Review Report

on the exchange of unevaluated data by the AIVD and the MIVD

investigation into the execution of Dutch House of Representatives motion no. 96 (by member Schouw)

CTIVD no. 49

04 May 2016

CTIVD

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence and Security Services

CTIVD no. 49

REVIEW REPORT

on the exchange of unevaluated data
by the AIVD and the MIVD

investigation into the execution of Dutch House of Representatives motion no. 96
(by member Schouw)

Table of contents

CTIVD no. 49

SUMMARY

of the review report on the exchange of unevaluated data by the AIVD and the MIVD

investigation into the execution of Dutch House of Representatives motion no. 96 (by member Schouw)

Motion no. 96 by member Schouw

On 9 April 2014, the Dutch House of Representatives held a debate on interception by the NSA and the role of the Netherlands in this activity. During and after the debate, various motions were submitted, including motion no. 96 by member Schouw (D66). The aim of this motion was to generate additional transparency and safeguards in the exchange of (meta)data with foreign intelligence and security services. In response to this motion, the Minister of the Interior and Kingdom Relations and the Minister of Defence indicated that, from now on, as also requested by the House of Representatives, they will give authorisation for this exchange. The procedures of the AIVD and MIVD have been duly modified. The CTIVD was requested to oversee execution of the motion.

Definition of terms

The CTIVD explains the term "(meta)data", as used in motion no. 96, as unevaluated data, in other words data that has not (yet) been assessed for relevance to the performance of the tasks of the AIVD or MIVD. This often refers to a larger volume of data (also known as "bulk"). "Exchanging" is understood by the CTIVD to mean both providing and receiving data.

The CTIVD investigation

In this report, the CTIVD assesses how the AIVD and MIVD, in their policies and in practice, implement the authorisation system for the exchange of unevaluated data with foreign intelligence and security services. The CTIVD has drawn conclusions concerning policy and practice in the light of the facts established. It is up to the Dutch House of Representatives to assess whether motion no. 96 by member Schouw has been adequately implemented.

Safeguards in the exchange of unevaluated data

The present law does not include firm rules for the provision of unevaluated data to foreign services. The promised ministerial authorisation system intends to provide stricter data protection. In implementing this authorisation system, the following points are important for the protection of privacy:

- Justified trust: foreign services must qualify for this form of cooperation. The level of this trust is assessed for each individual service based on cooperation criteria. The Minister evaluates whether the assessment defined in the "weighting note" is justified;
- Assessment in the specific case: the Minister assesses whether the exchange of unevaluated data is allowed based on justification which focuses on the foreign service and on that specific exchange. A two-fold assessment therefore takes place.

Conclusions concerning policy

Neither the AIVD nor the MIVD has established a written policy concerning what must be understood by unevaluated data and under what circumstances, how and when authorisation must be obtained from the Minister.

Conclusions concerning practice: web forums

In practice, it is evident that the AIVD does not regard web forums as unevaluated data. The AIVD has exchanged some web forums with foreign intelligence and security services without ministerial authorisation. The CTIVD finds that web forums, barring exceptional circumstances, must be regarded as unevaluated data. Generally speaking, therefore, the authorisation of the Minister is needed for the exchange of web forums. Special circumstances can be said to exist if the AIVD can provide supporting facts to show that a web forum is only being used to communicate regarding matters that relate to the AIVD's ongoing investigations. The decision not to request authorisation from the Minister and its basis in fact must then be established for each instance of provision, so that it can be assessed.

Conclusions concerning practice: cooperative partnerships

The AIVD and MIVD exchange unevaluated data on a structural basis with foreign intelligence and security services within five topically or geographically oriented cooperative partnerships. The Ministers in question have authorised this, albeit for an indefinite period. The CTIVD finds it important, for the protection of privacy, that this authorisation from the Ministers be linked to a specific period, for example one year. The services must also keep a clear record of which data (files) are being exchanged as part of the cooperative partnerships.

Conclusions concerning practice: assistance through selection

By selecting and providing unevaluated data, the MIVD provides structural assistance to some foreign services. The foreign services supply lists of selectors, for example telephone numbers. Based on these lists, the MIVD selects and provides data from its archive of telecommunication gathered through untargeted acquisition. Authorisation for this procedure is periodically requested from the Minister of Defence. The MIVD has made efforts to gain a clearer picture of the background to the needs of the foreign services in question. As a result, the MIVD has been in a position to better substantiate the requests for authorisation made to the Minister of Defence.

Conclusions concerning practice: data received

The AIVD and MIVD receive unevaluated data on a structural basis, including in the context of the topically or geographically oriented cooperative partnerships. When receiving this unevaluated data, both services comply with the same procedures as apply (legally) when they gather data themselves. In this way, privacy is similarly protected.

Review Committee
on the Intelligence and Security Services

CTIVD no. 49

REVIEW REPORT

**on the exchange of unevaluated data
by the AIVD and the MIVD**

**investigation into the execution of Dutch House of Representatives motion no. 96
(by member Schouw)**

1 Introduction

Background to the investigation

On 9 April 2014 the Dutch House of Representatives held a debate on interception by the NSA and the role of the Netherlands in this activity.[1] During and after the debate, various motions were submitted, including motion no. 96 by member Schouw (D66).[2] The motion reads as follows:

> "The House
>
> having heard the deliberations,
>
> noting that the Dutch intelligence and security services exchange sets of metadata with some foreign services on a structural basis;
>
> noting that the framework within which this takes place is not transparent;
>
> considering that, for the protection of Dutch personal data, it is very important that information only be shared after prior assessment and within the context of clear frameworks;
>
> considering that ECHR safeguards must be met for all the transactions and actions of the Dutch intelligence and security services;
>
> requests the government only to allow the Dutch intelligence and security services to exchange (meta)data with foreign services after having obtained authorisation from the relevant Minister in advance;
>
> furthermore requests the CTIVD, in its annual report on the intelligence and security services, to examine the execution of this motion;
>
> and proceeds to the order of the day.

1 *Proceedings II* 2013/14, no. 73, item 8.

2 *Parliamentary Documents II* 2013/14, 30 977, no. 96.

Schouw"

In a letter to the Dutch House of Representatives dated 30 June 2014, the Minister of the Interior and Kingdom Relations, partly on behalf of the Minister of Defence, discusses this motion further.[3] The Minister refers to his promise, made during the debate of 9 April 2014 that, from now on, authorisation from the Minister is required in order to share bulk (meta)data. To this end, the procedures of the AIVD and MIVD have been modified, according to the Minister. On 18 May 2014, motion no. 96 was forwarded by the Minister of the Interior and Kingdom Relations to the CTIVD, with the request to implement it and to duly inform the House of Representatives.

Investigative question

The investigative question answered by the CTIVD in this report is: **In their policies and in practice, how do the AIVD and the MIVD implement the authorisation system for the exchange of (meta) data with foreign services?** The CTIVD has drawn conclusions concerning policy and practice in the light of the facts established. It is up to the Dutch House of Representatives to assess whether motion no. 96 has been adequately implemented.

(Meta)data

In this review report, the CTIVD does not use the term (meta)data, as defined in motion no. 96. It also does not use the term "bulk", which is used by the Minister of the Interior and Kingdom Relations. It prefers to use the term "unevaluated data", which is also chosen in the ISS 20XX Act Draft Bill. This refers to all data – both metadata and content-data and both targeted and untargeted acquisition of data – that have not yet been assessed for relevance to the performance of tasks. This is the key to the decision to subject the transfer of data to ministerial authorisation. When providing unevaluated data to foreign services, the AIVD or MIVD does not know exactly what data is being provided. The term "unevaluated data" also includes an element of volume. When one or a few items of data are provided, these quickly can no longer be described as unevaluated data. After all, it quickly becomes clear what the relevance of the data is for the performance of tasks. The CTIVD therefore classifies the exchange of (meta)data as the sharing of **unevaluated data** with foreign services. This often refers to a larger volume of data (also known as "bulk").

Exchange

In motion no. 96, the term "exchanging" is used. In his statements to the House of Representatives, the Minister used the terms "exchanging", "sharing" and "providing" data interchangeably. The CTIVD understands the exchanging or sharing of data to mean both **providing** and **receiving** data. Under motion no. 96, the authorisation of the Minister is required for both directions. The CTIVD notes that the way in which the data is provided or received in that context makes little difference from a legal perspective. We can think here of the exchange of data using a data carrier, the (digital) sharing of data via a secure connection or making data available on a shared network.

Structure of the report

The review report has the following structure. Chapter 2 discusses the investigation plan, the methodology and the timeline. Chapter 3 deals with the legal framework applicable to the exchange of unevaluated data with foreign services. Chapter 4 covers the policies within the AIVD and the MIVD with respect to the exchange of unevaluated data with foreign services. Chapters 5 and 6 describe the practices of the AIVD and MIVD identified by the CTIVD. In Chapter 7, the CTIVD looks at the contents of the ministerial authorisation requirement. Chapter 8 presents the conclusions reached by the CTIVD. Together with the summary, the conclusions contain the key points of this review report.

The report has **no secret appendix**.

---

[3] *Parliamentary Documents II* 2013/14, 30 977, no. 104, p. 2-3.

2. Investigation plan, methodology and timeline

Previous investigation into the provision of data to foreign services

The provision of data to foreign intelligence and security services has repeatedly been discussed in the oversight practice of the CTIVD.[4] As a result, the CTIVD has a clear picture of the procedures of the AIVD and MIVD in this field, the extent to which the services have acted within the current framework of powers and the existing bottlenecks. In this investigation, the CTIVD has been able to build on its previous findings from other investigations.

Scope of this investigation

In this investigation, the CTIVD looked at the way in which the ministerial authorisation requirement for the exchange of unevaluated data with foreign services, as expressed in motion no. 96, is set forth in the internal policies of the AIVD and MIVD. The investigation also focused on the application of the authorisation system in practice. To this end, the CTIVD investigated the cases of unevaluated data exchange with foreign services, since the adoption of motion no. 96, in which authorisation was requested of and obtained from the Minister of the Interior and Kingdom Affairs or the Minister of Defence and the cases in which this did not take place.

