS. The Committee will report on this subject on an annual basis. The present

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

report is based on the investigation of the lawfulness of the application by GISS of articles 25 and 27 ISS Act 2002 in the period from September 2010 until the end of August 2011.

Every quarter, applications for permission to apply articles 25 and 27 are bundled and submitted to the minister of the Interior and Kingdom Relations.² Urgent new operations requiring a speedy start are submitted to the minister on an ad-hoc basis. The Committee carried out its investigation on a three-monthly basis shortly after the requested permission had been granted by the minister. It did so by examining the bundle of applications submitted to the minister³, as well as the urgent ad hoc applications submitted separately. In the bundle of applications every operation is mentioned, including the name and the communications data of the person or organisation with respect to whom or which the special power is to be used and it gives a brief explanation of the reason for the request to use the power (article 25(4) and article 27(4) ISS Act 2002). The quarterly examination of the bundle of applications enabled the Committee to obtain an overview of all means used pursuant to articles 25 and 27, ISS Act 2002, in the review period. These bundles of applications do not, however, give exhaustive reasons substantiating the necessity, proportionality and subsidiarity of using the special power in question.

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

In view of the great number of operations it was impossible for the Committee to examine all these documents. When examining the applications the Committee gave special attention to operations that stood out, either because of anomalies or a lack of clarity in the explanation, or because the operation focused on special categories of persons (non-targets⁴, third parties, professionals entitled to privilege, minors etc.). In the case of these operations the Committee examined the underlying documents, including the application for permission with the comprehensive substantiation of reasons and the detailed records of the intercepted conversations. These documents are stored in the internal digital system of GISS, to which the Committee has unrestricted access.

In addition, the Committee devoted attention to operations classified top secret or otherwise accessible to a smaller circle of persons than usual. These operations are not stored in the internal digital system of GISS and constitute highly sensitive material. To make its investigation as comprehensive as possible the Committee requested GISS to provide the documents concerning these operations separately. In the course of the review period the Committee established that the proportional number of operations classified top secret or otherwise subject to restricted access was much higher than the number received from GISS.

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

³ These bundled applications for permission are also known as “three-monthly collective decisions”

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

Upon the Committee's request GISS subsequently provided the documents on the operations identified by the Committee after all. The explanation given by GISS for the initially incomplete information provision was that with a view to the *need to know* principle the service did not keep a central list of operations that were classified top secret.⁵ Indeed, GISS could not guarantee that it had now delivered all operations in the review period that were classified top secret or otherwise made accessible to a smaller circle of persons than usual to the Committee. The argument given by GISS does not justify the absence of a list of these operations in which special powers had been used. It is the opinion of the Committee that keeping proper records is not at odds with the *need to know* principle. In addition, the absence of proper records had the result that GISS failed to fully inform the Committee. At the Committee's request the GISS unit responsible for supervising operations was then charged with the task of henceforth maintaining the list in question. Since then, the Committee has not established any further cases of incomplete information.

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

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

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

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

this would in fact have been advisable. Section 8 contains the conclusions and recommendations of the Committee.

3. General picture

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

3.1 Article 25 ISS Act 2002

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

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

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

3.2 Article 27 ISS Act 2002

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

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

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

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

In the next in-depth investigation of the use by GISS of the powers to tap/intercept and to select Sigint the Committee will examine to what extent the substantiation of the reasons for selection of Sigint has improved. The Committee takes the position that with the legal framework and the starting points provided by the Committee, in particular in review reports 19 and 28, GISS should be able to adequately substantiate the reasons for using this power. The Committee understands that an amendment of the ISS Act 2002 is being prepared which will among other things include an adjustment of the provisions on the use

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

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

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

¹⁰ CTIVD review report no. 26 on the lawfulness of the performance by GISS of the foreign intelligence task, *Parliamentary Papers II* 2010/11, 29 924, no. 68 (appendix), §5.4, available at www.ctivd.nl.

