REVIEW COMMITTEE
ON THE
INTELLIGENCE AND SECURITY SERVICES

CTIVD no. 19

REVIEW REPORT

on the application by the AIVD of Article 25 WIV 2002 (wiretapping) and Article 27 WIV 2002 (selection of undirected intercepted non cable-bound telecommunications)

Table of Contents

1. Investigation by the Committee

This Review Report of the Review Committee on the Intelligence and Security Services (hereinafter: the Committee) is about the application by the General Intelligence and Security Service (AIVD) of a number of special powers, namely those referred to in Article 25 and Article 27 of the Intelligence and Security Services Act 2002 (WIV 2002). Briefly, these concern the power to conduct wiretapping and the power to select undirected intercepted non cable-bound telecommunications, respectively. These powers will be explained in more detail in section 2 of this report.

Since late 2004, the Committee has been assessing the requests for and extension of the application of Articles 25 and 27 WIV 2002, which have been presented to the Minister of the Interior and Kingdom Relations (hereinafter: the Minister) and which the Minster has approved. In 2006 the Committee decided to perform an in-depth investigation into the application of these special powers. This in-depth investigation was announced to the Minister and the chairpersons of the Upper and Lower Houses of the States General by letter of 20 April 2006 in accordance with Article 78 paragraph 3 WIV 2002.
The Committee has since studied the requests on average once every three months. Most of the time all requests were examined; occasionally the Committee only examined a random sample. For the purpose of this in-depth investigation the requests were last reviewed in June 2008. After completion of this investigation, the Committee will continue to monitor the AIVD's application of the Articles 25 and 27 WIV 2002.

It is important to note that the Committee carries out supervision of the AIVD's activities after they have taken place. The requests for permission and extension, therefore, are not put to the Committee for approval before a decision is taken.
Pursuant to the WIV 2002 it is up to the Minister to grant permission for the application of the powers mentioned in the Articles 25 and 27 WIV 2002. In section 5 we will discuss the permission procedure in more detail.

During the investigation the findings of the Committee were always discussed with the AIVD's lawyers involved in this topic. Also interviewed were the present Minister of the Interior and Kingdom Relations, Mrs Ter Horst, and her predecessor, Mr Remkes, as the persons who had legal authority to grant permission for the application of these special powers by the AIVD.
Already during the investigation the discussions with the AIVD have resulted in the service carrying through several adjustments and improvements in the requests for permission and extension.

The review report at hand reports on the main findings. At any rate, insofar as these were found, mention is made of the requests which in the Committee's opinion do not meet one or more statutory requirement(s) including the requirements of necessity, proportionality and subsidiarity.

The review report has largely been organised based on the various statutory requirements laid down in the WIV 2002 for application of the Articles 25 and 27 WIV 2002.
After section 2 first explains what types of powers are involved, section 3 discusses that the powers can only be deployed for the proper performance of the A-task and D-task of the AIVD. Section 4 elaborates on the assessment criteria for the application of special powers. Subsequently, in section 5, attention is paid to the permission procedure. Sections 6 and 7

explain the requirements which the requests made to the Minister of the Interior and Kingdom Relations must meet to be allowed to apply Article 25 and/or Article 27 WIV 2002. Also because of the persistent social and political attention for the deployment of special powers against those having a (limited) right to withhold information, the review report has devoted a separate section to this (section 8).
Lastly, in section 9, we will discuss the obligation to remove and destroy unlawfully processed data, whilst section 10 lists the conclusions and recommendations from the report. The report contains a classified appendix, in which several issues are discussed in more detail.

The Committee has delineated the investigation by only looking at the *requests* that have been presented to the Minister of the Interior and Kingdom Relations in the context of the permission procedure and which the Minister has approved. The Committee has not looked into the actual application of the special powers from the Articles 25 and 27 WIV 2002 after the Minister's permission. This would make the investigation too comprehensive. The way in which the AIVD deals with the results of application of these articles therefore is not a topic of this investigation.
Other investigations of the Committee do pay attention to the execution and results. For example, the Committee investigates the official messages issued by the AIVD, whereby the underlying files often contain reports of the application of special powers (for example tapping reports). In that investigation the Committee checks whether these reports meet the statutory requirements.

Another aspect that falls outside the scope of this review report is the so-called notification obligation, which means that the AIVD, five years after termination of the application of certain special powers, including those laid down in the Articles 25 and 27 WIV 2002, reviews whether these may be reported to the person in respect of whom this power was exercised (Article 34 paragraph 1 WIV 2002). Considering the fact that the Act became effective on 29 May 2002[1], these notification investigations were only exercised for the first time in the second half of 2007. Therefore it is currently too early to draw any conclusions about this subject and to report on it. The Committee monitors the notification decisions of the AIVD and will report on its findings in due course.

2. The special powers of Article 25 and Article 27 WIV 2002

On 9 June 1994 the Administrative Jurisdiction Division of the Council of State ruled that the (old) Intelligence and Security Services Act (WIV 1987) did prescribe the (categories of) persons regarding whom the collecting of intelligence was allowed, but not the circumstances under which this was allowed to take place, nor which methods the – then – National Security Service (BVD) was allowed to use. The Council of State therefore concluded that the WIV 1987 did not meet the requirement laid down in Article 8 paragraph 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) that interference with the right to a private life may only take place if provided for by law.[2]

This ruling of the Council of State was the immediate cause for drafting the (new) Intelligence and Security Services Act 2002 (WIV 2002). This Act contains many changes

[1] Bulletin of Acts and Decrees 2002, 196.
[2] Administrative Jurisdiction Division of the Council of State 9 June 1994, *AB* 1995/238 (Van Baggum). At the same moment a ruling was given in the Valkenier case, which has not been published.

compared with the WIV 1987, the most important change for this report being that the special powers that the – newly named – AIVD and the Military Intelligence and Security Service (MIVD) have, are listed and described exhaustively in the Act. Two of these powers, Article 25 and Article 27, are described in more detail below.

2.1 Article 25 WIV 2002

Article 25 paragraph 1 WIV 2002 reads as follows:

> "The services are entitled with the aid of a technical device to wiretap, receive, record and listen in on any form of conversation, telecommunication or data transfer by means of an automated work, irrespective of where this takes place. The power, as mentioned in the first sentence, also includes the power to undo encryption of the conversations, telecommunication or data transfer."

Based on this article the AIVD may for example record conversations using a microphone, wiretap telephone conversations, read email messages and monitor a person's internet behaviour.

The article is broadly formulated. It involves *any form of* conversation, telecommunication or data transfer via an automated work. This means, among other things, that not only telephone *conversations* can be wiretapped, but also that data transfer taking place via a telephone line can be wiretapped.[3] For example, fax messages, or text messages. The advantage of such a broad formulation is that the AIVD can respond to new communication technology.

As shown by the description in the article it does not matter where the conversation, telecommunication or data transfer takes place ('*irrespective of where this takes place*'). A microphone may therefore be placed everywhere, including in someone's dwelling. Whether deployment of a means in a certain place is justified, is assessed on the basis of several assessment criteria including necessity, proportionality and subsidiarity. The assessment criteria are explained in section 4 of this review report.
During the drafting of the WIV 2002 the question was raised whether the words 'despite where this takes place' can mean that conversations, telecommunications and data transfer in other countries can be wiretapped from the Netherlands. The government provided the following answer to this:

> "First of all we note that the power of these services to wiretap conversations, telecommunications and data transfer as provided in Article 25 among other things, does not extend beyond the jurisdiction of the Dutch State. For the Dutch legislator cannot unilaterally create jurisdiction in other countries. However, this does not alter the fact that application of the power provided for in Article 25, in particular insofar as this concerns the interception of telecommunications as well as application of the powers laid down in the, by memorandum of amendment, inserted Article 25a [Committee: now Article 26] and Article 26 [Committee: now Article 27], can also extend to interception of telecommunications with an origin or destination abroad."[4]

Application of the methods referred to in Article 25 WIV 2002 implies a serious intrusion on a person's privacy, because cognisance is taken of the content of the communications of persons and organisations in a directed way. By application of this special power, the

[3] Parliamentary Documents II 1997/98, 25 877, no. 3, p. 41.
[4] Parliamentary Documents II 1999/2000, 25 877, no. 8, p. 65.

privacy of the telephone and telegraph laid down in Article 13 of the Constitution is violated. In the drafting of the WIV 2002, it was chosen not to provide a mandate arrangement for the special powers violating the more specifically provided rights of the Constitution, such as the right to inviolability of the home and the privacy of the telephone and telegraph.[5] This means that pursuant to Article 19 in conjunction with Article 25 paragraph 2 WIV 2002, only the Minister of the Interior and Kingdom Relations is competent to grant the AIVD permission for wiretapping. This permission can be given for a maximum of three months (Article 19 paragraph 3 WIV 2002). At the AIVD's request to this end, the permission may be extended each time by three months.

2.2 Article 27 WIV 2002

Article 27 paragraph 1 reads as follows:

> "The services are entitled to receive and record undirected intercepted non cable-bound telecommunications using a technical device. The power referred to in the first sentence also includes the power to undo encryption of the telecommunications."

As discussed in the previous section, Article 25 WIV 2002 provides that the AIVD may wiretap, receive, record and listen in on telecommunications. This provision provides for the *directed* wiretapping of the telecommunications of a person or an organisation known to the AIVD or of a telephone number known to the AIVD.

Article 27 paragraph 1 WIV 2002 also allows for the AIVD to intercept and records *undirected* telecommunications. This concerns non cable-bound telecommunications, i.e. ether traffic in the broadest sense of the word. In particular this refers to the interception of telecommunications traffic that takes place via satellites.[6] The AIVD does not intercept all ether traffic. Pursuant to Article 26 WIV 2002 (the so-called "searching") it is first assessed what frequencies or satellite channels are possibly interesting to keep under observation. If during searching, frequencies or satellite channels are taken cognisance of that may yield interesting intelligence for the AIVD, the AIVD may select undirected intercepted information sent via such frequencies or satellite channels. The term 'undirected' is referred to because, beforehand, it is unclear what the yield will be and whether it will contain any information relevant to the AIVD. In case of undirected interception and recording, no cognisance is taken as yet of the contents of the communication. The bulk information is only stored in the computer systems.
The AIVD does not need permission for this undirected interception and recording of information (Article 27 paragraph 2 WIV 2002). However, if the AIVD wishes to take cognisance of the contents of the communication, the AIVD must first ask the Minister of the Interior and Kingdom Relations for permission to select intercepted information on the basis of certain criteria, after which the selected part of the intercepted information, can be taken cognisance of. The power to select has been included in Article 27 paragraph 3 WIV 2002:

> "The services can select the data collected by exercising the power referred to in the first paragraph on the basis of:
> a. data concerning the identity of a person or an organisation;
> b. a number as referred to in Article 1.1, under bb, of the Telecommunications Act, or any technical feature;

[5] Parliamentary Documents II 1999/2000, 25 877, no. 8, p. 45-46 and Parliamentary Documents II 2000/01, 25 877, no. 59, p. 7-8.
[6] Parliamentary Documents II 1997/98, 25 877, no. 3, p. 44.

c. keywords related to a subject described in more detail."

The selection criteria mentioned under a and b do not require much explanation. These concern, for example, names, address details or social security numbers (sub a) or telephone numbers or IP addresses (sub b). Data collection based on these selection criteria concerns specific persons and organisations, as a result of which the search action is referred to as *directed.* Therefore for selection based on these data the same regime must be followed as with the application of Article 25 WIV 2002, which means that it is only the Minister of the Interior and Kingdom Relations who can give permission, for a maximum period of up to three months, after which a request for extension for another three months can be submitted.

For the selection based on keywords related to a subject to be described in more detail (sub c) a different arrangement has been formulated. In this case, data collection is not focused on a person or an organisation, but it is important for the investigations the AIVD is involved with (for example proliferations of chemical weapons)[7] in a general sense. Here, the keywords do not relate to persons or organisations, but to a specific subject. Upon introduction of this power in the WIV 2002, the following explanation was given:

> "A list of keywords related to a subject will as a rule consist of (combinations of) specific technical terms and specifications in various languages. Such a list is drafted in such a way that the selection system is optimally used to find the desired information. For example, a list of keywords in the context of an investigation into proliferation of certain dual-use goods to a specific country or region might consist, among other things, of the names of certain chemical substances and chemical compounds in combination with these countries or regions. A somewhat simplified example concerns the search for messages in which the word sodium (or the Dutch equivalent *natrium*) is found and also within two positions the word chloride or fluoride. A list of keywords to be used in an investigation into the export of a missile system to certain countries or regions might consist of various names by which the specific missile system is specified, any project names or designations of the various elements that make up part of the system in question."[8]

Because the personal privacy of persons and organisations is not directly at issue here – as the data collection is *not directed* at persons or organisations – the Minister of the Interior and Kingdom Relations may give permission for a longer period – namely for a maximum of one year – to select intercepted information in the context of the investigation of a certain described topic. Experts within the AIVD subsequently formulate keywords relating to this topic, on the basis of which the selection can be made.. Therefore the Minister of the Interior and Kingdom Relations does not need to give permission for the specific keywords. Legally, the permission regarding the formulated keywords must come from either the Head of the AIVD, or another officer appointed by him. However, the AIVD has opted for having this power exclusively exercised by the Head of the AIVD.