Investigative proceedings

The CTIVD studied the verbatim report of the Dutch House of Representatives' debate of 9 April 2014 on interception by the NSA and the role of the Netherlands in this activity, which led to the adoption of motion no. 96. The CTIVD requested files from the AIVD and MIVD. It asked the services to submit the cases in which unevaluated data has been exchanged with foreign intelligence and security services and the cases in which authorisation from the Minister has been obtained for that activity since motion no. 96 was adopted on 15 April 2014. The CTIVD also conducted searches in the services' systems. It investigated by way of a random sample whether, with the exception of the documents submitted, any exchange of data had taken place with foreign services. This investigation also took the findings from previous investigations, including the investigative activities of the AIVD on social media, in account. In addition to the file investigation, the CTIVD held interviews with the Director-General of the AIVD, with a staff member of the Joint Sigint Cyber Unit (JSCU) and with lawyers from the AIVD and MIVD. Written questions were also asked, to which the AIVD and MIVD responded in writing.

Timeline of the investigation

On 2 July 2015, the CTIVD announced the investigation to the Minister of the Interior and Kingdom Relations and the Minister of Defence and to the presidents of the Senate and the House of Representatives of the States General. The investigation concluded with the drafting of the report on 11 February 2016. The Minister of the Interior and Kingdom Relations and the Minister of Defence, in accordance with Article 79 ISS Act 2002, were given the opportunity to respond to the findings presented in the review report. The Minister of Defence indicated that she had no comments concerning the report. The response from the Minister of the Interior and Kingdom Relations was received on 15 April 2016. This response led the CTIVD to make some additions or clarifications to the report. The review report was adopted on 4 May 2016.

---

[4] CTIVD Review Report no. 22a on the cooperation by GISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2009/10, 29 924, no. 39 (appendix), available at www.ctivd.nl, section 7; CTIVD Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, section 6; CTIVD Review Report no. 28 on the use of Sigint by DISS, *Parliamentary Documents II* 2011/12, 29 924, no. 74 (appendix), available at www.ctivd.nl, section 9.3; CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, sections 5.4-5.6; CTIVD Review Report no. 39 on investigative activities of GISS on social media, *Parliamentary Documents II* 2013/14, 29 924, no. 114 (appendix), available at www.ctivd.nl, section 5.5.

3 The assessment framework

3.1 Exchange of unevaluated data in the ISS Act 2002

General frameworks for data processing and cooperation in the ISS Act 2002

The ISS Act 2002 does not include **any specific provision** for the provision of unevaluated data to foreign intelligence and security services, nor does the Act explicitly regulate the process of making a request to receive unevaluated data from a foreign service. This does not mean that the exchange of unevaluated data with foreign services is not subject to certain rules. The Act provides a **general framework for the processing of data** (Article 12 ISS Act 2002). For instance, the processing of the data must have a particular aim, must be necessary and must be carried out properly and with due care. This framework also applies here. It ensures that the AIVD and MIVD must consider, in each case, whether requesting data from or providing data to the foreign service in question is permitted in that case.

In addition, the Act includes some **provisions for cooperation with foreign intelligence and security services,** such as the requirement to assess whether a foreign service qualifies for cooperation and which forms of cooperation are permitted. The Act makes a distinction between forms of cooperation that take place in the context of the performance of the AIVD's and MIVD's tasks and forms of cooperation that take place in the interests of the relevant foreign service. When the interests of the foreign service are decisive, the Act imposes additional requirements. It is then necessary to assess whether the interests of the foreign service are compatible with the interests protected by the Dutch service and whether the proper performance of tasks by the Dutch service does not stand in the way of the cooperation.

The legal framework for cooperation with foreign services, including data exchange, has been discussed in various CTIVD review reports. Here, it suffices for the CTIVD to refer to the legal appendix to review report no. 22b on the cooperation of the MIVD with foreign services[5] and the legal framework of review report no. 38 on the processing of telecommunications data by GISS (AIVD) and DISS (MIVD)[6]. The assessments that play a role in the exchange of unevaluated data are examined below. The following section takes a look at the way in which the CTIVD, in its oversight practice, has implemented the generally applicable frameworks.

Assessments in the exchange of unevaluated data

Although the general framework for data processing in the ISS Act 2002 also applies to the exchange of unevaluated data, the assessments involved are not always easy to make. This is a result of the nature of the data exchange. Larger volumes of data are often involved in the exchange of unevaluated data. A particular aspect of unevaluated data is that it has **not yet been assessed for relevance** to the performance of the tasks of the services. This implies a risk that sensitive data is being provided, such as personal data, that is of no relevance to the performance of tasks. This data is then provided without this being in the interest of national security. Moreover, this implies that the assessments that have to be made on the basis of the ISS Act 2002 cannot be of the same depth as in the case of the exchange of evaluated data.

---

[5] CTIVD Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, legal appendix.

[6] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, p. 44 ff. legal appendix.

When providing unevaluated data to foreign intelligence and security services, it is difficult to make a firm assessment of whether the provision of that data is necessary in order to achieve the intended goal. After all, it is **not known exactly what data** is being provided. Moreover, the **intended goal is often general in nature**, even when this provision takes place in the context of the performance of the service's own tasks (Article 36 ISS Act 2002). The intention of the provision, for example, is to contribute to (part of) the counter-terrorism investigation of the service. Provision is often not aimed at processing data about a specific person or organisation. It is therefore only possible to a limited extent to weigh up the specific interests of the service, in the provision of data, against the potential infringement of privacy caused by the provision of data. When unevaluated data is provided in the interest of the foreign service (Article 59 ISS Act 2002), the provision of data is often aimed at a general goal. This is because the foreign service does not usually provide insight into the specific interests behind this request. The law provides for an additional test that has to take place before the data is provided in the interests of the foreign service. This refers to the assessment of whether the interests of the foreign service are compatible with the interests protected by the Dutch service and the proper performance of tasks by the Dutch service is not in conflict with the provision of the data (Article 59 (2) and (4) ISS Act 2002).[7]

When unevaluated data is received from foreign intelligence and security services, the question also arises of whether adequate safeguards are present for the protection of privacy. When the AIVD and MIVD use investigatory powers to collect data, for example by hacking a web forum[8] or selecting satellite communication[9], authorisation to do so must be obtained from the Minister. Reasons also have to be given to support the request for authorisation. These reasons must show why the deployment of the power is deemed necessary for the performance of the service's tasks, why it is deemed to be reasonably proportionate to the privacy infringement being made in this respect (proportionality) and that it is not possible to achieve the investigative goal by any less intrusive means (subsidiarity). The same test is required when the AIVD and MIVD receive unevaluated data from foreign services. However, this is implicit. The law implies that the assessment must be made. The law does not require that the reasons for receiving unevaluated data be written down and submitted to the Minister, who may or may not grant authorisation for receiving and using the data.[10]

The safeguard for the protection of privacy is found in the adequate statement of reasons for the exchange of data. The assessments that have to be made in this respect are needed to prevent the unauthorised infringement of privacy. In the exchange of unevaluated data, these **assessments** are often **difficult to define** or **no requirement** exists for them to be **recorded**. In these cases, the protection of privacy can be at issue without the presence of adequate safeguards. The Committee has previously come up against this issue in its oversight practice. This is discussed below.

---

7 In this context, see also the legal appendix to Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, p. 13-15.

8 Article 24 (1) ISS Act 2002.

9 Article 27 (3) ISS Act 2002.

10 See also CTIVD Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, legal appendix, p. 20-21.

3.2 Previous findings of the CTIVD

Oversight practice concerning the exchange of unevaluated data

In review report no. 28, the CTIVD described and assessed cooperation between the MIVD and foreign services in the area of sigint.[11] The CTIVD noted that the MIVD exchanged unevaluated data with foreign intelligence and security services on a structural basis. The CTIVD described this as a **form of assistance** to foreign services through the deployment of the **power to select non-cable-bound communications**, because the process that was applied matched the selection process. Authorisation must be requested from the Minister, stating reasons, for the selection of satellite communication. Wrongly, this did not happen in this case. The CTIVD reiterated its position in review report no. 38 on the processing of telecommunications data by the AIVD and the MIVD.[12] It again equated this form of data provision with the deployment of an investigatory power for the benefit of a foreign service. This ensured **better regulation**. From then on, the AIVD and MIVD had to request authorisation, stating reasons, from the Minister in question. In response to report no. 38, the Minister of the Interior and Kingdom Relations and the Minister of Defence stated that the procedures are being modified.[13] The CTIVD discusses how these promises have now been implemented in practice in section 6.2.

In review report no. 38, the CTIVD observed that the AIVD acquired web forums through the use of investigatory powers and also obtained web forums from foreign intelligence and security services. In the latter case, no substantiated assessment was recorded regarding why it was deemed justified to examine the contents of the web forum. The CTIVD recommended that, when **acquiring web forums** from foreign services, the AIVD also makes an assessment of the extent to which examining of the contents of the web forum in question meets the legal requirements of necessity, proportionality and subsidiarity. This assessment must also be laid down in writing.[14] With regard to the **provision of web forums** to foreign services, the CTIVD considered that this is only permissible if the provision of all the data in the web forum can be regarded as necessary and proper.[15] In other words, this can only involve web forums that exclusively contain data on persons who can be regarded as subjects of investigation by the AIVD. The CTIVD reiterated its positions in report no. 39. It regarded the provision of web forums to foreign services as lawful up to that point, with the exception of one case.[16] The exchange of web forums between the AIVD and foreign services in practice is discussed in more detail in section 5.2.

Oversight practice in the field of cooperation with foreign services

In review report no. 38, the CTIVD noted that the ISS Act 2002 gives the AIVD and MIVD broad powers to cooperate with foreign intelligence and security services. When the ISS Act 2002 was created, no explicit consideration was given regarding how to handle the exchange of collections of (unevaluated) personal data.

---

[11] CTIVD Review Report no. 28 on the use of Sigint by DISS, *Parliamentary Documents II* 2011/12, 29 924, no. 74 (appendix), available at www.ctivd.nl, section 9.3.

[12] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 5.5.

[13] Parliamentary Documents II 2013/14, 29 924, no. 105, p. 2.

[14] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 3.5.5.

[15] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 5.6.

[16] CTIVD Review Report no. 39 on investigative activities of GISS on social media, *Parliamentary Documents II* 2013/14, 29 924, no. 114 (appendix), available at www.ctivd.nl, sections 5.4 and 5.5.