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

of Sigint. The Committee is awaiting the proposed amendment with interest. However, these developments do not change the fact that GISS must satisfy the requirements set by the current ISS Act 2002 for the selection of Sigint.

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

When a team of GISS wishes to use a tap or microphone pursuant to article 25 ISS Act 2002, it prepares a detailed substantiation of the reasons for such use. In this substantiation it demonstrates the necessity, proportionality and subsidiarity justifying the use of this special power, as required by articles 18, 31 and 32, ISS Act 2002.¹² The (legal) tenability of these reasons is assessed within GISS by, successively, the team leader, a legal expert of the unit responsible for supervising operations, the head of the operational unit concerned and the head of GISS.

The number of taps and microphones for which the minister must grant permission is great. The minister of the Interior and Kingdom Relations has no departmental support staff for assessing the use and the applicable legal assessment framework. The bundle of applications which the minister receives every three months includes a summary of the more detailed internal substantiation of reasons. This summary deals only briefly with the necessity, proportionality and subsidiarity of using the special powers. This underlines the importance of the internal assessment procedure at GISS since in this procedure the relevant factors are indeed explained and explicitly assessed against the legal review framework. As stated above in section 3.1, the internal substantiation of reasons shows that GISS takes well-considered decisions with regard to using the power to tap or intercept. This thorough internal recording of the reasons stated for the application of article 25 ISS Act 2002 is essential for the Committee's review work.

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

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

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

5. Investigation of radicalisation trends

GISS may only use special powers for the purposes of performing the security task and the foreign intelligence task (article 6(2)(a) and (d) in conjunction with article 18, ISS Act 2002). For the purposes of the security task GISS may conduct an investigation if persons or organisations, because of the objectives they pursue or through their activities, give cause for serious suspicion that they pose a threat, briefly stated, to national security (article 6(2)(a) ISS Act 2002).¹³ These persons are also known as *targets*. An important part of the investigations conducted by GISS on the basis of the security task consists of investigating radicalisation trends. In this type of investigation the threat emanating from persons and organisations is often not yet clear or concrete. GISS is not only expected, however, to identify concrete terrorist threats but also to keep track of radicalisation trends. The wide approach to terrorism that has been chosen is also directed at forms of radicalisation which, though not

¹³ The foreign intelligence task is formulated more broadly. GISS may investigate persons and organisations if it is necessary to do so for the purposes of investigations concerning other countries pursuant to the Designation Order of the prime minister. No serious suspicion of a threat to national security is required, a national security interest suffices. In reports 19 and 26 the Committee established, based on judgments of the ECtHR, that additional requirements apply to the use of special powers. For the privacy infringement to be justified, a *potential harm to national security* must be established. See CTIVD review report no. 19 on the application by GISS of article 25 ISS ACT 2002 (taps) and article 27 ISS ACT 2002 (selection of non-directional interceptions of non cable-bound telecommunications), *Parliamentary Papers II* 2008/09, 29 924, no. 29 (appendix), §3.3 and CTIVD review report no. 26 on the lawfulness of the performance by GISS of the foreign intelligence task, *Parliamentary Papers II* 2010/11, 29 924, no. 68 (appendix), §3.5.1. The reports are also available at www.ctivd.nl.

leading directly to terrorist violence, may nevertheless have a disrupting effect on society.¹⁴ The Committee recognizes the importance of the radicalisation investigations of GISS. The Committee considers it its task to critically assess, when GISS has used special powers for the purposes of investigating radicalisation issues, whether the statutory criterion of serious suspicion of threat to national security is satisfied. When investigating the radicalisation investigations of GISS in the review period the Committee came across a number of operations where it was not immediately evident that the person against whom or the organisation against which the special powers were used did in fact give cause for such serious suspicion. This was reason for the Committee to examine these operations more closely.