2.3 "Silent tap"

The Committee has established that the AIVD applies a special power – a "silent tap" – under the denominator of Article 28 WIV 2002 (retrieving traffic data) whereas in the Committee's opinion this method falls under the description of Article 25 WIV 2002 (wiretapping telecommunications).

---

[7] Parliamentary Documents II 1997/98, 25 877, no. 3, p. 45.
[8] Parliamentary Documents II 2000/01, 25 877, no. 14, p. 33.

Article 28 WIV 2002 provides that the AIVD can retrieve (telephone) traffic data from providers of public telecommunications networks and public telecommunications services. This way the AIVD can obtain data about, among other things, the dates and times at which someone called and the telephone numbers used for making the contact.[9] Article 28 WIV 2002 does not serve to take cognisance of the content of the communications that take place via the telephone connection. In that case permission from the Minister of the Interior and Kingdom Relations would be required pursuant to 25 WIV 2002, because this concerns the interception of (any form of) telecommunication. This difference was touched upon briefly during the drafting of the WIV 2002, when the monitoring of military data traffic was discussed:

> "In our opinion violation of the privacy of the telephone is involved if taking cognisance of the content of a telephone conversation is aimed at the very content itself. If the content of a telephone conversation is taken cognisance of purely as a brief part of an investigation into the identity of persons or institutions communicating with one another, we do not consider this as a violation of the privacy of the telephone. Rather, the [Committee: monitoring of military data traffic] is comparable with an investigation into traffic data. Such an investigation can indeed be considered as a violation of the right of privacy as laid down in Article 10 of the Constitution, but not as a violation of the privacy of the telephone laid down in Article 13 of the Constitution."[10]

No permission from the Minister of the Interior and Kingdom Relations is required for retrieving (telephone) traffic data (Article 28 paragraph 3 WIV 2002). It is sufficient that the request is made to the telecommunication providers by the Head of the AIVD (Article 28 paragraph 4 WIV 2002).

Article 28 paragraph 1 WIV 2002 provides that the request may pertain both to data already processed at the time of the request and data processed after the request. Therefore the AIVD may ask the telecommunication providers for the data regarding the use of the telephone during, for example, the past month, but the AIVD can also request to keep the service informed of this data in, for example, the next two weeks. In the latter case a technical facility makes it possible that the AIVD has immediate ('real time') access to the current data regarding the use of the telephone by a person. This is also referred to as a "silent tap". Basically, a silent tap is a telephone tap, the difference being that the sound signal in a silent tap is not provided to the AIVD.

The Committee has established that in a silent tap the sound signal may not be forwarded to the AIVD, but that in a number of silent taps applied by the AIVD, the content of (a form of) telecommunication was taken cognisance of as it turned out that text messages were also reaching the AIVD via the silent tap. The Committee has come across a case of a silent tap, whereby the AIVD received approximately 150 text messages in a short period of time. This is an exception. In most cases a much smaller number of text messages are involved. The number of silent taps whereby text messages were received, moreover, involved a minority compared with the silent taps where no text messages were received.
The text messages ending up at the AIVD via a silent tap are (automatically) stored in the AIVD's digital systems. The AIVD has indicated that at the moment it is impossible to avoid the inclusion of text messages in a silent tap. Nor is it possible at this moment to separate the text messages in the AIVD's wiretapping room from the information provided to the

[9] A full listing of the data that can be retrieved has been included in the Governmental Decree to Article 28 paragraph 1 WIV 2002, to be referred via http://wetten.overheid.nl.
[10] Parliamentary Documents II 2000/01, 25 877, no. 14, p. 35.

operational teams. As it does not intend to take cognisance of the content of the communication when applying a silent tap, the AIVD is of the opinion that the received text messages are to be considered so-called by-catch.

The Committee does not share this view held by the AIVD. In Article 2 of the Governmental Decree to Article 28 WIV 2002[11] text messages are not designated as data that can be retrieved from the telecommunications services pursuant to Article 28. This is not without a reason. The Committee calls to mind the 2000 report of the Committee "Constitutional rights in the digital era", also referred to - after its chairman,- as the Franken Committee. This report noted the following on traffic data:

> "Traffic data does not concern the content of the data traffic.
> Because Article 13 of the Constitution [Committee: inviolability of the privacy of correspondence, telephone and telegraph] has the very intention of protecting the content of the communication, traffic data is not protected by this Article. This data is however protected by Article 10 of the Constitution [Committee: respect for and protection of the personal privacy]."[12]

The Franken Committee describes various data that will also become visible in traffic data due to ongoing technological developments, an example being that in using the internet not only traffic data is recorded that pertains to the telephone traffic between user and dial-in access point of the provider of internet services, but it is also registered which websites have been visited.[13] In the Franken Committee's report no examples are provided of data that actually provides an idea of the content of the communications, such as text messages.

In the government's response to the report it shares the position of the Franken Committee that traffic data does not fall under the protection of Article 13 of the Constitution.

> "In the Committee and government's view there exists insufficient justification to bring traffic data under the specific protection of Article 13. This conclusion is related to the fact that traffic data may tell much about persons in our information society, but that the same applies for much more sensitive data that do not fall under the scope of Article 13. No proper arguments can be put forward to make a distinction in the constitutional protection level between categories of personal data based on the fact that it is or is not related to a content that, independently, is subject to constitutional protection."[14]

The Review Committee agrees with the view that in itself traffic data does not necessarily fall under the scope of the specific protection of Article 13 of the Constitution. However, as the text messages included when current traffic data is sent do themselves contain confidential communication, these messages are not "related to a content enjoying independent protection", but are in themselves a content enjoying constitutional protection. The fact that a text message involves confidential communication has been phrased by the government in its response to Parliamentary questions on the report as follows:

> "Electronic data traffic between individual citizens via email and text messaging falls under the scope of the proposal for Article 13 of the Constitution because it concerns confidential communication. The protection of confidential communication is not limited to communication actively protected, for example by means of encryption of the message. As

[11] See footnote 9.
[12] Report Committee on Constitutional rights in the digital era, May 2000, p. 159.
[13] Report Committee on Constitutional rights in the digital era, May 2000, p. 160.
[14] Parliamentary Documents II 2000/01, 27 460, no. 1, p. 27.

> mentioned, the nature of the channel chosen, the (manner of) addressing and the nature of the communication may serve as a guideline in determining the confidentiality."[15]

The text messages included in a silent tap therefore, in the Review Committee's opinion, fall under the protection of Article 13 of the Constitution. This is in line with what the government has also included in its position on the traffic data:

> "Insofar as taking cognisance of traffic data coincides with taking cognisance of information concerning its content, content-related information is involved..This content-related information falls under the stricter regime of Article 13."[16]

For wiretapping, interception, recording and listening in on (any form of) telecommunication – as a result of which the privacy of the telephone laid down in Article 13 of the Constitution is violated – a special provision has been included in the WIV 2002, namely Article 25, the application of which has been surrounded by extra safeguards as it is only the Minister of the Interior and Kingdom Relations who can give permission for the application of this method.
The Committee is of the opinion that, as long as it is technically unfeasible to avoid text messages being sent along with a silent tap or to ensure that text messages are separated in the wiretap room, a silent tap falls under the description of Article 25 paragraph 1 WIV 2002, namely under 'any form of telecommunication', because as a result of text messages being sent along, cognisance is taken of the content of the communication. Therefore the Committee urgently recommends that the request for permission to apply a silent tap must be made to the Minister of the Interior and Kingdom Relations in the way set out in Article 25 WIV 2002.

3. Deployment of special powers only for A-task and D-task

Under strict conditions the AIVD may apply special powers for its investigations. These powers are special because they infringe (secretly) on a recognised human right or constitutional right, with the purpose of collecting information on a person , an organisation, a specific subject or country. The WIV 2002 contains an exhaustive listing of special powers available to the AIVD. Article 18 of this Act provides that the AIVD may only apply special powers if this is necessary for the proper performance of the A-task and D-task. A special power may therefore not be applied for conducting security clearance investigations concerning persons who wish to fulfil a position involving confidentiality (B-task), for ensuring security measures (C-task) and for drawing up, upon request, threat and risk analyses for the protection of specific persons and the surveillance and protection of various objects and services (E-task).

3.1 The A-task of the AIVD

The A-task comprises conducting investigations regarding organisations and persons who, because of the goals they pursue or because of their activities, give rise to the serious suspicion that they pose a danger to the continued existence of the democratic legal order or to other vital interests of the state (Article 6, paragraph 2 sub a, WIV 2002). This description of task comprises among other things investigations into terrorism, radicalisation, undesired interference of foreign powers (including espionage), right-wing extremism, left-wing extremism, and animal rights activism. The areas of attention and tasks of the AIVD are

[15] Parliamentary Documents II 2000/01, 27 460, no. 2, p. 59.
[16] See footnote 14.

described every year in the annual plan[17] and the annual report[18] of the service. From this it can be inferred which activities (may) attract the attention of the AIVD.

If a person or an organisation *gives rise to the serious suspicion* that he, she or it poses a danger to the national security, the AIVD can conduct an investigation of this person or organisation. The fact that a serious suspicion needs to be involved, prevents the AIVD from being permitted to conduct an investigation of persons and organisations at random on the basis of the A-task. During the drafting of the WIV 2002 a question was raised about the relationship with the phrase pertaining to criminal law of "reasonable suspicion of guilt". The answer of the government was as follows:

> "Article 27 of the Code of Criminal Procedure provides that before prosecution has started, the only person regarded as a suspect is the person regarding whom, based on facts and circumstances, a reasonable suspicion of guilt of any criminal act arises. (...) Investigation and prosecution are focused on criminal facts. (...) The activities of intelligence and security services are focused on threats to national security, irrespective of whether any criminal acts are committed. The activities of intelligence and security services concern in the first place the timely warning against threats and consequently avoiding harm being inflicted on national security. This means that intelligence and security services are to be able to obtain intelligence as early as possible - also if there is not yet any clear idea of the plans of evil-minded persons."[19]

The serious suspicion therefore is focused on a threat to national security and not on any criminal act. Of course it cannot be ruled out that the threat to national security will ultimately manifest itself in a criminal act being committed.

The above-mentioned quote shows that for assuming a serious suspicion there is no need for the existence of "a clear idea" of "the plans of evil-minded persons". In the debate on the legislative proposal WIV 2002 there was no discussion on the minimum requirement for assuming a serious suspicion.
The terminology (serious suspicion) was already used in the former Intelligence and Security Services Act of 1987 (WIV 1987).[20] For an interpretation of the concept we may therefore look at the explanation that was given during the drafting of the former WIV. During the parliamentary debate on the legislative proposal of 1982, various political groups in the Lower House raised the question under what circumstances persons or organisations could give rise to the serious suspicion that they were threatening national security and the question was also raised why, unlike in the previous Royal Decree of 1972[21], it was no longer "the existence of a serious suspicion", but "giving rise to the serious suspicion" that was the phrase used in the legislation.[22] In a response to these Parliamentary questions it was stated

[17] The annual plan is classified as a state secret. Every year, the Minister of the Interior and Kingdom Relations sends a letter to the Lower House, in which the outlines of the annual plan are presented, see Parliamentary Documents II 2007/08, 30 977, no. 8 for the annual plan 2008.
[18] The annual report of the AIVD is published on the website of the service: www.AIVD.nl.
[19] Parliamentary Documents I 2001/02, 25 877, no. 58a, p. 14 (Memorandum of Reply).
[20] Act of 3 December 1987, Bulletin of Acts and Decrees 635, laying down rules on the intelligence and security services (WIV 1987).
[21] Before the drafting of the WIB 1987 the duties of the intelligence and security services were provided for by Royal Decree of 5 August 1972, Bulletin of Acts and Decrees 437, laying down the rules for the duties, the organisational set-up, working method of and cooperation between the intelligence and security services.
[22] Parliamentary Documents II 1982/83, 17 363, no. 5 (preliminary report).

in the Memorandum of Reply that an important aspect of the task of the – then – National Security Service (BVD) is

> "creating access to information in circles from which terrorist acts can be expected. The BVD is therefore already active at a stage when no crime has yet been committed, nor is any preparatory act – which is to be taken seriously - to commit a crime involved yet."[23]

As regards the change of terminology compared with the Royal Decree of 1972, it was noted that this involved an attempt to formulate more accurately the envisaged task description of the BVD.