The CTIVD observed that, based on the ISS Act 2002, the AIVD and MIVD can pursue this exchange and that they actually do so in practice in various cooperative partnerships. This involves a far-reaching form of cooperation that takes place within close cooperative relationships with foreign services. According to the assessments of the AIVD and MIVD, these services meet the **criteria for cooperation**. Such relationships are based on a high degree of mutual trust. In report no. 38 the CTIVD adopted the position that, in the light of the current revelations, it was advisable to **examine whether this trust is still justified**. Specifically, this meant that the heads of the AIVD and the MIVD, under the political responsibility of the relevant Ministers, had to find out more about the legal powers and (technical) possibilities of foreign services so that they could make justified assessments. In this context, the CTIVD has recommended that the Minister of the Interior and Kingdom Relations and the Minister of Defence assess the cooperative relationships (including at international level) for transparency and further specify the assessments underlying the cooperation.[17] The discussion in Chapter 7 of the ministerial authorisation requirement deals with the importance of this recommendation. This question is discussed in more detail in the corresponding review report on the execution of House of Representatives motion no. 89 by members Schouw and Segers.[18]

3.3 Exchange of unevaluated data in the draft bill

The Intelligence and Security Services 20XX Act Draft Bill19 does include **rules** for the **provision of unevaluated data** to foreign intelligence and security services. This involves two provisions in the draft bill. Proposed Article 49 (3) states that, in the context of the proper performance of tasks, unevaluated data may be provided to a foreign service once the relevant Minister has given authorisation for this. Proposed Article 77 (2) includes a comparable provision for those cases where the provision of unevaluated data to a foreign service takes place in the interests of that foreign service. No provision is included for receiving unevaluated data.

The rule on the provision of unevaluated data has its origins in the cabinet response to the report of the Dessens Evaluation Committee, which was published at the same time as CTIVD review report no. 38. The cabinet announced that the exchange of bulk data would be subject to a system of ministerial authorisation.[20]

The explanatory memorandum to the draft bill explains that the provision of unevaluated data often involves the provision of large volumes of data ("bulk"). Although the incentive for the inclusion of the arrangement lies in the exchange of bulk data with foreign services, the legislator has, for the time being, opted for a broader approach. Since it is hard to define what a large volume is, this term is not used. The authorisation requirement therefore applies to the provision of all forms of unevaluated data. The decisive element is that it involves data, the relevance of which has not (yet) been established for the performance of the service's own tasks.

---

17 CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 5.1.

18 Review report no. 48, adopted on 4 May 2016, published simultaneously.

19 Intelligence and Security Services 20XX Act Draft Bill; legislative text (consultation version, June 2015), published on 2 July 2015. On 15 April 2016, the cabinet approved the bill. At the time of this report's adoption, the draft bill is with the Council of State for recommendation.

20 *Parliamentary Documents II* 2013/14, 33 820, no. 2, p. 7.

The cabinet has obviously reached the (provisional) conclusion that the unevaluated nature of the data to be provided – rather than the fact that a large volume is involved – is the reason why the safeguard of ministerial authorisation is appropriate. The Committee concurs with this reasoning. When unevaluated data is exchanged, the legally prescribed assessments are often difficult to define or are not an explicit component of the process (see also section 3.1), hence the importance of making data exchange subject to the additional safeguard of ministerial authorisation.

Furthermore, the explanatory memorandum also notes that authorisation can also relate to several consecutive instances of data provision of a comparable nature and as such does not have to be granted on a case-by-case basis. This is important for the provision of unevaluated data in the context of specific international cooperative partnerships.[21]

Examples of unevaluated data include complete websites and the untargeted acquisition of data (including satellite communication), to which no selection has yet been applied.

[21] Intelligence and Security Services Act 20XX Draft Bill, explanatory memorandum (consultation version, June 2015), p. 107 and 141-142

4. Policy for the exchange of unevaluated data

Policy within the AIVD and MIVD

It was clear to the Committee from its investigation that the contents of motion no. 96 and the promise made by the Minister that authorisation would be requested from him from now on in order to share bulk data have **not been incorporated into the policy** within the **AIVD** and have **been implemented within the policy of the MIVD** to a limited extent. Neither of the services has drawn up a written guideline stating what is and what is not covered by the terms "sets of (meta)data", "(meta)data in bulk" "bulk data" or "unevaluated data". Nor does any procedure set forth how and when authorisation must be requested from the Minister for the provision of unevaluated data or requests for unevaluated data to a foreign service or for the use of unevaluated data that has been provided by a foreign service without a request. Recently established written policy of the MIVD does state that authorisation from the Minister must be obtained.

Responses to written questions and conversations with representatives of the AIVD confirm that motion no. 96 has not led to the establishment of any arrangement, procedure or other policy document within the AIVD. Motion no. 96 is understood by the AIVD as relating to unevaluated bulk data, in other words satellite communication acquired through untargeted acquisition that has not yet been further processed. The AIVD did not immediately grasp that the motion can also apply to areas other than the untargeted acquisition of satellite communication. It was not regarded as necessary to formulate an AIVD-wide policy. The modification of processes within the JSCU was seen as sufficient.

The MIVD has also indicated that, according to the service, motion no. 96 relates to large volumes of unevaluated data, or bulk data. Specifically, this applies to the exchange of data between the JSCU and foreign services and not within other departments of the MIVD. The MIVD has indicated that the question whether to request authorisation from the Minister is discussed, considered and assessed on a case-by-case basis within the JSCU.

In January 2016, shortly before the conclusion of the investigation by the CTIVD, the management of the MIVD established a policy framework for international cooperation by the MIVD. With regard to the exchange of unevaluated data, the policy framework establishes only that, prior to the provision of such data, the Minister must grant authorisation for such an activity.

Definition

Both the AIVD and the MIVD refer, for the definition of bulk data or sets of (meta)data, to the terminology used in the draft bill and its explanatory memorandum (see section 3.3). Reference is made there to "unevaluated data", but without this necessarily involving a large volume or bulk. As examples, the explanatory memorandum to the draft bill cites a complete website or data acquired through untargeted acquisition (satellite communication), to which no selection has yet been applied.

Procedures at the JSCU

The JSCU is a joint unit of the AIVD and MIVD. The JSCU processes data in the field of *sigint* and *cyber*. The JSCU forms part of both services. The goal of the unit is to facilitate access to information from technical sources and to offer expertise and assistance to both services.

It was clear to the CTIVD from its investigation that **some modifications** were made within the procedures of the JSCU in the wake of motion no. 96. For instance, the manual of the JSCU dated June 2014, under "agreements on utilisation", states that an intent to provide bulk data to foreign services is submitted for the approval of the responsible Minister(s) via the management board. The legal appendix to the JSCU manual provides more text and explanation about the various forms of the provision of data to foreign services. It indicates that the provision of bulk is only possible with

the authorisation of the responsible Minister(s). Furthermore, it states that the assessment that must precede such provision based on Article 59 (2) ISS Act 2002[22] can be referred to at most as a "best effort". Why this is the case is not further elucidated in the text. The term "bulk" is not defined in the manual of the JSCU or in the appendix. However, it is repeatedly used as the opposite of evaluated data.

Furthermore, a memo to the management board of the JSCU dated 20 August 2014 indicates that ministerial warrants are needed in order to share substantial sets of (meta)data within cooperative partnerships. This will be implemented in accordance with the regular authorisation procedure. The memo also states that authorisation must be obtained from the Minister for application of the power to select non-cable-bound communications for the benefit of foreign services. These two new authorisation requirements will be implemented in accordance with the regular authorisation procedure. This procedure will be evaluated after six months. The way in which this has been put into practice is discussed in sections 5.1, 6.1 and 6.2.

Conclusions concerning policy

The CTIVD finds that, in the absence of a service-wide structured policy within the AIVD or MIVD, the starting point for the services is that it **must be assessed on a case-by-case basis** whether data exchange falls within the scope of motion no. 96 and whether ministerial authorisation must be obtained.

The CTIVD believes it is important, in anticipation of a possible amendment to the law, for the AIVD and the MIVD **to adopt a written policy** for both the provision and the receipt and subsequent use of unevaluated data.

The meaningful nature of this is illustrated by the practice encountered by the Committee in its investigation, specifically in terms of the exchange of web forums and the exchange of data within cooperative partnerships. This practice is discussed in the following chapters.

Reference must also be made here to the policy and practice of drawing up weighting notes. The CTIVD discusses this topic in Chapter 7 of this review report and in the corresponding review report on the execution of House of Representatives motion no. 89 by members Schouw and Segers.[23]

---

[22] This means the assessment as to whether the interests of the foreign service are compatible with the interests served by the Dutch service and the proper performance of tasks by the Dutch service is not in conflict with the provision of data.

[23] Review report no. 48, adopted on 4 May 2016, published simultaneously.

5 Practice within the AIVD

5.1 Exchange of data within cooperative partnerships

The AIVD exchanges unevaluated data with foreign intelligence and security services within three cooperative partnerships. Cooperation is topically or geographically oriented and enhances the performance of the tasks of the AIVD. The MIVD also participates in these cooperative partnerships. Cooperation takes place through the JSCU. Since this data exchange is to a large extent in line with other data exchange between the MIVD and foreign services and in order to avoid duplicate text, we have chosen to discuss this topic substantively in Chapter 6, on the MIVD (section 6.1).

The CTIVD also notes that, for the provision of unevaluated data by both services via the JSCU, authorisation must be obtained from both the Minister of the Interior and Kingdom Relations and the Minister of Defence. The request to the Minister of the Interior and Kingdom Relations and the subsequent authorisation for the exchange of data within one of the three cooperative partnerships were not to be found in the AIVD's systems. The CTIVD did, however, find a draft of the request. The AIVD has indicated that the Minister authorised this data exchange.

5.2 Exchange of web forums

Providing and receiving web forums

After conducting searches in the AIVD's systems, the CTIVD found that, since the adoption of motion no. 96, **some web forums have been both provided to and received from foreign intelligence and security services.**

Authorisation was requested, stating reasons, **from the Director-General of the AIVD** for receiving **and using** these web forums. The requests for authorisation indicate that this takes place with reference to CTIVD report no. 38. In accordance with the recommendation of the CTIVD,[24] the AIVD weighs up the extent to which examining the contents of the web forums in question meets the requirements of necessity, proportionality and subsidiarity. This is recorded in writing.