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

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

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

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

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

6. The power to tap or intercept and third parties

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

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

In the first scenario the application for permission is made in the name of the target since he is the person (or one of the persons) using the location or connection. In its review report no. 19 the Committee said that the substantiation of the reasons for using the power must expressly devote attention to the fact that the means of communication belongs to a third party. GISS must also exercise restraint in working out information relating to the acts of this third party.¹⁶ In addition, when applying for renewal of permission with a view to the results obtained by the use of the power GISS must assess whether the interest of keeping the target under surveillance still outweighs the infringement of the third party's privacy rights. Information about a third party collected by using the power can be considered bycatch which may only be worked out with great restraint. The Committee established that in a number of cases in the review period in which GISS applied article 25 ISS Act 2002 to a place or connection belonging to a third party, it failed to properly include the third party's interests in its substantiation of the reasons for applying the article. The Committee considers this a lack of due care. Especially so if several operations under article 25 ISS Act 2002 are ongoing with respect to one single target, including a tap or microphone at a location or connection belonging to a third party. In such cases GISS provides one set of reasons for all these taps combined, without devoting specific attention to the interest of the third party. GISS must, however, explain for each individual tap why it meets the requirements of necessity, proportionality and subsidiarity. This applies specifically where a tap or microphone is used at a place or in respect of a connection belonging to a third party. It is the

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

opinion of the Committee that in the cases in which it established that the substantiation of reasons was inadequate, adequate substantiation of reasons would in fact have been possible. The shortcomings were therefore *procedural* without involving any unlawful application of article 25 ISS Act 2002 of a *substantive* nature.

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

7. Consultation with DISS

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

One factor playing a role in this operation was the existence of weighty reasons to consult with DISS before using the tap. It was an operational situation in which GISS should have seriously considered the fact that DISS, too, had information that was relevant for the investigation. The Committee asked GISS why it did not contact DISS in order to obtain the information. GISS replied that there were two operational reasons for not approaching DISS. First, the investigation was in an early stage and there were still many operational uncertainties. GISS thought that it was not proper to contact DISS until it had become clear that there was a threat to interests to be protected by DISS. Secondly, GISS feared that prior consultation with DISS would entail a risk of failure for its own operational plans.

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

8. Conclusions and recommendations

- 8.1 The Committee has established, as it did in the preceding review report on the subject, that GISS takes well-considered decisions when applying article 25 ISS Act 2002. The Committee has not found any unlawful procedures in the operations it

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

investigated. This deserves a compliment given the large number of operations. (section 3.1)

- 8.2 On some points, however, the Committee has established a lack of due care, in particular in the matter of substantiating the reasons for operations. The Committee holds the opinion that in the cases of faulty substantiation of reasons adequate substantiation of the reasons would in fact have been possible. These cases are therefore a matter of *procedural* shortcomings without involving any unlawful application of article 25 ISS Act 2002 in the *substantive* sense. (section 3.1)
- 8.3 With respect to one special category of persons that is discussed in greater detail in the secret appendix to this report, the Committee has established several instances of lack of due care in substantiating the reasons for applying article 25 ISS Act 2002. (section 3.1)
- 8.4 In regard to the application of article 27 ISS Act 2002 the Committee has arrived at the same findings as in review reports 19 and 26. Once again, therefore, it refrains from expressing an opinion on the lawfulness of the selection of Sigint by GISS. (section 3.2)
- 8.5 It is the opinion of the Committee that it is only possible to assess necessity, proportionality and subsidiarity if all the available relevant information is used in making the assessment. The Committee came across one case in which contraindications regarding the threat emanating from a target were not included in the substantiation of the reasons for continuing a tap. GISS had, however, provided these contraindications to the authorities concerned and they were evidently considered reliable. The Committee therefore holds the opinion that the substantiation of the reasons for this tap was incomplete and consequently lacked due care. (section 4)
- 8.6 In the course of its investigation the Committee came across a procedure according to which GISS prepares two parallel sets of reasons, one classified secret and the other top secret, for the application of article 25 ISS Act 2002 in one operation. This procedure has the consequence, however, that the secret set of reasons is incomplete and therefore inherently faulty. In addition, this procedure promotes a lack of due care and makes the Committee's review work more difficult. In one operation in which this procedure was followed the Committee was unable to establish whether the staff members involved in the internal assessment procedure were aware of the fact that there was also a top-secret set of reasons. The minister has announced that GISS will henceforth introduce safeguards to prevent carelessness, including the safeguard of actively informing the Committee whenever this procedure is applied. The Committee holds the opinion, however, that this use of two parallel sets of reasons is still at odds with the interest of careful and unambiguous substantiation of reasons. The Committee therefore recommends changing the internal procedures and not applying the procedure in question, except in cases in which it can be demonstrated that its application is necessary. (section 4)
- 8.7 The Committee has established that in the investigation of radicalisation trends it is not always evident that the person against whom or the organisation against which special powers are used do in fact give cause for serious suspicion that they pose a threat to national security. If during several statutory three-month periods no - or