> "Also under the task description of the Royal Decree of 1972 this service will need to have *some minimal knowledge* [italics Committee] before *on the basis thereof* [italics Committee] the Minister of the Interior will be able to draw the conclusion that there exists a serious suspicion that a danger to the continued existence of the democratic legal order is involved, or to the safety or any other vital interests of the state. Most of this minimal knowledge can be obtained from sources accessible to anyone, in particular in those cases in which a danger to the democratic legal order is involved. For a small part this will be the result of exploratory activities by the service. This latter aspect plays a role in particular in the context of the service's counter-espionage activities and the prevention of terrorist crimes."[24]

The choice of words – *serious* suspicion – implies that more than merely a suspicion needs to be involved. The explanation to the terms shows that this can already be the case if the AIVD has *some minimal knowledge* about the activities and/or objectives of a person or an organisation. But also before the AIVD has this minimal knowledge, it may, according to the Memorandum of Explanation of the former WIV, perform exploratory activities in target areas where experience has shown that activities and objectives that are threatening to national security can be developed and can manifest themselves.

At the time the Lower House asked for an explanation with regard to these "exploratory activities" in which context the question was raised whether "in this preparatory phase the National Security Service only collects intelligence if the service itself has a serious suspicion that an investigation will lead to the Minister concluding that a serious suspicion is involved, based on the intelligence collected." The government gave the following answer:

> "In the Memorandum of Reply we noted that the exploratory activities of the BVD play a role in particular in counter-espionage and the prevention of terrorist activities. These exploratory activities of course involve in the first place those target areas from which, based on the experience both at home and abroad, espionage and terrorist activities can be developed and subsequently in those areas where these activities may manifest themselves. In this sense we answer the question of the members affirmatively. To avoid any misunderstanding, however, we immediately add that the execution of exploratory activities is of course a recurring subject of discussion in the regular consultation between the Minister of the Interior and the Head of the National Security Service."[25]

The Memorandum of Explanation of the WIV 1987 does not specify in what operational manner the exploratory activities may be engaged in. During the drafting of the WIV 2002 this was not explained, either. The Committee holds the opinion that exploratory activities in the context of the performance of the A-task may at any rate not involve the application of special powers, such as wiretapping (Article 25 WIV 2002) and the selection of undirected

---

[23] Parliamentary Documents II 1983/84, 17 363, Nos. 6-7, p. 2.
[24] Parliamentary Documents II 1983/84, 17 363, Nos. 6-7, p. 5.
[25] Parliamentary Documents II 1984/85, 17 363, no. 12, p. 3.

intercepted and recorded non cable-bound telecommunication (Article 27 WIV 2002), which powers are the subject of the Committee's present investigation. The application of special powers infringes on the privacy of a person or an organisation in a directed way. This infringement is justified if there is a serious suspicion that this person or organisation poses a danger to national security. If the knowledge – and therefore also the serious suspicion – is lacking that a person or an organisation, due to the objectives it pursues, poses a threat to national security, the application of special powers, in the Committee's opinion, is not permitted.
In the present investigation the Committee has established that in performing its A-task the AIVD does not perform any exploratory activities by means of the special powers mentioned in the Articles 25 and 27 WIV 2002.

3.2 The D-task of the AIVD

The D-task – also referred to as the foreign intelligence task or foreign task – concerns investigations into foreign countries as designated by the Prime Minister, the Minister of General Affairs, in agreement with the Minister of the Interior and Kingdom Relations and the Minister of Defence (Article 6 paragraph 2 sub d WIV 2002). Previously, the subjects were designated annually.[26] With effect from the year 2008 the Designation Order was given a duration of four years.[27]

With the entry into force of the WIV 2002 the foreign task was assigned to the AIVD as a new task. It is aimed at obtaining information regarding subjects that are not directly related to *specific* threats to national security (see on this also section 3.3)[28]
Previously, this task had been vested in the Foreign Intelligence Service (IDB), which was abolished in 1994. The reason for resuming the tasks of the abolished IDB was, among other things, that the termination of the Cold War had not – as had been expected when the IDB was abolished – resulted in the disappearance of conflicts and hotbeds in Europe and elsewhere in the world. The relatively clear situation during the Cold War had on the contrary resulted in a considerably less clear-cut political and economical situation in the world. Intelligence about foreign powers was therefore again considered important for formulating Dutch policy.[29]

Article 1 of the Designation Order 2008-2012 designated the following subjects:

a. Political intentions, activities and opinions of governments, institutions and inhabitants of specifically designated countries or regions (political intelligence). All countries and regions of investigation are viewed based on the question what the real motives of the main players are, what the actual influence is of the government and what objectives are pursued.

---

[26] See among other things Designation Order 2005, Government Gazette 23 December 2004, no. 248, p. 10; Designation Order 2006, Government Gazette 20 January 2006, no. 15, p. 11; Designation Order 2007, Government Gazette 8 December 2006, no. 240, p. 9.
[27] Decision of 10 July 2007 on designation of the subjects mentioned in Article 6, second paragraph, under d, and Article 7, second paragraph, under e, of the Intelligence and Security Services Act 2002, Government Gazette 25 July 2007, no. 141, p. 21. The decision became effective on 1 January 2008 and ceases to have effect as from 1 January 2012.
[28] Parliamentary Documents II 1999/2000, 25 877, no. 8, p. 23.
[29] Parliamentary Documents II 1999/2000, 25 877, no. 8, p. 24-25 and Parliamentary Documents II 2000/01, 25 877, no. 14, p. 16.

b. The timely identification and signalling of and responding to developments in countries or regions that constitute a potential threat to national security (early warning / quick response). In this context data is collected, both solicited and unsolicited, on countries and regions not falling under the scope of Article 1a.

In the explanation to the Designation Order 2008-2012 it was stated that the topics to be investigated are designated in order to collect intelligence that enables the Dutch government in determining its positions on foreign policy and in conducting international negotiations, to have at its disposal information that is impossible or difficult to obtain via other, for example diplomatic, channels. The explanation continues:

> "This concerns collecting missing data which is relevant from the perspective of national security and which is only available to foreign intelligence and security services or can only be obtained with one or both services' own efforts. This means that the activities of the AIVD or MIVD are complementary to the existing tasks of the Ministry of Foreign Affairs and its representatives abroad."[30]

The added value of the AIVD's involvement is that the AIVD is in frequent contact with its foreign sister services and therefore can obtain data via the exchange of information. Also, unlike the Ministry of Foreign Affairs, the AIVD can make use of the application of special powers.

The areas of investigation have been broadly defined in the public part of the Designation Order. In the classified appendix of the Order the subjects are worked out in more detail and the countries or regions are specified which may be the subject of investigation, so that only the subjects are designated that require the AIVD's (or MIVD's) attention in the context of national security (Article 6 paragraph 2 preamble WIV 2002).

On 10 September 2007 the Committee announced an investigation into the legitimacy of the performance of the foreign task by the AIVD. The investigation involves the performance of the D-task in a broad sense.
In the investigation that is the topic of this report, we have only looked into the performance of the D-task insofar as the application of Articles 25 and 27 WIV 2002 was involved.

3.3 The importance of national security

Both the A-task and the D-task are to be performed in the interest of national security (Article 6 paragraph 2 preamble WIV 2002).

The concept of 'national security' was introduced as an overarching concept for the activities of the services. For this concept alignment was sought with Article 8 paragraph 2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), as a result of which the substance of this concept is also determined by the relevant case law.
In the drafting of the WIV 2002, the government held the opinion that – based on case law of the European Court of Human Rights (ECHR) – there is room for a further (national) interpretation of the concept:

> "The national legislator is given a (wide) margin of appreciation. This observation has led us to conclude that the concept of national security can and may be interpreted so broadly as to

[30] See footnote 27.

include at any rate everything that the services are currently doing based on their present mandate; this applies – with one or two caveats as far as the AIVD is concerned – also to the new tasks (the so-called foreign intelligence task of the AIVD and MIVD)."[31]

There is no case law on the general content and scope of the concept of national security. The ECHR's case law shows that the European Court assesses in each individual case whether a Signatory State has rightly invoked national security to justify the infringement of a human right. The ECHR indeed gives the Signatory States, as established by the government in the drafting of the WIV 2002, a broad discretion in the interpretation of the concept. Matters in which national security was at issue were related for example to the publication of state secrets[32], threats on account of espionage and terrorism[33] and the integrity of the civil service[34].

In the description of tasks of the AIVD (Article 6 WIV 2002) it is provided that an investigation based on the A-task can only take place with regard to persons and organisations who, because of the objectives they pursue or because of the activities they perform, give rise to the serious suspicion that they are a *danger* to the continued existence of the democratic legal order to the security or other vital interests of the state (Article 6 paragraph 2 sub a WIV 2002). Such a requirement that a *danger* to national security is involved is not expressed in the description of the AIVD's D-task (Article 6, paragraph 2 sub d, WIV 2002). For the D-task it therefore suffices that the investigation takes place in the interest of national security, as provided for in the preamble of Article 6 WIV 2002. In the drafting of the WIV 2002 the government explained this by considering:

"The new foreign intelligence task also allows the AIVD to perform activities aimed at obtaining information regarding subjects that are not directly related to concrete threats to national security."[35]

The ECHR's case law demonstrates that for a justification of secret investigations by intelligence and security services in the interest of national security there is no need for an *actual* violation of national security. The minimum requirement is a possibility of harm being inflicted on national security, in other words a *potential* infringement of national security.[36] Intelligence and security services may take measures that restrict human rights with the aim of seeking to avoid national security actually being harmed. If no harm to national security is to be expected at all, an infringement of human rights cannot be justified. In the in-depth PhD study of J.P. Loof into the compatibility of human rights and state security, the following is observed:

"In cases in which an infringement of the right to privacy is involved, the human right which usually is also at issue in government activities to combat espionage and in investigations by security services, this infringement is in principle also assumed to be 'in the interest of national security' if national security is not yet actually threatened, but may be jeopardised. The fact that the authorities in Strasbourg make a less stringent requirement in cases like these, is logical and inevitable with regard to the extent of danger to national security. Actions

[31] Parliamentary Documents II 1999/2000, 25 877, no. 9, p. 14.
[32] ECHR 26 November 1991 (Observer and The Guardian/United Kingdom).
[33] ECHR 6 September 1978 (Klass et al/Germany), § 48; ECHR 5 July 2001 (Erdem/Germany).
[34] ECHR 12 December 2001 (Grande Oriente d'Italia di Palazzo Giustiniani/Italy), § 21.
[35] Parliamentary Documents I 2001/02, 25 877, no. 58a, p. 2 (Memorandum of Reply).
[36] See for example ECHR 6 September 1978 (Klass et al/Germany) and ECHR 26 March 1987 (Leander/Sweden).

> of and investigations by security services are often (also) aimed at avoiding situations that threaten or harm state security (...). It is however logical to require in such a case that the possibility of state security being in danger, is at least demonstrated by factual circumstances or specific suspicions, otherwise states will all too readily be given a permit to subject everyone to a security investigation (and the inherent infringement of the privacy)."[37]

The requirement referred to by Loof that there must be facts or specific suspicions in order for a potential violation of national security to be involved, with regard to the A-task of the AIVD is expressed in the requirement that there must be a serious suspicion (more about this in section 3.1). For the foreign task the WIV 2002 does not contain such a requirement.

It should be noted that the potential violation of national security is different for the A-task and the D-task. The difference is found in particular in the fact that the possible violation is normally more concrete for the A-task than for the D-task. The A-task often concerns threats that may manifest themselves in the short term, for example a terrorist attack, a (violent) action by right-wing or left-wing extremists, state secrets or confidential information ending up with unauthorised persons (for example relating to espionage), et cetera. Such violations of national security will typically manifest themselves within a shorter term than potential violations the AIVD investigates based on its D-task. The D-task mainly involves investigations into the potential violation of national security in the long(er) term. International developments are monitored that may have an adverse effect on national security in the Netherlands in the future. Precisely how this violation may ultimately manifest itself is more difficult to assess than within the A-task. At any rate in designating the subjects which the AIVD is to investigate in the context of its D-task (Article 6 paragraph 2 sub d WIV 2002), sufficient attention needs to be paid to the question whether the subjects constitute a potential violation of national security.