No authorisation was requested from the Director-General of the AIVD for the **provision** of web forums to foreign services, nor from the Minister. The CTIVD found that in one case, in a request to the Minister for authorisation for extension of the use of a hack, a summary is given of the foreign services to which the web forum obtained using the hack was provided. Authorisation is not explicitly requested for the provision of the web forum. The fact that this provision had taken place was mentioned in the account given of the results of the hack.

The CTIVD asked the team at the AIVD that provided the web forums whether the provision of web forums is not covered by the scope of motion no. 96. In response, the team indicated that this is not the case because these web forums are "specifically selected data sets acquired in a targeted manner and which, as a result of their nature, have been established prior to acquisition as a collection that as a whole meets the requirements of necessity, proportionality and subsidiarity". In this respect, the team refers to the CTIVD's assessment of the acquisition of these web forums in report no. 38. The team asserts that some web forums exclusively contain data on persons who can be regarded as

[24] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS (AIVD) and DISS (MIVD), *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 3.5.5.

subjects of investigation[25] by the AIVD. The CTIVD stated, in this respect, that the acquisition of such web forums easily meets the requirements of necessity, proportionality and subsidiarity.

Previous assessment of the CTIVD

The CTIVD did indeed indicate in report no. 38 that, generally speaking, the acquisition of such web forums easily meets the legal requirements. Moreover, the CTIVD stated, in report no. 39 on investigative activities by the AIVD on social media, that the acquisition of these web forums was necessary for the performance of the tasks of the AIVD.[26]

In report no. 38, the CTIVD noted with regard to the provision of web forums to foreign services that this is only permissible in so far as it involves web forums that exclusively contain data on persons who can be regarded as subjects of investigation by the AIVD.[27] Only these types of web forum, not other web forums that have a wider scope, may be provided to foreign services. Moreover, In report no. 39, the CTIVD found that the provision of the web forums concerned to foreign services was lawful.[28]

The term "unevaluated data"

Irrespective of lawful acquisition and provision, the question remains of whether these web forums are covered by the scope of motion no. 96. If that is the case, authorisation must be obtained from the Minister as an additional safeguard for the protection of privacy. In the absence of an internal AIVD policy and with reference to the draft bill, the CTIVD notes that the scope of motion no. 96 must be understood to mean the sharing of unevaluated data with foreign services. The question is **whether these web forums must be regarded as unevaluated data**.

The CTIVD establishes that the way in which the **data** was acquired (in a targeted or untargeted way) in fact makes **no difference** in assessing whether the data can be classified as evaluated or unevaluated data.[29] The AIVD can very specifically focus on a certain (part of a) web forum and acquire it through targeted acquisition. The data that is then acquired is unevaluated at that point. It cannot be referred to as evaluated data until it has been assessed as relevant to the performance of the tasks of the AIVD. This can be compared to telephone tapping. Tapping is a form of targeted data collection. The conversations acquired are unevaluated. and the data cannot be referred to as evaluated until the conversations have been listened to in full. Only those conversations that are relevant to the performance of tasks may be written up. When conversations acquired through tapping are provided to a foreign service without first listening to them in full and assessing them for relevance, this is the provision of unevaluated data. The issue here is not how the data was acquired, but that a certain volume of data has been acquired or provided, the contents of which **have not been assessed** for **relevance** to the performance of tasks.

---

[25] Organisations that and persons who, because of the objectives they pursue, or through their activities, give cause for serious suspicion that they are a danger to the continued existence of the democratic legal system or to the security or other vital interests of the state, Article 6 (2) under a, ISS Act 2002.

[26] CTIVD Review Report no. 39 on investigative activities of GISS on social media, *Parliamentary Documents II* 2013/14, 29 924, no. 114 (appendix), available at www.ctivd.nl, section 5.4.2.

[27] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 5.6.

[28] CTIVD Review Report no. 39 on investigative activities of GISS on social media, *Parliamentary Documents II* 2013/14, 29 924, no. 114 (appendix), available at www.ctivd.nl, section 5.5.2.

[29] The targeted nature of the acquisition is, however, decisive for the risk that knowledge is acquired of data regarding persons or organisations that are not the subjects of investigation by the service and are entirely separate from national security, or for the risk of an unauthorised infringement of privacy.

The question that can then be asked is whether web forums exist that can be regarded as relevant as a whole, given their nature, to the performance of tasks and can thus be regarded in advance as evaluated data. One example could be a jihadist web forum that is known as a forum for communication exclusively by persons who can be regarded as subjects of investigation by the AIVD. The aforementioned team that provided the web forums asserted that such web forums meet the legal requirements to be classified as an organisation. This type of web forum could in that sense be regarded as a subject of investigation as a whole.

The CTIVD is of the opinion that, however justified it may be for such web forums to be acquired and exchanged with foreign services, evaluated data can only exist once the specific data has been assessed for relevance to the performance of tasks. Again, the CTIVD makes the comparison with tapping. The AIVD must assess data resulting from tapping the telephone of a known foreign terrorist fighter to see which conversations are relevant to the performance of tasks and which are not. Data cannot be referred to as evaluated until the assessment has taken place.

The CTIVD stresses that a **distinction** must be made between the **acquisition of data** on the one hand and the **provision of data** on the other hand.

The acquisition of a web forum or of other (larger volumes of) data, for example a computer hard disk, can be aimed at a specific target or a certain target group. Despite the volume of data acquired, the AIVD can state in advance that the data is related to the target or target group and argue that the acquisition meets the requirements of necessity, proportionality and subsidiarity. The targeted nature of the acquisition can say something about the risk of data being acquired regarding persons who are not being investigated by the AIVD. The risk is small or non-existent and can be justified by the AIVD.

When the AIVD wants to provide this data to a foreign service, another assessment must be made, separate from the question of whether it was lawful in the first place to acquire the data. The AIVD must assess whether it is allowed to provide the data to a foreign service. However, this assessment is difficult to make without the AIVD having assessed the relevance of the data that has been acquired. The provision of a target's communication about plans for a trip is entirely different from the provision of a target's communication about this child's school report or his neighbour's double parking. The example of a computer's hard disk presents a similar picture. It can contain files that are critical to national security but it can also contain holiday snaps, family videos and other privacy-sensitive data that are not at all relevant to national security.

The provision of data without having assessed its relevance to the performance of tasks leads to a potential compromise of the protection of privacy. After all, the AIVD cannot adequately define the assessment of whether the provision of data to a foreign service is permitted. For this reason, an additional safeguard is sought in the ministerial authorisation requirement.

Conclusion: web forums generally involve unevaluated data

The CTIVD concludes from the above considerations that the **web forums** must in principle be **regarded** as **unevaluated data**. Therefore, pursuant to motion no. 96, **authorisation must be obtained from the Minister** for both provision of web forums to, and receiving/using web forums from, foreign intelligence and security services. This has not taken place.

A web forum as a whole cannot be regarded as evaluated until the AIVD has assessed the contents of all data included on the web forum as relevant to the performance of its tasks. Without assessing the contents of all data, a web forum is in principle unevaluated, barring exceptional circumstances. The CTIVD envisages some scope here when the AIVD can provide facts to demonstrate that a web forum is being used to communicate exclusively regarding matters related to ongoing investigations by the AIVD in the context of national security. Where appropriate, the AIVD will then have to make

the case itself and state the reasons for it. The decision not to request ministerial authorisation for the provision of a web forum to a foreign service and the facts that support the decision must then be recorded so that they can be assessed. This had not been done in the above-mentioned cases.

Response from Minister of the Interior and Kingdom Relations

In his response to the draft review report, the Minister of the Interior and Kingdom Relations indicated that the CTIVD's interpretation of the motion means that data can only be shared with foreign services if they have been assessed as relevant in the context of the performance of the tasks of the AIVD, or if the Minister has given authorisation. The Minister has indicated that this course of action cannot always be taken in the daily practice of cooperation. On the one hand, rapid action can be required, which is not compatible with having to request ministerial authorisation. On the other hand, data may be involved that does not initially seem relevant to the performance of the tasks of the AIVD but does in fact prove to be relevant after assessment (and, if possible, addition) by the foreign service. This can cause the AIVD to see the data in a different light. Assessment of the relevance of the data takes place, as it were, in consultation with the foreign service. Being able to quickly share and mutually assess data is specifically important in the context of an investigation into terrorism.

The CTIVD understands the Minister's concern. International cooperation in investigation fields such as combating terrorism is crucial to the proper performance of the tasks of the AIVD (and the MIVD). It is correct that the outcome of the considerations of the CTIVD is that either an assessment of the relevance of the data must be made by the AIVD or authorisation must be obtained from the Minister. Indeed, the authorisation of the Minister is needed in all cases for the sharing of unevaluated data with foreign services with the aim of first assessing jointly whether this data is relevant. This does not alter the fact that the Minister can give authorisation for the exchange of unevaluated data with foreign services in the context of cooperative partnerships with a particular topical or geographical orientation (see section 5.1), such as a specific terrorism investigation. In such cases, it is important for the relevant foreign services to qualify for this form of cooperation (see Chapter 7), for the Minister to give periodic authorisation for the exchange of data and for a record to be kept of which data is exchanged (see section 6.1).

The Committee also notes that when an investigatory power (for example, tapping or hacking) is deployed to assist a foreign service, the provision of the collected data forms part of that assistance. Authorisation does not then have to be obtained separately from the Minister. After all, authorisation must be requested from the Minister, stating reasons, for assistance through the deployment of an investigatory power. In this respect, see also section 6.2 on the assistance provided by the MIVD to foreign services through the deployment of the power to select non-cable-bound communications.

5.3 Practice in other cases

During the CTIVD's investigation, the AIVD initially indicated that, apart from exchanges within three topically or geographically oriented cooperative partnerships (see sections 5.1 and 6.1), no unevaluated data was exchanged with foreign services. The CTIVD asked written questions about this. In response to the requests for information from the CTIVD, the AIVD requested further details about which exchanges of data fall within the scope of motion no. 96 and in which cases the authorisation of the Minister is required.

In the absence of a policy, the AIVD has not recorded every instance of the provision of unevaluated data to foreign services. The service was only able to submit to the CTIVD a few requests to the Minister for authorisation (see section 5.1). The AIVD was not able to give a conclusive answer to the question of whether this is everything and whether, in other cases, authorisation should have been obtained from the Minister.