hardly any - confirmation of the serious suspicion of the threat to national security is obtained, then after some time it is no longer justified to use the special powers. The Committee recognizes that in those cases it is difficult to make an assessment, but emphasizes the importance, in these cases, of continuously and critically evaluating the use of special powers. This is even more cogent if no or hardly any data is obtained that confirm the serious suspicion. (section 5)

- 8.8 In one case, in the context of a radicalisation investigation, GISS applied article 25 ISS Act 2002 for several years in order to establish the nature of the threat emanating from the secret activities of a number of persons. GISS did not succeed, however, in obtaining clarity as to this threat. The use of special powers has been terminated by now. It is the opinion of the Committee that particularly in the final period of this investigation the use of the power to tap or intercept approached the borderline of what is permitted by law. (section 5)
- 8.9 In one case in the context of its radicalisation investigations GISS used article 25 ISS Act 2002 in respect of a person who wished to publish a certain message. The Committee has established that at the start of the investigation GISS possessed limited information which did, however, offer sufficient leads for a serious suspicion of threat to national security. Although the Committee holds the opinion that the use of a telephone tap was lawful, it draws attention to the latitude which the wording of the reasons leaves for using this means in comparable cases. It is stated that it cannot be *excluded* that the message will be seen as an incitement to activism or serious disturbance of public order, or in the worst case scenario as an incitement to violence. This wording is very broad. The (mere) possibility of a threat to national security is insufficient to justify the use of telephone taps, a serious suspicion must have been established. The Committee also considers this important because individuals may in principle assume that their privacy will not be infringed merely because they wish to express their ideas. It is only when the publication may incite to e.g. radicalisation or the use of violence that it is lawful to use special powers. The Committee therefore recommends that in cases like the above GISS exercises restraint in using special powers. (section 5)
- 8.10 The Committee has established that GISS, when applying 25 ISS Act 2002 to a place or connection belonging to a third party but being used by a target, failed in a number of cases to properly include the third party's interests in its substantiation of the reasons for applying the special power. The Committee considers this a lack of due care. Especially so if several operations under article 25 ISS Act 2002 are ongoing with respect to one single target, including a tap or microphone at a location or connection belonging to a third party. In such cases GISS provides one set of reasons for all these taps combined, without devoting specific attention to the interest of the third party. GISS must, however, explain for each individual tap why it meets the requirements of necessity, proportionality and subsidiarity. This applies specifically where a tap or microphone is used at a place or in respect of a connection belonging to a third party. (section 6)
- 8.11 The Committee has established that GISS exercises adequate great restraint in applying article 25 ISS Act 2002 in respect of *non-targets*. (section 6)
- 8.12 In one case the Committee has established that GISS applied article 25 ISS Act 2002 while there were weighty reasons to consult with DISS before using a tap. In this case

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

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