3.4 Findings of the Committee

The Committee has established that the AIVD – in accordance with the law – does not make use of the special powers of the Articles 25 and 27 WIV 2002 in performing the B-task mentioned in Article 6 paragraph 2 WIV 2002 (performing security clearance investigations concerning persons who wish to fulfil a position involving confidentiality), the C-task (promoting security measures) and the E-task (drawing up threat and risk analyses upon request for the protection of certain persons and the protection and security of various objects and services).
Both for the A-task and the D-task the AIVD makes use of the special powers mentioned in the Articles 25 and 27 WIV 2002. The investigations for which these special powers are applied fall under the task description of the AIVD.

4. Assessment criteria for the deployment of special powers

The AIVD has to observe the provisions in the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). Article 8, paragraph 1, ECHR provides that everyone is entitled to respect for his private life, his family life, his home and his correspondence. When the AIVD applies special powers, one or more of these rights are

[37] J.P. Loof, *Mensenrechten en staatsveiligheid: verenigbare grootheden? Opschorting en beperking van mensenrechtenbescherming tijdens noodtoestanden en andere situaties die de staatsveiligheid bedreigen* (Human Rights and State Security: are they compatible? Suspension of and limitation to human rights protection during emergency situations and other situations that are a threat to state security) (dissertation University of Leiden), Nijmegen: Wolf Legal Publishers 2005, p. 339.

violated. The second paragraph of Article 8 ECHR contains a restrictive clause and provides that no interference by any public authority in exercising this right is permitted, if not provided for by law and *necessary in a democratic society,* in the interest of national security or another interest as referred to in the second paragraph.

The amount of case law of the European Court concerning cases where, in the interest of national security, the right to privacy has been violated because of secret investigations by an intelligence and/or security service, is limited. Based on the case law available and similar case law in matters where, albeit not by an intelligence and/or security service, a fundamental right has been violated in the interest of national security (for example a restriction of the freedom of speech to prevent state secrets from being published), a few observations can be made on the ECHR's assessment in answering the question whether an infringement on a human right is necessary in a democratic legal order.
In the drafting of the WIV 2002 the assessment criteria of the ECHR ended up in the act in different places. Below we will discuss the assessment criteria of the ECHR and the provisions in the WIV 2002 in their mutual context, thus providing an overview of the criteria which are to be met in order to be permitted to infringe on the privacy of persons and organisations by applying special powers.

The assessment criteria for the application of special powers can be divided into two categories:

1. The necessity criterion (section 4.1)
2. Proportionality and subsidiarity (section 4.2)

4.1 The necessity criterion

Article 18 WIV 2002 provides that a special power may only be exercised insofar as this is *necessary* for a proper execution of the A-task or D-task. This provision is relevant in particular to the application of special powers. For all of the AIVD's tasks, the necessity requirement is also found in Article 12 paragraph 2 WIV 2002, which provides that the processing of data only takes place for a specific purpose and only insofar as necessary for a proper implementation of this Act or the Security Clearance Act. Collecting data, for example by applying special powers, is a form of data processing (Article 1 sub f WIV 2002), as a result of which the use of special powers is subjected to the principle of necessity if only on the basis of Article 12 paragraph 2 WIV 2002.

In order to meet the necessity criterion, according to ECHR case law there must be a pressing social need that justifies the violation of the human right in question.[38] Whether there is such a need, is to be assessed on a case-by-case basis.
In the Handyside vs the United Kingdom ruling from 1976, the ECHR tightened the concept of necessity by considering that it may not be put on par with "indispensable", "absolutely necessary", "strictly necessary" and "strictly required by the exigencies of the situation", but on the other hand that it is not such an elastic concept that it may be interpreted as "admissible", "ordinary", "useful", "reasonable" or "desirable".[39] Two years later in the ruling Klass et al vs Germany (1978) the ECHR found that in the case of a secret investigation by an intelligence and security service, the concept of necessity is to be interpreted more restrictively:

[38] See for example ECHR 26 March 1987 (Leander/Sweden), § 58.
[39] ECHR 7 December 1976 (Handyside/United Kingdom), § 48.

> "Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention *only insofar as strictly necessary* [italics Committee] for safeguarding the democratic institutions."[40]
> (…)
> "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction. The Court has therefore to accept that the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, *under exceptional conditions* [italics Committee], necessary in a democratic society in the interests of national security and/or for the prevention of disorder or crime."[41]

This restrictive approach by the ECHR was confirmed in its more recent case law.[42] Thus, the AIVD is only permitted to infringe on a human right if a pressing social need is involved, which in case of a secret investigation means that the infringement must be strictly necessary in a democratic society.

The method used to infringe on the rights of a person must contribute to the purpose for which it is used, in order to be classified as necessary.
In the WIV 2002 this requirement is laid down in Article 12 paragraph 2, which provides, among other things, that data processing only takes place for a specific purpose. In addition, Article 32 WIV 2002 provides that application of a special power is to be stopped immediately if the purpose for which the power is exercised, has been achieved. It is self-evident that if the employed method does not – or can not - contribute to the purpose (any longer), this method may not (longer) be employed.

This means that prior to the application of a special power the AIVD must have a purpose for which this power is employed and that the expectation exists that the result of exercising this power will contribute to achieving the goal. After commencement of the application, the result must actually contribute to the investigation. For example, if due to a shortage of audio processors it is impossible to listen to a telephone tap, the telephone tap has to be stopped because in this case it does not contribute to the purpose for which the tap was applied (any longer), and therefore is not necessary (any longer). In case of a request for extension of the application of a special power, explicit attention must be paid to the result of the method and the added value of it for the investigation.

4.2 Proportionality and subsidiarity

The infringement made on the fundamental right is to be reasonably proportionate to the purpose served with the infringement (the proportionality principle).[43] This requirement is found in the WIV 2002 in Article 31, which provides that the power will not be exercised if it concerns a disproportionate disadvantage to the person involved when compared with the goal to be pursued (paragraph 3) and that exercising a power is to be in proportion to the

[40] ECHR 6 September 1978 (Klass et al/Germany), § 42.
[41] ECHR 6 September 1978 (Klass et al/Germany), § 48.
[42] ECHR 4 May 2000 (Rotaru/Romania), § 47, ECHR 6 June 2006 (Segerstedt-Wiberg et al/Sweden), § 88 and by analogy for secret investigations in the context of criminal law: ECHR 2 November 2006 (Volkhy/Ukraine), § 43.
[43] See for example ECHR 26 March 1987 (Leander/Sweden), § 58 and ECHR 6 June 2006 (Segerstedt-Wiberg et al/Sweden), § 88

purpose envisaged (paragraph 4). The interest served with the application of the special power – national security – is to be weighed up against the interests of the person involved.
The interests of the person involved are in the first place the right to respect of privacy (Article 8 ECHR and Article 10 Constitution). Several times the ECHR has ruled that also business activities fall under the scope of 'private life'.[44] Depending on which special power is employed and the social position a person or an organisation regarding whom the power is employed holds, other interests can play a part as well, such as the privacy of the telephone (Article 13 Constitution), the lawyer-client privilege and the right to withhold information for other holders of confidential information and the right to source protection for journalists. In section 8 the (limited) right to withhold information is entered into in more detail.

In determining the proportionality the ECHR uses among other things the criterion that the infringement made to achieve the goal is to be as limited as possible. This can be achieved by using a less severe (special) power, but also by applying the same special power in a way that produces the least infringement for the person involved. In the ruling Erdem vs Germany (2001) the ECHR found for example that reading the correspondence between a prisoner and his lawyer was proportionate, among other things, because the reading was done by an independent judge who was not involved in the criminal investigation, because this judge had to treat the correspondence confidentially and because the prisoner was allowed to communicate with his lawyer undisturbed.[45]

In the WIV 2002 the condition that the infringement has to be as light as possible – also known as the subsidiarity requirement – can be found in Article 31 paragraphs 1 and 2 and in Article 32. Article 31, paragraph 1, provides that the application of special powers is only allowed if the envisaged collection of data cannot be (timely) performed by consulting publicly accessible sources of information (such as the newspaper or the internet) or sources of information for which the service has been granted a right of access to the data (for example the Municipal Person Records Database and the police registers).
If the data cannot be obtained from these sources of information, according to Article 31 paragraph 2, the method will be employed which, considering the circumstances of the particular case in hand, including the severity of the threat to the interests to be protected by the service, also in comparison with other available powers, is least disadvantageous to the person involved. Likewise Article 32 WIV 2002, which provides among other things that the application of a special power is stopped if a less severe power suffices. In the drafting of the WIV 2002, the government has given an example of a situation in which the application of a special power results in a disproportionate disadvantage to the person involved:

> "If it is necessary to establish with whom a certain person conducts telephone conversations, this can be done in several ways. For example by fixing a telephone tap, but also via a so-called numerator action. It is evident that, considering the data required, the fixing of a telephone tap in this case constitutes a disproportionate disadvantage to the person involved and therefore a numerator action is to be opted for."[46]

It is sometimes difficult to apply a hierarchic structure to the various special powers that can be applied by the AIVD, based on the extent of infringement of the rights of the person involved. However, the legislator has applied different levels of permission to be given for

[44] See among other things ECHR 25 March 1998 (Kopp/Switzerland), § 50 and ECHR 25 October 2007 (Van Vondel/Netherlands), § 48.
[45] ECHR 5 July 2001 (Erdem/Germany), § 67.
[46] Parliamentary Documents II 1999/2000, 25 877, no. 8, p. 74.

the application of the various methods of gathering intelligence. A higher permission level implies a more serious infringement of the rights of the person involved. A tap (Article 25 WIV 2002) and the selection of undirected intercepted non cable-bound telecommunications (Article 27 WIV 2002) therefore can be considered as more serious special powers, because only the Minister of the Interior and Kingdom Relations has the competence to give permission for the employment of this method. For an observation, for example (Article 20 WIV 2002), and the deployment of agents (Article 21 WIV 2002), permission at team head level is allowed via an authorisation. As a result, these can be regarded as less severe special powers.

The actual gravity of the infringement is however determined more by the (technical and practical) way in which a special power is used, and the duration and result of the application. For example, if a telephone is wiretapped for just one day or if selection of undirected intercepted non cable-bound telecommunications does not result in any hits, the actual infringement is less serious than if the AIVD retrieves telephone traffic data of a person each month during a whole year. It therefore needs to be assessed in each individual case whether the conditions of proportionality and subsidiarity have been met. This is to be found in the reasons given for the application of a special power.

5. Permission procedure

The AIVD is only entitled to wiretap a person or an organisation or examine whether the undirected intercepted non cable-bound telecommunications contain information that is relevant for the investigation, if the service has been given permission for this by the Minister of the Interior and Kingdom Relations (Article 25 paragraph 2 and Article 27 paragraphs 4 and 5 WIV 2002, respectively). Contrary to most of the other special powers, for these special powers the legislator has not considered it desirable that the Head of the AIVD or, via authorisation, subordinate officers (Article 19 paragraph 2 WIV 2002) can give permission on behalf of the Minister (Article 19 paragraph 1 WIV 2002).

Before the executive level of the AIVD puts a request for permission to apply a special power or to extend this application to the Minister of the Interior and Kingdom Relations, the request will have passed through the service for an assessment of its (legal) tenability. Besides the team that has initiated the request, successively, the lawyer involved in the operational processes within a board, the director of the directorate under which the team falls, and the Legal Affairs Cabinet (the central legal department) are to have consented to the request.
The Committee has established that this internal assessment contributes to more careful deliberation processes within the AIVD. Often the team involved needs to state further reasons for the request before it is approved, and sometimes the request is denied and does not even reach the Minister.