The CTIVD has observed, from previous investigations and from random tests conducted in this investigation, that the authorisation of the Minister has not always been obtained for the exchange of web forums (see section 5.2). It has not conducted any further exhaustive investigation in order to find out of whether any other unevaluated data have been provided to or received from foreign services. This was outside the remit of this investigation.

6 Practice within the MIVD

6.1 Exchange of data within cooperative partnerships of the AIVD and the MIVD[30]

Five requests for authorisation

The exchange of unevaluated data with foreign intelligence and security services takes place within a few cooperative partnerships. Cooperation is topically or geographically oriented and enhances the performance of the tasks of the AIVD or MIVD. Cooperation takes place through the JSCU. In the context of three cooperative partnerships in which both the AIVD and MIVD participate, authorisation was requested, stating reasons, from the Minister of the Interior and Kingdom Relations and the Minister of Defence to continue the exchange of data. The exchange of data has taken place on a structural basis and for a long time, even before motion no. 96 was adopted. The requests for authorisation are dated 23 June 2014, 19 September 2014 and early November 2015.

In addition, cooperative partnerships exist with foreign intelligence and security services in which exclusively the MIVD participates. In this context, authorisation was requested, stating reasons, from the Minister of Defence with regard to two topics; for authorisation to participate on a structural basis in the relevant cooperative partnership and, in that context, to share unevaluated data, among other things. These requests are dated 25 November 2014 and 19 December 2014.

Each of the five requests for authorisation explain what is covered by the cooperative partnership in question and with which foreign services cooperation takes place. In most cases, this involves foreign services with which close cooperative relationships exist. In addition, the importance of the cooperation in question is explained with reference to the performance of the tasks of the AIVD and MIVD, respectively. The various forms of data exchange that (will) take place are also discussed. This relates mainly to the exchange of satellite communication acquired in an untargeted manner. In one cooperative partnership, the exchange is confined to metadata.[31] Two of the cooperative partnerships involve the exchange of both evaluated and unevaluated data.

The requests for authorisation state that data connected to Dutch telecommunication characteristics[32] (where identifiable) are not provided.

Time of authorisation

The exchange of unevaluated data within the three cooperative partnerships in which both the AIVD and MIVD participate has been taking place for quite some time. Even before motion no. 96 was adopted, this exchange of data was taking place. It is clear to the Committee that, in two of the three cases, authorisation was not requested from the two Ministers for the exchange of data that was already taking place until quite some time after adoption of the motion (five and eighteen months respectively).[33]

The CTIVD asked what the reasons were for this. Regarding one of the requests for authorisation, the MIVD indicated that the Minister was aware of the cooperation, that the cooperative partnership

---

[30] This section also refers to cooperative partnerships in which the AIVD participates. Since this exchange of data is to a large extent in line with data exchange between the MIVD and foreign services and in order to avoid duplicate text, we have chosen to include a substantive discussion of this topic in the chapter on the MIVD.

[31] Data about a communication session. The metadata of a telephone call, for example, comprises the telephone numbers involved, the starting and ending times of the call and the data of the mobile phone masts involved.

[32] An example of this is a telephone number with country code 0031 or +31.

[33] In the third case, authorisation was requested after approximately two months.

has been assessed as lawful by the CTIVD in report no. 38 and that the coordination of a request for authorisation with the AIVD takes time. For this reason, a request for authorisation was not submitted until five months had passed. The other request has long been a topic of discussion between the two services and, for that reason, was submitted to the Ministers about eighteen months later. The AIVD and MIVD explained that the discussion centred on the question of whether the form of cooperation in question should be regarded as an exchange of unevaluated data. Ultimately, the cooperation was correctly designated as data exchange for which authorisation must be obtained from the Minister.

The CTIVD is of the opinion that it could reasonably be expected that the ministerial authorisation for the exchange of unevaluated data be requested soon after the motion was adopted on 15 April 2014. It makes no difference that this exchange had already been ongoing for some time and was common practice. After all, the House of Representatives motion made it clear that additional safeguards are needed for this form of data exchange. The CTIVD certainly appreciates that the mutual coordination of the contents of a request for authorisation takes some time. However, it finds five and eighteen months too long. The CTIVD finds that authorisation should have been obtained earlier.

Evaluated and unevaluated data

The five requests for authorisation are general in nature. A general insight is provided into the intended goal of the cooperation and the need for the exchange of data in order to achieve that goal. The assessments made in that respect are not very specific. Section 3.1 explains that making the assessments required for the exchange of data sufficiently specific is challenging where unevaluated data is concerned. After all, it is not clear what data is being provided. Moreover, the provision of data is often not aimed at processing data about a specific person or organisation. For this reason, additional safeguards, such as the authorisation of the Minister, are regarded as necessary in order to reduce the risk of an unauthorised infringement of privacy.

The above applies to the exchange of unevaluated data but not to the exchange of evaluated data. After all, where evaluated data is concerned, it is possible to make a thorough assessment of why that specific data must be provided in that specific case to that specific foreign service. Reasons can then be stated regarding the goal that makes it necessary to provide the data. Interests can also be weighed, namely the interests of the service in achieving the intended goal and the possible disadvantage for the person or organisation to whom the data relates.

The CTIVD notes that two of the five requests for authorisation include the exchange of evaluated data as well as the exchange of unevaluated data. The CTIVD sees it as a positive step for the Ministers to be informed of this form of data exchange. It does however point out that this does not cover everything. The protection of privacy requires a specific assessment in every individual case of data exchange. That is the starting point.

Indefinite authorisation

The authorisation of the Ministers is **not limited in time**. The requests are drawn up based on the general objective of the cooperative partnership in question. This objective ensures some delimitation. The requests for authorisation are otherwise unlimited. Two requests do state that **periodic reviews** are carried out to check whether it is still necessary, in the context of the objective, to exchange data. The ISS 20XX Act Draft Bill gives scope for the Ministers to give broad authorisation. The explanatory memorandum to the draft bill states that the authorisation can also relate to several consecutive instances of provision of a comparable nature, which is particularly important for the exchange of such data in the context of specific international cooperative partnerships. The authorisation does not then have to be given on a case-by-case basis.[34]

---

[34] Intelligence and Security Services 20XX Act Draft Bill; explanatory memorandum (consultation version, June 2015), pp. 141-142.

Although the draft bill provides for this procedure, the CTIVD believes it is important that the authorisation granted should not automatically be valid indefinitely. The CTIVD asked the services what is involved in the aforementioned periodic review and how this is given a place in the process. In response, it was indicated that internal review is performed to see whether the need for data exchange still exists. According to the services, this review takes place regularly, for example when preparing for the consultations that take place in the context of the cooperative partnership. This is an underlying process, part of the normal decision-making that takes place in the context of the cooperative relationship. No firm review time is built in. It was also indicated that the limitation of the ministerial authorisation is connected to the topic that forms the focus of the cooperative partnership. If, for example, armed forces are being deployed abroad, the need to exchange data will cease once the relevant mission has been completed. Furthermore, the need can change, for example because the character of the cooperation changes. In such cases, the Ministers will be informed.

The CTIVD is of the opinion that the periodic review described above is of only limited value for the protection of privacy. Given the vulnerability of the exchange of data, the Committee believes it is important for the policy of the services to prescribe that assessments be carried out periodically (for example, every six months) to ascertain whether, in the context of the objective of the cooperative partnership, the exchange of unevaluated data is still permitted and that these assessments be laid down in writing so that they can be reviewed.

Furthermore, the CTIVD believes it is **necessary** for the ministerial authorisation to be linked to a fixed **authorisation period**, for example one year. It suggests that the legislator consider providing for this in the forthcoming amendment of the ISS Act 2002. The CTIVD believes it is important for the AIVD and MIVD, in anticipation of the amendment of the Act, to stipulate an authorisation period in their policies.

Obligation to keep records

Following on from Article 42 of the ISS Act 2002, which states that a record must be kept of the provision of personal data, the CTIVD believes it is important for the AIVD and MIVD to keep clear records of which data (files) are being exchanged in the context of the cooperative partnerships.

Received data

The CTIVD notes that the **same safeguards** apply to unevaluated data received from foreign services in the context of these cooperative partnerships as to data gathered by the AIVD and MIVD themselves. The metadata is used for metadata analysis.[35]

The content data cannot automatically be used in the intelligence process and is not made available until it has been selected. Authorisation for selection, using selection criteria, must be requested from the Minister (Article 27 (3) ISS Act 2002), with statement of reasons. This process is no different when receiving data. The safeguards for the protection of privacy are the same.

[35] In review report no. 38, the CTIVD recommended that the process of metadata analysis provide by law for safeguards to protect against the unauthorised infringement of privacy, such as stating reasons for the necessity, proportionality and subsidiarity of the data processing in order to obtain the relevant internal or external authorisation. CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, p. 15.

6.2 Assistance through deployment of power to select

Assistance through deployment of power to select

In review report no. 28, the CTIVD described and assessed cooperation between the MIVD and foreign services in the area of *signals intelligence* (sigint).[36] The CTIVD noted that the MIVD exchanged unevaluated data on a structural basis with foreign intelligence and security services. This involved bilateral cooperation that did not take place within a cooperative partnership with a specific topical or geographical orientation. The foreign services supplied lists of selectors, for example telephone numbers, which the MIVD used to filter the data from the archive[37] and subsequently provide them to the foreign services in question. The MIVD found that this provision of data was an extension of the power to acquire satellite communication in an untargeted manner (Article 27 (1) ISS Act 2002). No authorisation is required for this. Since it was difficult in practice to share large volumes of data, the volume of data was limited, based on the need of the foreign service in question, using the list of selectors. The MIVD itself did not examine the data.