Pursuant to the provisions laid down in Article 19, paragraph 3, WIV 2002 the permission, insofar as this has not been deviated from in the WIV 2002, is granted for a period of no more than three months, which period may be extended upon request for another three months. The maximum period for which permission can be given, i.e. three months, applies to wiretapping persons and organisations (Article 25) and the selection of undirected intercepted non cable-bound telecommunications based on data concerning the identity of a person or an organisation (Article 27 paragraph 3 sub a) and based on a number or any technical feature (Article 27 paragraph 3 sub b). For selection based on keywords that are related to a subject (Article 27 paragraph 3 sub c), a different period is applicable, namely a

period of one year (Article 27 paragraph 5). In the drafting of the WIV 2002, the following explanation was given:

> "The different period for which permission is given for a selection based on keywords, is based on the fact that this does not automatically involve a directed search for data that concerns a specific person as a result of which the personal privacy is immediately at stake. In a selection based on keywords related to subjects, the search is more focused on data that is relevant to a specific investigation the service is involved in."[47]

The Committee has established that in practice almost all requests for granting permission are for the maximum period. This is mainly for practical reasons. The AIVD has structured the permission procedure by running it in three-monthly cycles. This avoids having the Minister of the Interior and Kingdom Relations constantly deal with requests for permission. In the present procedure, all requests are bundled once every three months and submitted to the Minister of the Interior and Kingdom Relations, which the AIVD also refers to as the "three-monthly collective decision". Only urgent matters are presented to the Minister in the interim, after which these operations, if extended, are taken up in the collective decision to afterwards be included in the three-monthly cycles.
The second advantage is that as a result of this procedure the telecommunication companies will not constantly receive requests from the AIVD to fix or unfix wiretaps. In the present procedure the telecommunication company, with the exception of the intermediate (emergency) connections, has to check only once every three months which communication lines are to be opened for the AIVD.
Another advantage for the AIVD is that the results can be optimised if the special power is deployed for the maximum period.
Also when the permission has been granted for the maximum period of three months, the AIVD must constantly ask itself whether employment of the method in question is still justified. If, for example, it turns out that another person makes use of a telephone connection than the person the AIVD intended to wiretap, the telephone tap is to be ended immediately, even if the AIVD formally has permission to wiretap the telephone number for the period of three months. This is also the case if the purpose for which the special power is applied, has been achieved. If, for example, the purpose of retrieving a person's telephone number via a wiretap of another person's telephone number has been achieved, it is no longer permitted to wiretap the telephone line.
It would be stretching the present investigation too far to investigate whether the AIVD discontinues the application of special powers in all cases where there is cause for this. However, based on the phrasing chosen by the AIVD in its requests for permission or extension thereof, the Committee has established that the AIVD is aware that the application of a special power is to be stopped if there is no longer any basis for it. That the AIVD indeed acts upon this, has also become apparent from the reasoning in written decisions to terminate the application of a special power, which have given the Committee insight into the reasons given by the AIVD for discontinuing this application. These decisions to terminate the application of a special power show that the AIVD stops this application when there are clearly identifiable circumstances that lead to the conclusion that the application of a special power is no longer justified.

[47] Parliamentary Documents II 2000/01, 25 877, no. 59, p. 25.

6. Requirements for the request for permission or extension under Article 25 WIV 2002

The request made to the Minister of the Interior and Kingdom Relations for applying Article 25 or Article 27 WIV 2002 is to meet several requirements, in order that a well-founded opinion can be formed on the question whether the infringement, by application of a special power, of the rights of the person(s) involved is permitted. The (formal) requirements for the requests to apply Article 25 WIV 2002 and Article 27 WIV 2002, respectively, differ from one another on some points, as a result of which these will be discussed in two separate sections. Below, we will first enter into the requirements for the requests pursuant to Article 25 WIV 2002. Next, in section 7, we will discuss the requirements for the requests pursuant to Article 27 WIV 2002.

For several years now, the Committee has been examining the requests for permission and extension submitted to the Minister of the Interior and Kingdom Relations.[48] In some periods, the requests have been examined by means of a random check. In most periods the Committee has assessed all requests. Matters that the Committee noticed in this context were communicated to the AIVD. The Committee can establish with satisfaction that the AIVD has carried through various improvements in its requests for permission and extension. For example, the grounds provided in the requests for application of Article 25 WIV 2002 have become clearer over the years. Presently the request generally contains more detailed grounds, which are also more specifically related to the person involved. Therefore more attention is paid to the statutory requirements for the deployment of special powers. The requests for extension also pay more attention to actual results achieved over the previous period.
On several points the requests for permission and extension are capable of improvement.

Article 25 paragraph 4 WIV 2002 under a, b and c lists the requirements the request to the Minister of the Interior and Kingdom Relations for wiretapping must meet. These requirements will successively be discussed below.

6.1 An indication of the power and, insofar as applicable, the number

Article 25 paragraph 4 sub a WIV 2002 provides that the request must include a designation of the power the service wishes to apply and, insofar as applicable, the number, referred to in Article 1.1, under bb of the Telecommunications Act[49].

The request is to specify whether it concerns (a) listening in on and recording conversations (for example using a microphone), (b) wiretapping and recording telecommunication (for example using a telephone tap) or (c) wiretapping and recording data transfer via an automated work (for example wiretapping of data communication between computers).
Another requirement is that the number is stated on which the tap is to be fixed. Sometimes, at the moment of submitting the request, the AIVD is not (yet) aware of the number, but

[48] The supervision by the Committee takes place afterwards (Parliamentary Documents II 1997/98, 25 877, no. 3, p. 79). The Committee is therefore not involved in the permission procedure.
[49] Article 1.1., under bb, of the Telecommunications Act provides that "number" should be understood to mean: "figures, letters or other symbols whether or not in combination, that are intended for access to or identification of users, network operators, services, network connection points or other network elements." A further explanation of the concept can also be found in the Explanatory Memorandum to the Telecommunications Act (Parliamentary Documents II 1996/97, 25 533, no. 3, p. 74-76).

expects to know it in the future. In order to proceed as quickly as possible to the application of the power, the WIV 2002 has opened the possibility to ask for permission without stating the number. In that case permission is granted under the condition that the power may only be exercised once the relevant number is known (Article 25 paragraph 5 WIV 2002).
Based on this provision the AIVD, in the context of the three-monthly collective decision (see section 5), simultaneously requests the Minister of the Interior and Kingdom Relations, in one general request, for permission for all persons and organisations that are wiretapped, to also perform the power with respect to any newly disclosed telecommunication characteristics of the persons and organisations that are wiretapped. If for example the AIVD asks for permission to wiretap the mobile phone belonging to a target and then discovers after a month that the target has a second mobile phone, the AIVD does not have to ask the Minister for separate permission for this. The AIVD's internal guidelines provide that the Legal Affairs Cabinet is to give permission to also exercise the power with regard to the new number.
If in the interim wiretapping takes place on a new number, at the next three-monthly collective decision, a separate request for extension is submitted which states the new number. Thus, if two mobile telephone numbers are being wiretapped, two requests for extension are submitted.
The major practical advantage of the procedure that the Minister gives prior permission for applying the power with regard to the other numbers as well, is that a power can be applied to a target quickly.

The Committee has established that a mid-term extension of the power with regard to new telecommunication characteristics is often performed. The Committee has no objections to this, provided the AIVD ensures that the extension pertains to the same type of power (see above: a, b or c) for which the Minister has granted permission. For wiretapping and recording telecommunications (category b) the provision in Article 1.1 under bb of the Telecommunications Act is relevant. Specifically, this means that when the AIVD has given permission for wiretapping a telephone number, this permission can be extended with for example an IP-address (another number pursuant the Telecommunications Act).

The Committee has also established that, in one case, the AIVD has interpreted the general permission of the Minister of the Interior and Kingdom Relations to extend the power to other numbers of the person involved, too broadly. In this case the initial permission concerned a telephone tap on a target. In the meantime the AIVD had reason to suspect that the target was using another person's telephone to (covertly) conduct telephone conversations (see in this context section 6.2.2, under category II). The AIVD decided to also wiretap this telephone, but failed to request the Minister for new permission. It simply included the wiretapping of the new telephone number under the Minister's general permission for extending powers to other telecommunication characteristics. However, in the Committee's opinion, a separate decision-making process is required to assess whether infringing the rights of this other person – for it is his telephone that is being wiretapped and his privacy that is infringed on – is justified, and therefore specific permission from the Minister of the Interior and Kingdom Relations is required. The application of the special power, in the Committee's opinion, did however meet the requirements of necessity, proportionality and subsidiarity.

6.2 Data concerning the identity of the person or organisation

The request for permission must also state against whom the power is exercised. Article 25, paragraph 4, sub b, WIV 2002 provides that the request is to include data concerning the

identity of the person or organisation against whom exercising the power in question is requested.

It will be clear that in most cases the AIVD is has knowledge of some data concerning the person or organisation it intends to wiretap. The AIVD knows the identity data of most targets. However, not in all cases does the AIVD have this identity data. Consider for example the situation in which a person with a pre-paid telephone has frequent contact with targets under the AIVD's tap, and the contents of the conversations give rise to wiretap this person's telephone also. The name and address of this person may not be known to the AIVD (yet), nor can these be retrieved from the telecommunication provider if it concerns a pre-paid telephone. In that case permission for a so-called NN-tap[50] can be asked on the basis of Article 25 paragraph 6 WIV 2002. The permission will only be granted under the condition that the identity data of the person are supplemented as soon as possible.

6.2.1 Supplementing data in requests regarding an organisation

Article 25 paragraph 6 WIV 2002 offers the possibility to supplement the data concerning the identity of an *organisation* at a later stage. The Committee has established that the AIVD also includes in this identity data the names of the members of the organisation. Sometimes for wiretapping a group of persons the AIVD makes use of *requests regarding an organisation* (also referred to by the AIVD as "organisation requests") in which reasons are given to the effect that an investigation into the organisation on the basis of Article 25 WIV 2002 is necessary. In a request regarding an organisation the members of the organisation, as far as these are known to the AIVD, are listed which the AIVD wishes to wiretap. These persons are not always (all) known to the AIVD beforehand. For this reason, in its request regarding an organisation, the AIVD also requests the Minister's permission to wiretap the persons who meet certain criteria (for example a specific position within the organisation). If, after receiving permission, the AIVD identifies a new member of the organisation who meets the criteria in the organisation request, and the AIVD wishes to wiretap this person, the AIVD will proceed to do this without separately asking prior permission from the Minister of the Interior and Kingdom Relations for this individual person. The AIVD has laid down in internal guidelines that the team that wishes to apply the power, requires the prior permission of the legal department, the so-called Legal Affairs Cabinet, in order to wiretap the new individual.

In the Committee's opinion it is better to ask for separate permission for each individual to whom the AIVD wishes to apply this special power, in order that a careful assessment can be made as to whether all statutory requirements have been met. The Committee has however established that Article 25 paragraph 6 WIV 2002 indeed allows the AIVD room to independently wiretap newly disclosed members of the organisations in the interim. The Committee recommends that as regards organisation requests, the AIVD carefully describe why an organisation is involved, which category of persons from the organisation can be wiretapped and why the statutory requirements of necessity, proportionality and subsidiarity to wiretap this category of persons from the organisation, have been met. If in the interim a newly disclosed person is wiretapped, it is important to record why in the AIVD's opinion this person falls under the category of persons stated in the request regarding an organisation. The Committee considers it positive that the internal guidelines include that the Legal Affairs Cabinet is to give permission to also wiretap new individuals, so that a legal assessment is made internally with regard to this individual, in particular by

[50] NN = nomen nescio.

assessing whether the person involved meets the criteria stated in the request regarding an organisation.
The Committee has established that in one case the AIVD did not formulate a clear organisation request, while it had already started wiretapping a newly disclosed member of the organisation. The Committee considers this careless, and recommends that the AIVD draw up a clear organisation request each time the service wishes to wiretap a group of persons as an organisation.

6.2.2 Data on the identity of a target or a non-target

Insofar as the identity data of the person (in case of individual requests) or the organisation (in case of organisation requests) is known, this are to be included in the request for permission or extension immediately (Article 25 paragraph 4 sub b WIV 2002). Previously, the AIVD interpreted this article in such a way that the request was to include the identity data of the person or organisation *regarding whom* the AIVD wished to obtain more information, in other words: the target of the investigation. For example, if the AIVD conducted an investigation of a target whose place of residence was unknown (as yet) and the AIVD expected to be able to find out the place of residence using a wiretap on a person in the immediate environment of the target (a non-target), the AIVD would request the wiretap on the basis of the name of the target and not the name of the non-target.
The Committee considered this to be incorrect and has made some comments about this to the AIVD. In cases such as these it is not (solely) the privacy rights of the target that are violated, but in particular the privacy rights of the non-target, because his conversations are wiretapped.

This discussion is important in particular for the AIVD's notification obligation (Article 34 WIV 2002). This obligation entails that within five years after termination of the application of several special powers (including Article 25 WIV 2002), the AIVD is to inform the person involved that a special power has been applied to him, unless there are reasons not to notify this person. At that moment it is important to know exactly whom the special power was applied to.

The AIVD has endorsed the Committee's views and has meanwhile adjusted the requests for permission and extension to the Committee's ideas on this.
Roughly speaking three categories can be distinguished:

I. The place or connection to which the special power is applied belongs to the target.

In these cases, for example, if the mobile telephone or fixed telephone connection of the target is wiretapped, a microphone is installed in the target's home or his internet connection is tapped. By employing such means the AIVD attempts to learn of the actions (in particular communication) of the target. The request for permission must therefore be made on the basis of the name of the target.
In some cases the activities of persons other than the target may be taken cognisance of. For example, if housemates also use the fixed telephone connection or if a microphone in a dwelling intercepts noises from other residents. The application of the power is not intended for this, but it is unavoidable that the privacy rights of these third parties are violated. Insofar as this exposes information that is relevant for the AIVD's investigation, this can be regarded as by-catch.

II. The place or the connection to which the special power is applied does not belong to the target, but the target makes use of it.

Persons in whom the AIVD is interested are often (to some extent) aware of this. For this reason these targets sometimes do not make use of their own home or means of communication to perform secret actions, but they opt for another location or public means of communication to hide their activities from the AIVD. In order to still closely monitor such "smart targets" the AIVD can apply the special power in places or to means of communication that may not belong to the target, but which the target makes use of. In these cases also, as with category I, the purpose of the AIVD is to learn of the actions (in particular communication) of the target and the request for permission will need to be submitted on the basis of the name of the target. In stating reasons, explicit attention is to be paid to the circumstance that the place or means of communication belongs to a third party.

This method also infringes on the privacy rights of persons other than the target, namely the persons to whom the place or means of communication belongs. In weighing the interests involved, to decide whether application of the special power is justified, it needs to be continually considered whether the importance of surveillance of the target (still) outweighs the infringement made on the rights of third parties. A strong indication for this is the result of employing the chosen method. This means that the result must show that the target indeed makes use of the place or means of communication belonging to the other person, for (secret) activities. The result must also show that the information gathered by this method is relevant to the investigation, and that this knowledge cannot be obtained in any other way.

As with category I, application of the special power may produce relevant by-catch. It is obvious that there exists a proper ratio between the result that is the very aim of the application and the by-catch, because the purpose of the application is not to trace the actions of third parties. The AIVD therefore is to exercise restraint in processing information regarding activities of these third parties. If as a result of by-catch the AIVD starts collecting targeted information about this third party or these third parties (category I) or via this third party or these third parties about the target (category III, see below), and the application of the power (also) serves a different purpose than the initial purpose to trace the target's actions, in the Committee's opinion another request is to be submitted based on category I or category III.

III. The place or connection for which the special power is deployed does not belong to the target and the target does not make use of it.

This category concerns the application of the special power to a so-called non-target. The purpose is to take cognisance of the actions the non-target performs, as a result of which the AIVD expects to receive information on the target. The request for permission or extension therefore needs to be submitted on the basis of the name of the non-target. The previously mentioned example in which the AIVD attempts to find out the place of residence of a target by placing a telephone tap on a person in the target's environment, falls under this category.

In some cases the AIVD does not get a sufficiently clear picture of a target if powers are applied solely to the target himself. In these cases it can be desirable to apply a special power to a person in the (immediate) environment of the target, as a result of which information on the target can be obtained via the non-target. The Committee considers this to be a very far-reaching method and is of the opinion that the AIVD is to be very reticent in employing it. The method is not employed on a large scale and in almost all cases, there is, in the

Committee's opinion, a threat to national security involved such that employment of the method is considered necessary, also because other methods provide an insufficiently clear picture of the target.
The Committee has established a slight increase in the application of Article 25 WIV 2002 against non-targets. The Committee will continue to pay special attention to this method in monitoring the application by the AIVD of the Articles 25 and 27 WIV 2002.

During its investigation the Committee came across two operations in which the application of Article 25 WIV 2002 against non-targets was disproportionate in the Committee's opinion. In both cases the Committee is of the opinion that the importance of investigating a certain target does not outweigh the serious infringement of the rights of the non-targets. Moreover, in one of these operations a holder of confidential information was involved. In section 8 the Committee will discuss the application of special powers to those having a (limited) right to withhold information. Both operations have meanwhile been terminated.

6.3 The reason for which application is requested

The request for permission or extension must also contain the reason for application of the special power in question (Article 25, paragraph 4, sub c, WIV 2002).

The AIVD is to demonstrate that it has become interested in the person or organisation in the context of its A-task or D-task, and that it is necessary to subject him or it to a further investigation. This importance of the investigation is to be weighed against the rights of the person(s) or organisation(s) involved which are violated by applying the special power (proportionality assessment).

As mentioned in the introduction to section 6, after comments made by the Committee the AIVD has to a larger extent fitted its reasoning to the person or organisation involved.
In the Committee's opinion, with the exception of the case that is dealt with in the classified appendix to this report, the reasons stated in the requests show that the AIVD works in a well-considered way in applying this very far-reaching special power. There is no wiretapping at random, as is sometimes thought in circles outside the AIVD. The decision to apply a special power laid down in Article 25 WIV 2002 to a person or an organisation is well-considered. Partly, of course, this has to do with the AIVD's limited capacity, as a result of which the AIVD is unable to make unlimited use of the application of special powers. However the reasons stated in the requests also show that the AIVD is aware that the application of a far-reaching special power is involved, whereby serious infringement is made on human rights and that it is to exercise restraint in applying such a power.

In its request the AIVD is to include an explanation why *this* method is to be employed to collect information. What results does the AIVD intend to obtain by wiretapping a person's telephone, by fixing a microphone in a dwelling or monitoring someone's internet behaviour? Is there no other means of intelligence with which the same result can be achieved whilst making less infringement on the rights of the person(s) involved, in other words: has the requirement of subsidiarity been met?
The result of the application is important in order to determine whether an extension is justified. Each time it needs to be considered whether the result is in proportion to the infringement made on the rights of the person(s) involved. Previously, in its requests for extension the AIVD paid little attention to the actual results achieved. After the Committee had made some comments about this, it has visibly improved. In its requests for extension the AIVD now states what the results have been over the past three months. Because the

AIVD now asks itself the question every three months whether the employed methods (still) contribute to the intended results, it avoids applying a special power over an unnecessarily long period.
It can happen that the application of a certain special power has not led to relevant results over the past three months. Consider for example the situation that a telephone tap on a target intercepts conversations of the target, but the content of the conversations has no (direct) relevance to the investigation. In some cases, because of the importance of monitoring a certain target, the AIVD still asks for extension of application of the special power. The Committee holds the opinion that this is justified if the extension serves to see whether relevant results can indeed be achieved over the next three months. However, if also in this period no progress is made in the investigation, it is generally not justified according to the Committee to extend the application of a special power yet again. The AIVD generally appears to make a careful decision as to whether continued application of Article 25 WIV 2002 is justified in view of the result achieved.

Due to the AIVD's careful deliberation process and its recording thereof in the requests for permission and extension, in only a limited number of cases the Committee has had to ask for more detailed reasons for the application of the special power. In many instances these more detailed reasons gave sufficient clarity as to the legitimacy of the application of the power.

During the investigation the Committee – in addition to the two operations against non-targets referred to previously (see par. 6.2.2, under category III) – came across two operations in which the infringement of the rights of the party involved is/was, in the Committee's opinion, disproportionate to the purpose it serves/served. In both cases the application of Article 25 WIV 2002 in the context of the AIVD's foreign task was involved. One of these operations has meanwhile been terminated, the other operation is still ongoing at the moment of preparing this review report. In the classified part of this review report the operation that is still ongoing is discussed in more detail.

7. Requirements for the request for permission or extension pursuant to Article 27 WIV 2002

Article 27 paragraphs 4 and 5 WIV 2002 provide which information is to be included in a request for permission or extension for selecting undirected intercepted non cable-bound telecommunications.

The first requirement is a designation of the data the AIVD wishes to use to make a selection. This concerns either data regarding the identity of a person or an organisation or the number or a technical feature (Article 27 paragraph 4 sub a) which the AIVD wishes to use to make a selection. If the AIVD wishes to select on the basis of keywords related to a subject, the request is to contain an accurate description of the subject (Article 27 paragraph 5 sub a).

The second requirement is that the request must contain the reason for making the selection (Article 27 paragraph 4 sub b and paragraph 5 sub b). Like in the requests for permission and extension for application of Article 25 WIV 2002 (see section 6), reasons for application of the special power are to be provided by paying attention to the mandate and the requirements of necessity, proportionality and subsidiarity. The requests for extension must also include the results achieved.

The AIVD has structured its requests for permission to select undirected intercepted non cable-bound telecommunications (Article 27) differently from its requests for permission to wiretap (Article 25). For the latter, one individual request is submitted per wiretapped part. For example, if a person's two mobile telephones, his landline and his internet connection are wiretapped, in total four separate requests are submitted.

In requests to select undirected intercepted non cable-bound telecommunications the AIVD does not draw up a separate request for each selection criterion separately. For each investigation the selection criteria are combined in one request. The Committee has no objection against this method if the request sufficiently shows that in respect of each individual selection criterion the statutory requirements have been met. However, in most requests for application of Article 27 WIV 2002 this is insufficiently the case. The AIVD does state its reasons for the investigation (for example the investigation into a subject that has been designated in the Designation Order), but subsequently pays too little attention to the question why the selection has to be made on the basis of the criteria included in the request.

The requests based on Article 27, paragraph 3 sub a and b, WIV 2002 (selection on the basis of identity data or the number of a technical feature) contain many numbers and technical features without it being explained whom or which these relate to. When it is explained to whom or which these relate, often an explanation as to why this person or organisation is to be kept under surveillance in the context of the investigation and reasoning regarding the necessity, proportionality and subsidiarity, is lacking. In these cases the Committee is unable to check whether the selection is justified. Also the internal (legal) control at the AIVD (see section 5), in the Committee's opinion, cannot take place in this way. Even so, the requests are submitted for permission to the Minister of the Interior and Kingdom Relations and the Minister gives permission for selection on the basis of the criteria included in the request.
It was observed during the drafting of the WIV 2002 that for the selection based on the criteria mentioned under a and b, in the government's opinion, the same regime is to be applied as for the application of Article 25 WIV 2002.[51] For in these cases the AIVD makes a directed attempt to take cognisance of the content of the communications of persons and organisations. This infringement therefore requires the stating of reasons specifically relevant to the person or organisation.
In the Committee's opinion the application of this special power, also considering the number of selection criteria used for selection, is currently not handled with due care. Failing to state the reason why the selection is applied based on identity data or numbers or technical features, is not in accordance with the WIV 2002.
As the Committee has insufficient knowledge of the reasons behind the selection, it is unable to render an opinion on the legitimacy of the selection pursuant to Article 27 paragraph 3 sub a and b WIV 2002. The Committee strongly recommends providing the requests for permission or extension for application of this special power with reasons specifically relevant to the selection criteria.

The requests pursuant to Article 27 paragraph 3 sub c WIV 2002 – the selection based on keywords related to a subject– are subject to a different regime. This concerns a different type of infringement because this does not initially concern a directed search action for data relating to a person or an organisation, as a result of which the personal privacy is not directly at stake. In the Explanatory Memorandum to the WIV 2002, it is stated that this concerns data that is generally important for investigations the service is involved in (for example the proliferation of chemical weapons). The Explanatory Memorandum continues:

[51] Parliamentary Documents II 1997/98, 25 877, no. 3, p. 44-45.

> "However once specific persons come into play as a result of such a search action, regarding whom there will be a directed selection, the Head of the service is to submit a request for this as referred to in Article 26, fourth paragraph, [Committee: now Article 27, fourth paragraph]. Incidentally, as to the possibility of selection based on criteria as referred to under c it is observed that this power will be used very selectively (predominantly limited to satellite traffic) and with restraint. Whether this actually happens, will in our opinion be adequately supervised by the independent supervisory committee, as referred to in Article 59 of the legislative proposal [Committee: now Article 64]. For, like the intelligence and security services committee of the Lower House, it is informed of such a selection in great detail pursuant to Article 26, sixth paragraph (Committee: now Article 27, seventh paragraph]." [52]

Considering this observation from the government, the Committee notes that the AIVD – unlike the situation regarding selection based on sub a and b – makes a very cautious selection based on keywords relating to a subject (sub c). The Committee has not established any peculiarities relating to this type of selection.

The Committee has established that application of this relatively new special power (Article 27 paragraph 3 sub a, b and c WIV 2002) is currently still in a state of development. Via projects attempts are made to make a more efficient and effective use of the selection of undirected intercepted non cable-bound telecommunication. Although the application of this special power does not always generate any - or the desired - result, the personal privacy of persons and organisations is violated if, by means of selection, in the undirected intercepted non cable-bound telecommunication information on the person or organisation is found and cognisance is taken of the content of this information. This infringement is intended if the AIVD submits a request for permission to make the selection. Already at that moment the AIVD will therefore have to account for the fact that the selection is justified. The Committee urges the AIVD to pay sufficient attention to this in its requests for permission and extension.

8. Deployment of special powers against those having a (limited) right to withhold information

In two previous review reports the Committee already paid attention to the application of special powers to persons who, pursuant to the law or case law, had a full or limited right to withhold information.[53] Before discussing this in more detail, the most recent (relevant) development concerning the rights of holders of confidential information will be discussed.