The CTIVD described this procedure as a form of **assistance** to foreign services through the deployment of the **power to select non-cable-bound communications** (Article 27 (3) ISS Act 2002). The process that was applied to limit the volume of data, on the basis of selectors supplied by the foreign service, corresponded to a significant extent to the selection process. Authorisation must be requested from the Minister, stating reasons, for the selection of satellite communication. Wrongly, this did not happen in this case. The CTIVD reiterated its position in review report no. 38 on the processing of telecommunications data by the AIVD and the MIVD.[38] By equating this form of data provision to the deployment of an investigatory power for the benefit of a foreign service, **better regulation** was ensured. From then on, authorisation had to be requested from the Minister(s), stating reasons. In response to report no. 38, the Minister indicated that the procedure was being modified.[39]

Requests for authorisation

The CTIVD found that, since 18 April 2014 (three days after motion no. 96 was adopted), **authorisation** has been requested periodically from the Minister of Defence. The MIVD sought to take example from the normal authorisation procedure for the selection process: every three months, the Minister is given reasons why the selection of certain data meets the requirements of necessity, proportionality and subsidiarity. The requests for authorisation to assist foreign services are therefore also submitted to the Minister every three months. A separate request is drawn up for each foreign service.

Need of the foreign service

The MIVD must give reasons to support the requests for authorisation made to the Minister. This statement of reasons takes place based on the need of the foreign intelligence and security service.

The CTIVD notes that the MIVD has made efforts to gain a further understanding of the need of the relevant foreign services. The MIVD has set up a format for the lists of selectors. The information that must be filled in, apart from the selectors themselves, is the corresponding identity of the person or organisation and a description of the file or investigation topic to which it relates. This therefore gives the MIVD a (limited) explanation. As a result, the MIVD was in a position to **better substantiate**

---

[36] CTIVD Review Report no. 28 on the use of Sigint by DISS, *Parliamentary Documents II* 2011/12, 29 924, no. 74 (appendix), available at www.ctivd.nl, section 9.3.

[37] The archives involve the storage of data acquired through untargeted acquisition that has not yet been selected (Article 27 (1) ISS Act 2002).

[38] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 5.5.

[39] *Parliamentary Documents II* 2013/14, 29 924, no. 105.

requests made to the Minister. Moreover, the lists are attached as an appendix to the requests for authorisation.

The MIVD has indicated to the Minister that any particular details observed are mentioned in the requests for authorisation, including notable changes. In one case, the CTIVD found that a marked change in the need of one foreign service was briefly mentioned but that no further explanation or justification was given. One foreign service's list of selectors was almost tripled at one point. Admittedly, the request to the Minister did mention the number of selectors but did not indicate that this involved a sharp increase and what the (possible) reason for this was.

Common ground with the performance of tasks

The CTIVD observes that the need of the foreign services in some cases shares **no common ground** with the **tasks** of the MIVD. The MIVD wondered whether provision of the assistance is nevertheless permitted in such cases. The service consulted on this matter with the Legal Affairs Department of the Ministry of Defence. Both the MIVD and the Legal Affairs Department of the Ministry take the position that the MIVD is permitted to provide assistance in this way. According to them, a connection must exist with the performance of tasks of the foreign service, not so much with the performance of tasks of the MIVD. It is important from the perspective of *quid pro quo*[40] considerations to provide the requested assistance when possible.

The CTIVD can largely endorse this and notes the following. The ISS Act 2002 includes the possibility of providing assistance to a foreign service in the interests of that service (Article 59 (4) ISS Act 2002). **Two restrictions** are included.[41] The interests of the foreign service may not **be incompatible** with the interests protected by the MIVD. The **interests** protected by the MIVD must be understood to include fundamental and human rights, which are defined in the Constitution and in the international treaties ratified by the Netherlands. Other international legal standards, such as the public international law framework that applies to a military mission abroad, must also be included here. Moreover, the **proper performance of the tasks** of the MIVD may not be **in conflict with the assistance**. If these two restrictions are not an obstacle to the assistance, the MIVD is in principle permitted to provide this assistance.

The starting point of the current legislation is that the foreign service is regarded as remaining within its own legal framework.[42] Without firm indications to the contrary, the MIVD may assume that the foreign service has respected the laws and regulations applicable to that service when drawing up and providing the lists of selectors. In principle, the MIVD may trust in this (see page 24). However, the MIVD is not permitted to provide assistance if the suspicion exists that the foreign service is asking it to deploy a power that the service itself does not possess (the U-turn construction). This suspicion was not present in this case.

When **an investigatory power is deployed** to assist a foreign service, **additional conditions** must be met. The deployment must be necessary in the context of certain tasks of the MIVD (Article 18 ISS Act 2002) and must meet the requirements of proportionality and subsidiarity (Articles 31 and 32 ISS Act 2002). The problem here relates to necessity. The crucial question is how the assistance, which is provided exclusively in the interests of the foreign service, can at the same time be necessary for the performance of tasks of the MIVD. These two facts are not compatible. The CTIVD has previously

---

[40] The starting point of *quid pro quo* or "one good turn deserves another" plays an important role in cooperation among intelligence and security services.

[41] For a further itemisation of these limitations, see CTIVD Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, legal appendix, p. 12.

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

stated that this is a conflict in the law.[43] The CTIVD has always taken the position that, nonetheless, for the use of investigatory powers in assistance of a foreign service, authorisation must be requested and this request must be substantiated as well as possible. In that respect, it is important to seek additional safeguards, where possible, to protect privacy.

Additional safeguards

The CTIVD found that the selection process to assist a foreign intelligence and security service is largely a computerised process. Based on the list of selectors supplied, a computer examines which data already intercepted by the MIVD (in the bulk archives) meets the need of the foreign service. This data is then provided to the foreign service. The MIVD has provided additional safeguards: firstly, a **check on the selectors supplied** by the foreign service. Staff at the JSCU as well as lawyers at the MIVD and the Ministry of Defence independently examine whether the need of the foreign service is not incompatible with the interests protected by the MIVD. An example of incompatibility would be when the foreign service focuses on spying in allied countries. If such incompatibility exists, the data is not selected and therefore not provided to the foreign service. Furthermore, **Dutch selectors**[44] (where identifiable) are **removed** from the lists before the data is selected and provided. The CTIVD is of the opinion that these safeguards are adequate. It has not conducted any further exhaustive investigation in order to find out whether any other unevaluated data has been provided to or received from foreign services. This was outside the remit of this investigation.

Receiving data

In a similar way, the MIVD obtains unevaluated data from foreign services. The Committee observes that the **same safeguards** apply to unevaluated data received in this context from foreign services as to data gathered by the MIVD itself. After interception, the data is stored in the archive. The metadata is used for metadata analysis.[45] The content data cannot automatically be used in the intelligence process and is not made available until it has been selected. Authorisation for selection, based on the selection criteria, must be requested from the Minister (Article 27 (3) ISS Act 2002), with statement of reasons. This process is no different when receiving data from foreign services. The safeguards for the protection of privacy are the same.[46]

6.3 Practice in other cases

During the CTIVD's investigation, the MIVD indicated that no unevaluated data was exchanged with foreign services, with the exception of the exchange of data with foreign intelligence and security services via the JSCU (see sections 6.1 and 6.2). In the absence of a policy, the MIVD did not record every instance of the provision of unevaluated data to foreign services.

In a previous investigation, the CTIVD noted that, in some cases, unevaluated investigation results, for example telephony and traffic data, were provided as a whole to a foreign service. At the time, the CTIVD stated that it did not find this unlawful in principle. The CTIVD was, however, of the opinion that

---

[43] CTIVD Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, legal appendix, p. 22-23.

[44] An example of this is a telephone number with country code 0031 or +31.

[45] In review report no. 38, the CTIVD recommended that the process of metadata analysis provide by law for safeguards to protect against the unauthorised infringement of privacy, such as stating reasons for the necessity, proportionality and subsidiarity of the data processing in order to obtain the relevant internal or external authorisation. CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, p. 15.

[46] In this context, see also H. Born, I. Leigh, A. Wills, "Making International Intelligence Cooperation Accountable" (DCAF 2015), p. 98-99.

the MIVD must deal cautiously with this data and must ask itself to what extent it is necessary and proportional to provide the data as a whole.[47] The cases cited occurred long ago.

In previous investigations and in random tests conducted in this investigation, the CTIVD found no other cases of the exchange of unevaluated data, for which authorisation must now be obtained from the Minister. However, the CTIVD has not carried out any exhaustive investigation in order to find out whether other unevaluated data has been provided to or received from foreign services. This was outside the remit of this investigation.

[47] CTIVD Review Report no. 22b on the cooperation by DISS with foreign intelligence and/or security services, *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl, p. 30.

7 Trust in foreign services

Cooperation with foreign intelligence and security services is crucial to the proper performance of tasks by the AIVD and MIVD. Given the geopolitical nature of the threats to national security, the exchange of data with foreign services forms a condition for the existence of the AIVD and MIVD. Taking this into consideration, the legislator thought it was important, before entering into a cooperative relationship, for the AIVD and MIVD to **assess** whether a foreign service **qualifies for cooperation**. Based on cooperation criteria, the potential nature and intensity of the cooperation must be determined.

The AIVD and MIVD have indicated that the foreign services with which unevaluated data are exchanged meet the **criteria for cooperation**, such as democratic anchorage, respect for human rights and reliability and professionalism. Far-reaching forms of cooperation can take place with intelligence and security services that meet all the cooperation criteria. The CTIVD notes that the exchange of unevaluated data on a structural basis is one of the **most far-reaching forms of cooperation**. Moreover, it is a form of cooperation in which **trust** in the foreign service is assigned an **important role**. This refers to the trust that the foreign service has lawfully acquired the unevaluated data that this service provides to the AIVD and MIVD. It also means the trust that the foreign service subsequently processes the unevaluated data that this service obtains from the AIVD or MIVD with due care and, in so doing, remains within its own legal framework.

Moreover, in report no. 38, the CTIVD considered that the **trust** placed by the AIVD and MIVD in the foreign services with which cooperation takes place, given the discussion at the time about interception by the NSA, **merits reconsideration**. The CTIVD stated that consideration must be given, under the political responsibility of the Minister, to whether foreign services still qualify for the various forms of cooperation that take place in the context of close cooperative relationships. In specific terms, this means that the Ministers must find out more details about the legal powers and (technical) possibilities of foreign services so that they can make justified assessments. The CTIVD also recommended that the Ministers assess the cooperative relationships (including in international context) for transparency and further define the assessments underlying the cooperation.[48] The Ministers accepted this recommendation.[49]

The assessment on the basis of the cooperation criteria must provide some insight into the **boundaries** of **the trust** that can be placed in the foreign service. Based on the assessment of the cooperation criteria, the nature and intensity of the cooperation must be defined. Any possible risks associated with the cooperation must also be named and weighed up. For instance, attention must be devoted to the level of data protection by the foreign services, on the basis of the contents of the rules applicable to that service and on the basis of the practice that must ensure compliance with those rules. In that context, attention must also be devoted to the safeguards in the area of data processing, such as the storage and destruction of data. In the event of changes or indications that the trust placed in the foreign service is unjustified, the assessment must be repeated and the considerations made in the process must, if necessary, be adjusted.