On 22 November 2007 the ruling of the European Court of Human Rights was published in the case of Voskuil vs the Netherlands, in which the ECHR ruled that a committal of the journalist Voskuil in 2000 for failure to comply with a judicial order was an unjustified infringement of the freedom of information guaranteed in Article 10 ECHR.[54] In its ruling, the ECHR expressed its astonishment about the far-reaching measures – seventeen days of

---

[52] Parliamentary Documents II 1997/98, 25 877, no. 3, p. 44-45.

[53] '*Toezichtsrapport inzake het onderzoek van de Commissie van Toezicht naar het AIVD-onderzoek naar radicaal dierenrechtactivisme en links-extremisme*' (*Review report on the investigation of the Review Committee into the AIVD investigation into radical animal rights activism and left-wing extremism*), CTIVD no. 6 (2006), p. 5-7 and '*Toezichtsrapport inzake het onderzoek van de AIVD naar het uitlekken van staatsgeheimen*' (*Review report on the AIVD investigation into the leaking of state secrets*), CTIVD no. 10 (2006), p. 10- 14. Both reports can be found on www.ctivd.nl.

[54] ECHR 22 November 2007 (Voskuil/the Netherlands).

commitment for failure to comply with a judicial order – that the authorities in the Netherlands were prepared to take in this case in order to find out the identity of the source of the journalist.[55]
Shortly after the ECHR's ruling the Minister of Justice informed the Lower House (of the States General) that statutory provisions would be prepared stating which persons are eligible to invoke source protection in the interest of freedom of press in a democratic state under the rule of law and in which context an assessment framework vis-à-vis the importance of establishing the truth in criminal cases is provided.[56]
The right to source protection of journalists – like the right to withhold information - is not an absolute right. This was recently reiterated by the Supreme Court in the rulings of 25 March 2008 and 11 July 2008. Both cases involved measures used by the government against two journalists of the Dutch daily newspaper *De Telegraaf*, after they had published two articles in *De Telegraaf* which stated among other things that the daily newspaper had classified documents (state secrets) of the former National Security Service (BVD), now the General Intelligence and Security Service (AIVD) and that these state secret documents would circulate in the criminal circuit. The ruling of the Supreme Court of 25 March 2008 concerns the seizure by the Public Prosecutions Department of the state secret documents from the journalists. The ruling of 11 July 2008 concerns the special powers applied by the AIVD to the journalists. In both rulings the Supreme Court ruled that the right to journalistic source protection is not an absolute right. The protection of journalistic sources is limited, among other things, by the protection of national security and the necessity to impede the dissemination of confidential information, according to the Supreme Court.[57]

In late 2007 the value attached to the lawyer-client privilege came up again in a ruling of the District Court Amsterdam, criminal division. The District Court declared the Public Prosecutions Department inadmissible in the prosecution of a group of members of the Hells Angels MC Holland because of the circumstance that conversations with holders of confidential information, wiretapped in violation of the existing legislation, had not been destroyed.[58] Also in criminal proceedings at the Court of Appeal in The Hague the fact that a wiretapped telephone conversation between a suspect and his lawyer had not been destroyed, was considered to be an irreparable breach of procedural rules.[59]

The developments mentioned above show all the more that the right to withhold information and the journalistic right to source protection are important rights in a democratic society. Infringement of these rights can only be justified if there are compelling reasons to do so.

In previous review reports of the Committee it was already concluded that the rules for the right to withhold information that apply in criminal procedures are not fully applicable to the AIVD. However, the AIVD needs to exercise restraint in applying special powers to those having a (limited) right to withhold information. Insofar as the AIVD applies special powers in these cases, explicit attention needs to be paid to these rights in the reasoning underlying the application of the special power in question. A well-considered answer is to be given to the question whether the application of powers with such a special and infringing nature,

[55] See legal ground 71.
[56] Parliamentary Documents II 2007/08, 31200 VI, no. 92, p. 1.
[57] HR 25 March 2008, LJN number BB2875, legal ground 4.4 and HR 11 July 2008, LJN number BC8421, legal ground 3.7.4.1.
[58] District Court Amsterdam 20 December 2007, LJN number BC0685.
[59] Court of Appeal The Hague 3 April 2007, LJN number BA2127.

meets the statutory requirements set in this context, including necessity, proportionality and subsidiarity.

In the Committee's review report on the AIVD's investigation into the leaking of state secrets (the *De Telegraaf* investigation), the Committee recommended putting more emphasis on the political responsibility of the Minister in these special cases by reducing the (maximum) period for which the Minister gives permission from three months to, for example, one month.[60]
In response to this recommendation of the Committee the AIVD has included in the Handbook AIVD that in the case of holders of confidential information who are regarded as a non-target, the Minister of the Interior and Kingdom Relations' permission is granted for a maximum period of one month. If holders of confidential information are also a target of the AIVD, the period for which permission is granted is decided on a case-by-case basis. In the recently issued review report on compliance with the recommendations made by the Committee in its previous review reports, the Committee held the opinion that no distinction is to be made between targets and non-targets.[61] In both cases an infringement of special rights is involved; rights which mainly serve the interest of the persons with whom those having a (limited) right to withhold information come into contact (patients, sources, clients, et cetera). The question whether the person having a (limited) right to withhold information is himself a target or a non-target, is therefore of lesser importance. Both in the case of targets and of non-targets, restraint is to be exercised in applying special powers to this special group, for which reason it is recommended to involve the Minister more frequently in both cases. In her response to the review report to the Lower House, the Minister of the Interior and Kingdom Relations reported that she considered it in particular important that

> "where holders of confidential information are concerned, when deciding whether special powers are to be applied to these persons, stricter criteria are to be used and that the decision-making process and conclusions to be attached are specified (in even greater detail than is customary) and furthermore that in such cases this is explicitly pointed out to the Minister."[62]

The Minister adds to this that in response to the Committee's observations she has decided to apply a shorter period for which permission is given to all holders of confidential information, both targets and non-targets. The Handbook AIVD will be adjusted on this point.

In the weighing of interests to decide whether applying the special power to a holder of confidential information is justified, the question whether this person is a target or a non-target is of course relevant. In its report on the *De Telegraaf* investigation, the Committee noted the following about this:

> "The important question is whether the person in question is a target of the AIVD, or a so-called non-target. If the person involved is a target, the AIVD basically has more liberty to apply special powers. The special decision-making process that must always be followed in

---

[60] '*Toezichtsrapport inzake het onderzoek van de AIVD naar het uitlekken van staatsgeheimen*' (*Review report on the AIVD investigation into the leaking of state secrets*), CTIVD no. 10 (2006), p. 14, www.ctivd.nl.
[61] '*Toezichtsrapport inzake het onderzoek naar de nakoming door de AIVD van de toezeggingen van de Minister van BZK op de aanbevelingen van de Commissie*' (*Review report on the implementation by the AIVD of the promises given by the Minister of the Interior and Kingdom Relations in relation to the Committee's recommendations*), CTIVD no. 18A (2008), p. 8, www.ctivd.nl.
[62] Parliamentary Documents II 2007/08, 29 924, no. 25, p. 3.

applying special powers to the groups of persons referred to, is even more important if the special powers are applied to a non-target."[63]

If a person with a (limited) right to withhold information because of the objectives he pursues or his activities gives rise to the serious suspicion that he poses a danger to the continued existence of the democratic legal order, or to the security or other vital interests of the state (Article 6 paragraph 2 sub a WIV 2002) and if therefore this person can be considered as a target by the AIVD, there exists a major interest to monitor this person. The right to withhold information does not have to stand in the way of an investigation by the AIVD. Obviously, in applying special powers all statutory requirements have to be met including the requirements of necessity, proportionality and subsidiarity, in which context the fact that a holder of confidential information is involved is an aggravating circumstance in the legitimacy test.
A parallel can be made with criminal procedure, in which context the rights of a holder of confidential information can be restricted if very exceptional circumstances are involved, for example if the holder of confidential information himself is regarded as a suspect of a *serious criminal act*, as a result of which the importance that the truth is uncovered prevails over the right to withhold information.[64] The Committee holds the opinion that the importance of conducting an investigation into threats to national security can be equally important as the importance of conducting an investigation into serious criminal acts.

If the person having a (limited) right to withhold information is not a target of the AIVD and therefore a non-target, in principle the Committee considers apllication of a special power to this person unacceptable. The threat to national security in such cases does not come from the person having a (limited) right to withhold information, but the AIVD would like to obtain information about a target via this person. The application of special powers to non-targets is already subject to a strict test, because the rights of persons who themselves do not pose a threat to national security are infringed. Moreover, if the non-target has a (limited) right to withhold information, an infringement on his rights is hardly ever justified. For the moment the Committee can only think of one situation in which this exceptionally severe infringement is acceptable, namely if there are indications that a threat to national security by violent action(s) will manifest itself in the short term and the information needed for the investigation can only be obtained by applying a special power to a person having a (limited) right to withhold information.
The Committee is of the opinion that in one instance the application of a special power laid down in Article 25 WIV 2002 against a holder of confidential information also being a non-target did not meet the statutory requirements of necessity, proportionality and subsidiarity (see also section 6.2.2, under category III). Via the wiretapped person the AIVD attempted to obtain information on a target of the AIVD. Although the AIVD was very cautious in the handling of data collected via application of the special power, the Committee holds the opinion that the threat posed by the target at that moment was not sufficiently specific to justify the use of this far-reaching method of obtaining information.

---

[63] '*Review Report inzake het onderzoek van the AIVD naar het uitlekken van staatsgeheimen*' (*Review report on the AIVD investigation into the leaking of state secrets*), CTIVD-no. 10 (2006), p. 13, www.ctivd.nl.
[64] See for example HR 30 November 1999, NJ 2002/438. For a comparison see also the Public Prosecution Department's policy rules on this point: the '*Aanwijzing toepassing opsporingsbevoegdheden en dwangmiddelen tegen advocaten*' (Designation deployment of investigative powers and coercive measures towards lawyers) and the '*Aanwijzing toepassing dwangmiddelen bij journalisten*' (Designation deployment of coercive measures against journalists), which can be consulted via www.om.nl.

The requirement of subsidiarity deserves special attention in the application of special powers to those who have a (limited) right to withhold information. The AIVD is to make as small an infringement as possible on the interests protected by the right to withhold information. If, for example, a lawyer or physician is wiretapped by the AIVD, the AIVD is in principle not permitted to process the wiretapped communication with clients or patients. Processing these confidential conversations is only permitted if this is strictly necessary for the AIVD's performance of its tasks. The details of confidential conversations may not be passed on to third parties, unless in exceptional situations due to which the interest of free communication with a holder of confidential information must make way for the interest of protecting society. Consider for example a situation in which during a conversation with a confidential advisor specific information on an imminent attack emerges. It is evident that such information will be shared with the Public Prosecutions Department by means of an official message. The Committee is currently conducting a follow-up investigation into the AIVD's official messages.[65] In this investigation the Committee will in particular monitor the use (if any) of this special information.

The Committee observes that it is not always clear whether a person has a (limited) right to withhold information. Generally known are the so-called classic holders of confidential information: lawyers, physicians, clergymen, civil-law notaries. Pursuant to ECHR case law the journalist has a so-called limited right to withhold information, namely insofar as this concerns the right of a journalist to protect his sources from publication.
Regarding other job categories and regarding persons with a secondary right to withhold information, the answers given to this question in the case- aw are generally case-specific. This makes it difficult to give general rules.
As to several of the acknowledged groups of holders of confidential information, the question can be asked when a person can be considered as belonging to one of these groups. In the *De Telegraaf* investigation the Committee has expressed itself as regards the journalistic right to source protection:

> "The Committee observes that the journalistic profession does not have a closed nature. Unlike several of the classic holders of confidential information – for example the lawyer or the civil-law notary – there are no requirements for entering the journalistic profession. Therefore, in principle, anyone can call himself a journalist. This makes this profession, from a legal point of view, a diffuse group. In some cases this can make it difficult to assess whether the journalistic source protection right is at stake. A case-specific approach is called for here, whereby it is to be assessed in each case individually whether the journalistic right to source protection is applicable."[66]

Like journalists, clergymen, too, are not a clearly defined profession. There are many religious convictions in the Netherlands and within these convictions various movements can be distinguished. Each one has its own officiating minister who is chosen in different ways and may perform different tasks per religious conviction. The Committee believes it would take things too far to grant each person who considers himself a clergyman a right to withhold information. Whether a person can invoke a right to withhold information will have to be decided in each case individually. Indications in this context can be, according to

---

[65] This investigation is the continuation of the investigation on which the Committee has reported in the '*Toezichtsrapport inzake de door de AIVD uitgebrachte ambtsberichten in de periode van januari 2004 tot oktober 2005*' (*Review report on the official messages issued by the AIVD in the period from January 2004 to October 2005*), CTIVD no. 9a (2006), www.ctivd.nl.
[66] '*Toezichtsrapport inzake het onderzoek van de AIVD naar het uitlekken van staatsgeheimen*' (*Review report on the AIVD investigation into the leaking of state secrets*), CTIVD no. 10 (2006), www.ctivd.nl, p. 12.

the Committee, whether the person is a clergyman of a generally acknowledged religion, whether the person has become an officiating minister in a way that is customary for the religion in question (for example by attending certain training programmes) and whether his job as a clergyman (also) entails that he acts as a confidential counsellor for the followers of this religion.