---

[48] CTIVD Review Report no. 38 on the processing of telecommunications data by GISS and DISS, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix), available at www.ctivd.nl, section 5.1.

[49] *Parliamentary Documents II* 2013/14, 29 924, no. 105.

Each individual case of cooperation, for example the provision of certain data or the deployment of an investigatory power to assist a foreign service, must involve assessment of whether the requirements of necessity, proportionality and subsidiarity are met. This must be tested against the general assessment of how a foreign service handles its powers and a judgement of whether trust can be placed in it. Therefore, a two-fold assessment must take place in each individual case: does it fit within the boundaries of the cooperation as defined in the weighting note and, within those boundaries, does it meet the requirements of necessity, proportionality and subsidiarity? In this way, the assessment of whether a foreign service qualifies for cooperation forms a major **safeguard** for **the protection of privacy**.

Where risks are present in individual cases of cooperation, the general assessment on the basis of the cooperation criteria is the most relevant. For example, this is the case when the AIVD or MIVD provides unevaluated data to a foreign service because it is not clear exactly what data is being provided. The weighting notes indicate, in a balanced and well-reasoned manner, which fields of cooperation can potentially involve risks and under what circumstances cooperation is permitted. In each individual case, the AIVD and MIVD must assess whether the risks cited in the weighting note are present and, if so, which compelling (operational) conditions would still lead to provision of data or assistance to the foreign service. The assessment based on the cooperation criteria thus forms the basis for being able to take justified risks in the cooperative relationship.

The CTIVD is of the opinion that the requirement of **ministerial authorisation** is particularly apt in this context. The required authorisation of the Minister may not degenerate into a rubber stamp (authorisation inflation). A **substantive review** must take place that forms an actual safeguard for the protection of privacy.[50] The exchange of unevaluated data can only take place with foreign services that qualify for this form of cooperation. The AIVD and MIVD assess whether this is the case and whether they can trust that the foreign service complies with the legislation and regulations applicable to that service and with the arrangements made in the cooperative relationship. It is up to the Minister to review whether this assessment is correct and can support the exchange of unevaluated data in that specific case.

The CTIVD discusses the way in which the AIVD and MIVD implement the assessment on the basis of the cooperation criteria in its corresponding review report on the execution of House of Representatives motion no. 89 by members Schouw and Segers.[51] The CTIVD observes in that report, among other things, that the policies of the two services and the practice of drawing up weighting notes devote no attention to the system of data protection of foreign services and that the exchange of unevaluated data is only covered to a limited extent. The result of this can be that the aforementioned **review by the Minister can be regarded as of minor significance under these circumstances**. The CTIVD provides guidelines for the AIVD and MIVD for the future drawing up of weighting notes and the improvement of previously established weighting notes so that the trust that is placed in foreign services can have firm foundations and the review by the Minister can form a genuine safeguard for the protection of privacy.

---

[50] In this context, see also H. Born, I. Leigh, A. Wills, "Making International Intelligence Cooperation Accountable" (DCAF 2015), p. 120-128.

[51] Review report no. 48, adopted on 4 May 2016, published simultaneously.

8 Conclusions

Assessment framework

Scope of motion

Motion no. 96 (15 April 2014) relates to the exchange, in other words providing and receiving, of unevaluated data with foreign services. Unevaluated data is data that has not yet been assessed for relevance to the performance of tasks by the AIVD or MIVD. Authorisation from the relevant Minister must be obtained for the exchange of unevaluated data. It is up to the Dutch House of Representatives to assess whether motion no. 96 has been adequately implemented. (Chapter 1)

ISS Act 2002

The ISS Act 2002 does not include specific provisions for the exchange of unevaluated data with foreign intelligence and security services. The present law does offer general frameworks for the processing of data and for cooperation with foreign services. These frameworks also apply here. Among other things, the law requires that assessments be made prior to the exchange of data, regarding the necessity and propriety of the exchange. When unevaluated data is involved, specific assessments can often be difficult to make. One major reason for this is that the services do not know exactly what data is being provided or received. Since adequate reasons cannot be stated for the data exchange, limited safeguards exist for the protection of privacy. (section 3.1)

CTIVD oversight

The CTIVD encountered this issue earlier in the practice of its oversight. It observed, in various review reports, that additional safeguards must be provided for the exchange with foreign services of satellite communication (sigint) acquired by untargeted acquisition and for the exchange of web forums. The previous recommendations of the CTIVD are intended to ensure better regulation of these forms of cooperation with foreign services. (section 3.2)

Draft bill

The Information and Security Service Act 20XX Draft Bill does provide rules for the provision of unevaluated data to foreign intelligence and security services. Authorisation from the Minister in question must be obtained prior to this provision. The draft bill does not include any provisions for receiving unevaluated data from foreign services. (section 3.3)

Policy and practice

AIVD and MIVD policy

The CTIVD establishes that the AIVD has not drawn up a written policy in the wake of motion no. 96. The MIVD has included a provision in its policy stating that authorisation must be obtained from the Minister. Neither of the services has defined, in a written policy guideline or procedure, what must be understood by the term “unevaluated data” and under which circumstances, how and when authorisation must be obtained from the Minister. The CTIVD notes that, in the absence of such written policy, the starting point for the services is that an assessment must be made on a case-by-case basis to determine whether the data exchange in question falls within the scope of motion no. 96 and for which the authorisation of the Minister must be obtained. The CTIVD believes it is important for the AIVD and the MIVD, in anticipation of a possible amendment of the law, to adopt a structured policy in this area. The significance of doing so is illustrated by the practice encountered by the CTIVD. (Chapter 4)

Exchange of web forums

Since the adoption of motion no. 96, the AIVD has received some web forums from foreign intelligence and security services. Authorisation was requested, with statement of reasons, from the head of the service. The AIVD also provided some web forums to foreign services. The AIVD took the position that the web forums in question were not covered by the concept of unevaluated data, partly because they were specifically selected data sets acquired in a targeted manner and, in that case, authorisation from the Minister is not required. According to the AIVD, it is possible to establish prior to the acquisition of web forums, based on their nature, that as a whole they meet the requirements of necessity, proportionality and subsidiarity.

The CTIVD notes that the deciding factor, when answering the question of whether authorisation should have been obtained from the Minister, is whether unevaluated data is being exchanged. In fact, how the data was acquired (targeted or untargeted) makes no difference. The point is whether the contents of the data have been assessed as relevant to the performance of tasks. The CTIVD makes a comparison with telephone tapping. Even if the tapping was targeted at a specific person, the data collected from tapping is unevaluated. Data is only referred to as evaluated when the tapped conversations have been listened to in full and have been assessed as relevant to the performance of tasks. This applies equally to web forums. The CTIVD stresses that a distinction must be made between acquisition on the one hand and the provision of data on the other hand. If the acquisition of data can be regarded as necessary for the performance of tasks and meets the requirements of proportionality and subsidiarity, this does not mean that the data acquired is also (all) relevant to the performance of tasks. This assessment must be made separately.

The CTIVD concludes that, in principle, web forums must be regarded as unevaluated data. Therefore, pursuant to motion no. 96, authorisation must be obtained from the Minister for both the provision of web forums to, and the reception and use of web forums from, foreign services. This has not taken place.

The web forum as a whole cannot be regarded as evaluated until the AIVD has assessed the contents of all data included in the web forum as relevant to the performance of tasks. Without assessing the contents of all data, a web forum is in principle unevaluated, barring exceptional circumstances. The CTIVD can see some scope here if the AIVD can provide facts to demonstrate that a web forum is being used to communicate exclusively on matters that are related to ongoing investigations by the AIVD. The decision not to request authorisation from the Minister and its basis in fact must then be recorded for each instance of provision, so that it can be assessed. This has not taken place. (section 5.2)

Exchange within cooperative partnerships

The AIVD and MIVD exchange unevaluated data on a structural basis within five topically or geographically oriented cooperative partnerships with foreign intelligence and security services. These involve three cooperative partnerships in which both services participate and two cooperative partnerships in which only the MIVD participates. The exchange of data in the context of the three joint cooperative partnerships has been taking place for some time. The CTIVD notes that authorisation from the relevant Ministers for a successive exchange of unevaluated data in the context of two of these cooperative partnerships, which had already started before motion no. 96, was not obtained until five and eighteen months, respectively, after the adoption of motion no. 96. No good reason was given for this delay. The CTIVD is of the opinion that authorisation should have been obtained earlier.

The CTIVD establishes that ministerial authorisation has been granted within these five cooperative partnerships for an indefinite period. Two requests for authorisation indicate that reviews will take place periodically to see whether it is still necessary, in the context of the objective of the cooperative partnership, to exchange data. The CTIVD notes that this is an internal review that is not further secured and that its results are not presented to the Minister. The CTIVD is of the opinion that this

review has only limited value for the protection of privacy. It believes it is important for the policies of the services to prescribe that assessments be made periodically (for example, every six months) to establish whether the exchange of unevaluated data is still permitted in the context of the objective of the cooperative partnership and that these assessments be laid down in writing so that oversight can be exercised in that respect. The AIVD and the MIVD must also keep a clear written record of which data (files) are exchanged in the context of the cooperative partnerships.

The CTIVD observes that some scope is deliberately created, in the rules for the provision of unevaluated data in the draft bill, for broad authorisation from the Minister. The explanatory memorandum indicates that the Minister in question can give authorisation for several successive provisions of data in the context of international cooperative partnerships. The CTIVD finds it necessary, for the protection of privacy, for the authorisation of the Minister to be linked to a firm authorisation period, for example one year. It suggests that the legislator consider this in forthcoming changes to the ISS Act 2002 and regards it as important for the AIVD and MIVD to include an authorisation period in their policies in anticipation of the change in the law. (sections 5.1 and 6.1)

Assistance through deployment of power to select

The MIVD exchanges telecommunication gathered through untargeted acquisition on a structural basis with foreign intelligence and security services. The foreign services supply lists of selectors, for example telephone numbers, which the MIVD used to filter the data from the archive and subsequently provide them to the foreign services in question. In previous review reports, the CTIVD described this procedure as a form of assistance to foreign services through the deployment of the power to select non-cable-bound communications. The CTIVD notes in this review report that periodic authorisation for this has been requested from the Minister of Defence since 18 April 2014 (three days after motion no. 96 was adopted).