The Committee has concluded that the AIVD only applies the special powers mentioned in the Articles 25 and 27 WIV 2002 to those who have a (limited) right to withhold information in exceptional cases. The AIVD is very aware that this is a very far-reaching method of obtaining information. In the Committee's opinion, it is right that this investigative method is rarely employed. The Committee recommends that the AIVD continue this level of restraint.

Possibly unnecessarily the Committee observes that it has not performed any investigation into the details of conversations that wiretapped targets (not being holders of confidential information) conduct for example with their lawyer, civil-law notary or GP. If, in the course of one of its investigations, the Committee comes across such details, it will carefully check whether all statutory requirements have been complied with.[67]

9. Removal and destruction of unlawfully processed data

The Committee observes that Article 43 paragraphs 2 and 3 WIV 2002 provide that if the conclusion is reached that certain data is incorrect or has been unlawfully processed, this data will be corrected or removed, respectively. The relevant Minister is to inform the person or persons to whom the data was provided of this as soon as possible. The removed data is destroyed, unless statutory provisions on storage dictate otherwise.
The Committee recommends that the AIVD apply Article 43 paragraphs 2 and 3 WIV 2002 to the data regarding which the Committee has judged, in the present report (including the classified appendix), that it has been unlawfully processed.

As regards the text messages intercepted in the course of the application of a silent tap, as described in section 2.3 of this report, the Committee considers it disproportionate for the AIVD to be obligated to trace, remove and destroy the text messages. Therefore the text messages intercepted before the date of adoption of this report do not need to be removed and destroyed.

The Committee has included in this report a highly secret classified list in which the Committee has designated which data is to be removed and destroyed.

10. Conclusions and recommendations

1. A silent tap is in effect a telephone tap, the difference being that the sound signal in a silent tap is not provided to the AIVD. Via a silent tap the AIVD can get *current* telephone traffic data. According to the AIVD, a silent tap can be applied pursuant to Article 28 WIV 2002, for which no permission from the Minister of the Interior and Kingdom Relations (BZK) is required.

[67] For example in the pending, continued investigation of the Committee into the official messages of the AIVD.

The Committee has established that in several silent taps applied by the AIVD cognisance is taken of the content of (a form of) telecommunication, as text messages do reach the AIVD via the silent tap.
In the Committee's opinion, as the AIVD indicates that it is not possible technically to avoid text messages being sent along with a silent tap and therefore a silent tap involves taking cognisance of the content of communications, the silent tap falls under the description of Article 25 paragraph 1 WIV 2002, namely under 'any form of telecommunication'. The Committee therefore strongly recommends that for a silent tap the AIVD asks the Minister of the Interior and Kingdom Relations for permission in the way prescribed by Article 25 WIV 2002. (section 2.3)

2. Before the AIVD has a serious suspicion that a person or an organisation poses a danger to national security, it can already perform exploratory activities.
In what operational way the exploratory activities can be developed has not been described in more detail in the legislative history. In the Committee's opinion exploratory activities in the context of performing the A-task at any rate cannot involve the application of special powers, such as wiretapping (Article 25 WIV 2002) and the selection of undirected intercepted non cable-bound telecommunication (Article 27 WIV 2002).
In its present investigation the Committee has established that for the performance of its A-task the AIVD does not perform any exploratory activities by means of the application of the special powers mentioned in the Articles 25 and 27 WIV 2002. (section 3.1)

3. The Committee has established that the AIVD – in accordance with the law – does not apply the special powers of the Articles 25 and 27 WIV 2002 in the performance of the B-task, C-task and E-task mentioned in Article 6 paragraph 2.
Both for the A-task and the D-task the AIVD applies the special powers mentioned in the Articles 25 and 27 WIV 2002. The investigations for which these special powers are applied fall under the task description of the AIVD. (section 3.4)

4. Before the AIVD's executive level submits a request to the Minister of the Interior and Kingdom Relations for permission to apply a special power or to extend the application of a special power, the request is passed through the service for an assessment of its (legal) tenability.
The Committee has established that this internal assessment contributes to a more careful deliberation process within the AIVD. Often the team involved is required to state further reasons for the request before it is approved, and sometimes the request is denied and does not even reach the Minister. (section 5)

5. The Committee has established that in practice almost all requests for permission are for the maximum period. Also when the permission has been granted for the maximum period of three months, the AIVD must constantly ask itself whether application of the special power is still justified.
Based on the phrasing chosen by the AIVD in its requests for permission or extension, the Committee has established that the AIVD is aware that the application of a special power is to be stopped if there is no longer any basis for it. That the AIVD indeed acts upon this, has also become apparent from the reasoning in decisions to terminate the application of a special power, which have given the Committee insight into the reasons given by the AIVD for discontinuing this application. (section 5)

6. Based on Article 25 paragraph 5 WIV 2002 the AIVD, in the context of the "three-monthly collective decision", simultaneously requests the Minister of the Interior and Kingdom Relations for permission, in respect of all persons and organisations that are wiretapped, to also perform the power with respect to any newly disclosed telecommunication characteristics of the persons and organisations that are wiretapped.
Based on Article 25 paragraph 5 WIV 2002 the Committee considers it permissible if the AIVD decides to wiretap a newly disclosed (mobile) telephone number of a target or another number in the sense of Article 1.1 under bb of the Telecommunications Act, in between two three-monthly collective decisions if the Minister of the Interior and Kingdom Relations has already given permission to wiretap one telephone number of the target.
The Committee has established that a mid-term extension of the application of the special power to new telecommunication characteristics is often performed. The Committee has no objections against this, provided the AIVD ensures that the extension pertains to the same type of special power for which the Minister has granted permission. (section 6.1)

7. The Committee has established that in one instance the AIVD stretched the general permission of the Minister of the Interior and Kingdom Relations to extend the power to other numbers of the person involved (pursuant to Article 25 paragraph 5 WIV 2002) too far. (section 6.1)

8. Article 25 paragraph 6 WIV 2002 offers the possibility to supplement the data concerning the identity of an *organisation* in the request for permission or extension for application of the special power at a later stage. The Committee has established that the AIVD also includes in this identity data the names of the members of the organisation. If, after having been given permission to wiretap an organisation, the AIVD identifies a new member of the organisation who meets the criteria in the organisation request, and the AIVD wishes to wiretap this person, the AIVD will proceed to do this without separately asking prior permission from the Minister of the Interior and Kingdom Relations for this individual.
In the Committee's opinion, it is better to ask for separate permission for each individual to whom the AIVD wishes to apply this far-reaching special power, in order that a careful assessment can be made as to whether all statutory requirements have been met. The Committee has however established that Article 25 paragraph 6 WIV 2002 indeed allows the AIVD room to independently wiretap newly disclosed members of the organisations in the interim.
The Committee recommends that in organisation requests the AIVD carefully describe why an organisation is involved, which category of persons from the organisation can be wiretapped and why the statutory requirements of necessity, proportionality and subsidiarity to wiretap this category of persons from the organisation, have been met.
If in the interim a newly disclosed person is wiretapped, it is important to record why, in the AIVD's opinion, this person falls under the category of persons stated in the organisation request. The Committee considers it positive that the internal guidelines include the requirement that the Legal Affairs Cabinet gives permission to also wiretap new individuals, so that a legal assessment is made internally with regard to this individual, in particular by assessing whether the person involved meets the criteria stated in the organisation request.

The Committee has established that in one case the AIVD did not formulate a clear organisation request, while it had already started wiretapping a newly disclosed member of the organisation. The Committee considers this careless, and recommends that the AIVD draw up a clear organisation request each time the service wishes to wiretap a group of persons as an organisation. (section 6.2.1)

9. The AIVD can apply a special power against a person in the (immediate) environment of the target, in order to obtain information on the target via this person (the non-target). The Committee considers this to be a very far-reaching method and is of the opinion that the AIVD is to be very reticent in employing it. The method is not applied on a large scale and in almost all cases, there is, in the Committee's opinion, a threat to national security involved such that employment of this method is considered necessary, also because other methods provide an insufficiently clear picture of the target.
The Committee has established a slight increase in the application of Article 25 WIV 2002 against non-targets. The Committee will continue to pay special attention to this method in monitoring the application by the AIVD of the Articles 25 and 27 WIV 2002.
During its investigation the Committee has come across two operations regarding which the application of Article 25 WIV 2002 against non-targets was disproportionate in the Committee's opinion. In both cases the Committee is of the opinion that the importance of investigating the subject in question does not outweigh the serious infringement of the rights of the non-targets. Moreover, in one of these operations a holder of confidential information was involved. (section 6.2.2)

10. In the Committee's opinion the reasons stated in the requests show that the AIVD works in a well-considered way in applying Article 25 WIV 2002 (wiretapping). There is no wiretapping at random, as is sometimes thought in circles outside the AIVD. The decision to apply a special power laid down in Article 25 WIV 2002 against a person or an organisation is well-considered. Partly, of course, this has to do with the AIVD's limited capacity, as a result of which the AIVD is unable to make unlimited use of the application of special powers. However, the reasons stated in the requests also show that the AIVD is aware that the application of a far-reaching special power is involved, whereby serious infringement is made on human rights and that it is to exercise restraint in using it. (section 6.3)

11. The Committee holds the opinion that it is justified to extend the application of a special power despite the lack of a (relevant) result over the past period, if the extension serves to examine whether a relevant result can be achieved in the next three months. However, if also in this period no progress is made in the investigation, it is generally not justified, according to the Committee, to extend the application of the special power yet again. The AIVD has generally appeared to make a careful decision as to whether continued application of Article 25 WIV 2002 is justified in view of the result achieved. (section 6.3)

12. During the investigation the Committee – in addition to the two operations against non-targets referred to previously under point 9 – came across two operations in which the infringement of the rights of the party involved is/was, in the Committee's opinion, disproportionate to the purpose it serves/served. (section 6.3)

13. The requests pursuant to Article 27 paragraph 3 sub a and b WIV 2002 (selection based on identity data or the number or a technical feature) contain many numbers and technical features without it being explained to whom or which these refer. When this is explained, often an explanation is lacking as to why the person or organisation is to be kept under surveillance in the context of the investigation (objective) and also, in such cases, a reasoning regarding the necessity, proportionality and subsidiarity requirements is often lacking.
The Committee holds the opinion that currently, also in view of the number of selection criteria on which a selection is based, the application of this special power is not handled with due care. Not stating the reason why the selection is used on the basis of identity data or numbers or technical features, is not in accordance with the WIV 2002.
As the Committee is insufficiently aware of the reasons for making the selection, the Committee is unable to render an opinion on the legitimacy of the selection based on Article 27 paragraph 3 sub a and b WIV 2002. The Committee strongly recommends providing the requests for permission or extension of application of this special power with reasons specifically relevant to one of the selection criteria. (section 7)

14. Unlike the selection pursuant to Article 27 paragraph 3 sub a and b WIV 2002 (selection based on identity data or the number or a technical feature) the AIVD adopts a very reticent attitude in selecting on the basis of keywords relating to a subject (Article 27 paragraph 3 sub c WIV 2002). The Committee has not established any peculiarities with regard to this form of selection. (section 7)

15. The Committee has concluded that the AIVD only applies the special powers referred to in the Articles 25 and 27 WIV 2002 to those who have a (limited) right to withhold confidential information in exceptional circumstances. The AIVD is very much aware that this is a far-reaching method of obtaining information. In the Committee's opinion it is right that this investigative method is seldom used. The Committee recommends that the AIVD continue this level of restraint. (section 8)

16. In the Committee's opinion the application of a special power laid down in Article 25 WIV 2002 to a holder of confidential information who was also a non-target did not meet the statutory requirements of necessity, proportionality and subsidiarity in one instance (see also under point 9). Via the wiretapped person, the AIVD attempted to obtain information about a target of the AIVD. Although the AIVD showed restraint in handling the data obtained via application of the special power, in the Committee's opinion the threat posed by the target at that moment was not sufficiently specific to justify the application of this far-reaching special power. (section 8)

17. The Committee recommends that the AIVD implement Article 43 paragraphs 2 and 3 WIV 2002 – the removal and destruction of unlawfully processed data – with regard to the data which, the Committee has concluded in this report (including the classified appendix), was unlawfully processed. (section 9)

Adopted at the meeting of the Committee of 7 January 2009.