Furthermore, the CTIVD notes that the MIVD has made efforts to gain more insight into the background to the need of the foreign services in question. As a result, the MIVD has been in a position to better substantiate the requests for authorisation made to the Minister of Defence. Moreover, the lists of selectors supplied by the foreign services are also attached as an appendix to the requests for authorisation. The CTIVD found that a marked change in the need of one foreign service was briefly mentioned in one case but that no further explanation or justification was given.

The CTIVD establishes that, in some cases, the need of the foreign services shares no common ground with the tasks of the MIVD. The CTIVD is of the opinion that, nonetheless, the MIVD is permitted to provide support. The ISS Act 2002 imposes two restrictions on the provision of assistance to foreign services. The interests of the foreign service may not be incompatible with the interests protected by the MIVD, which include fundamental and human rights. Moreover, the proper performance of the tasks of the MIVD may not be in conflict with the assistance. If these two restrictions are not an obstacle to the assistance, the MIVD is in principle permitted to provide this assistance. In this respect, the starting point is that the foreign service is deemed to comply with the laws and regulations applicable to that service. The ISS Act 2002 also imposes additional requirements when the assistance involves the deployment of an investigatory power. The deployment must meet the requirements of necessity, proportionality and subsidiarity. The problem here relates to necessity. The question is how the assistance, which is provided exclusively in the interests of the foreign service, can at the same time be necessary for the performance of tasks of the MIVD. These two facts are not compatible. The CTIVD has previously stated that this is a conflict in the law. The CTIVD has always taken the position that, nonetheless, for the deployment of investigatory powers to assist a foreign service, authorisation must be requested from the Minister and this request must be substantiated as well as possible. In that respect, it is important to seek additional safeguards, where possible, to protect privacy.

It is clear to the CTIVD that the MIVD has provided additional safeguards for its procedure. A two-fold check is performed on the selectors supplied by the foreign service. Staff at the JSCU as well as lawyers at the MIVD and the Ministry of Defence independently examine whether the selectors supplied are compatible with the interests protected by the MIVD. Furthermore, Dutch selectors (where identifiable) are removed from the lists before the data is selected and provided. The CTIVD is of the opinion that these safeguards are adequate. (section 6.2)

Other exchange of unevaluated data

In the absence of a structured policy, the AIVD and MIVD have not recorded every instance of the provision of unevaluated data to foreign services. The AIVD and MIVD were only able to submit to the CTIVD a few requests to the Minister for permission. In addition, the CTIVD noted that the exchange of web forums takes place for which, in principle, the permission of the Minister should have been obtained. It has not conducted any further exhaustive investigation to find out whether any other unevaluated data has been provided to or received from foreign services. This was outside the remit of this investigation. (sections 5.3 and 6.3)

Safeguards for data received

The AIVD and MIVD receive unevaluated data from foreign services in the context of the aforementioned cooperative partnerships. In addition, the MIVD receives unevaluated data from foreign services based on lists of selectors supplied by the MIVD. The Committee observes that the same safeguards apply to unevaluated data received as to data gathered by the AIVD and MIVD themselves. After interception, the data is stored in the archives. The metadata is used for metadata analysis. The content data cannot automatically be used in the intelligence process and is not made available until it has been selected. Substantiated authorisation for selection, based on the selection criteria, must be requested from the Minister. This process is no different when receiving data from foreign services. The safeguards for the protection of privacy are the same. (sections 6.1 and 6.2)

Trust in the foreign service

The CTIVD notes that the AIVD and MIVD exchange unevaluated data with foreign services that, according to the AIVD and MIVD, all meet the criteria for cooperation, such as democratic anchorage, respect for human rights and reliability and professionalism. The CTIVD notes that the exchange of unevaluated data on a structural basis is an extremely far-reaching form of cooperation, in which trust in the foreign service with which cooperation takes place is assigned an important role. The CTIVD stated in a previous review report that the AIVD and MIVD may not take this trust for granted.

The assessment on the basis of the cooperation criteria must provide some insight into the boundaries of the trust that can be placed in the foreign service. The requirement of ministerial authorisation is particularly apt in this context. The required authorisation of the Minister may not degenerate into a rubber stamp (authorisation inflation). A substantive review must take place that forms an actual safeguard for the protection of privacy. The exchange of unevaluated data can only take place with foreign services that qualify for this form of cooperation. The AIVD and MIVD assess whether this is the case and whether they can trust that the foreign service complies with the legislation and regulations applicable to that service and with the arrangements made in the cooperative relationship. It is up to the Minister to evaluate whether this assessment, which is set forth in the weighting note, is correct. The Minister also assesses whether the exchange of unevaluated data fits within the framework defined in the weighting note, based on a statement of reasons focused on the foreign service and on that specific exchange. A two-fold assessment must therefore take place.

The CTIVD discusses this topic in its corresponding review report on the execution of House of Representatives motion no. 89 by members Schouw and Segers. The CTIVD observes in that report, among other things, that the policies of the two services and the practice of drawing up weighting notes devote no attention to the system of data protection of foreign services and that the exchange of

unevaluated data is only covered to a limited extent. As a consequence, the aforementioned review by the Minister under these circumstances can be regarded as of minor significance. The CTIVD provides guidelines for the AIVD and MIVD for the future drawing up of weighting notes and the improvement of previously established weighting notes so that the trust that is placed in foreign services can have a firm foundation and the review by the Minister can form a genuine safeguard for the protection of privacy. (Chapter 7)

Thus adopted by the CTIVD on 4 May 2016.

CTIVD no. 49

DEFINITIONS

of the review report on the exchange of unevaluated data by the AIVD and the MIVD

investigation into the execution of Dutch House of Representatives motion no. 96 (by member Schouw)

This list explains a number of terms used in the review report. In the descriptions provided, the CTIVD's aim was not completeness, but to try to give the reader as clear a picture as possible of the terms in question.

Assistance	The deployment of powers for a foreign service and at the latter's request. Such deployment does not take place in the context of the AIVD or MIVD's task execution, but in the interest of the foreign service (Article 59 (4) ISS Act 2002).
Bulk data	Large volumes of raw data.
Cooperative partnership	Cooperation based on arrangements made among three or more intelligence and/or security services, targeted at a particular topic, geographical area or technical knowledge.
Director (AIVD)	Officer at the AIVD positioned in the organisation's hierarchy as follows: director-general, *director*, head of unit, head of team.
Director (MIVD)	Officer in charge of the MIVD. At MIVD, the director is positioned in the organisation's hierarchy as follows: *director*, head of department, head of bureau, head of section.
Director-General (AIVD)	Officer in charge of the AIVD. The position in the organisation's hierarchy is as follows: *director-general*, director, head of unit, head of team.
Data processing	Collecting, recording, arranging, storing, updating, altering, demanding access to, consulting or using data, providing data by forwarding, dissemination or any other means of making data available, assembling or combining data, and protecting, deleting or destroying data (Article 1(f) ISS Act 2002). The mere act of gathering data is also referred to as data acquisition.
Data protection	Safeguards for the protection of data as evident from legal rules and practice, for instance concerning data processing, such as the storage and destruction of data.
Evaluated data	Data which has been assessed for relevance.
Exchange of data	The provision and reception of data.
Foreign service	An intelligence and/or security service of another country.
Hacking	Gaining access to a computerised device with the aim of acquiring or changing data.

Hard disk	The memory of a computer, for example, used to store data.
Head of bureau (MIVD)	Officer at MIVD who occupies the following position in the organisational hierarchy at MIVD: director, head of department, *head of bureau*, head of section.
Head of department (MIVD)	Officer at MIVD who occupies the following position in the organisational hierarchy at MIVD: director, *head of department*, head of bureau, head of section.
Head of unit (AIVD)	Officer at the AIVD positioned in the organisation's hierarchy as follows: director-general, director, *head of unit*, head of team.
Head of section (MIVD)	Officer at MIVD who occupies the following position in the organisational hierarchy at MIVD: director, head of department, head of bureau, *head of section*.
Head of team (AIVD)	Officer at the AIVD positioned in the organisation's hierarchy as follows: director-general, director, head of unit, *head of team*.
Intelligence service	A service that conducts investigations regarding other countries for the purpose of identifying (potential) threats to the service's own national security.
Interception	The interception of data.
Investigatory power	A power conferred on a service by law to use a specific method that infringes privacy, which provision of law also lays down the circumstances and conditions under which the power may be exercised. Investigatory powers are usually exercised in secret. The investigatory powers are set out in Articles 20-30 Intelligence and Security Services Act 2002 (e.g. interception and surveillance).
ISS Act 2002	Intelligence and Security Services Act 2002. This law is in force at the time of the investigation by the CTIVD.
ISS Act 20XX	Amendment of the Intelligence and Security Services Act 2002. In July 2015, the ISS 20XX Act Draft Bill was published for internet consultation. On 15 April 2016, the cabinet approved the bill. At the time of preparation of this report, the bill is awaiting the recommendation of the Council of State.
JSCU	Joint Sigint Cyber Unit, joint unit of the AIVD and the MIVD that processes data in the areas of Sigint and Cyber.
Metadata	Data about a communication session. The metadata of a telephone call, for example, comprises the telephone numbers involved, the starting and ending times of the call and the data of the mobile phone masts involved .
Metadata analysis	The process of looking for relevant links and data in a collection of metadata and of combining data already available (what/who has made contact with what/whom, for how long, how often, from where, etc.).
Motion no. 89	Motion no. 89 by members Schouw and Segers, adopted on 9 April 2014 following the debate in the Dutch House of Representatives, on interception by the NSA and the role of the Netherlands. The motion envisages more detailed implementation of the criteria for cooperation.

Motion no. 96	Motion no. 96 by member Schouw, adopted on 9 April 2014 following the debate in the Dutch House of Representatives, on interception by the NSA and the role of the Netherlands. The motion envisages making the exchange of unevaluated data with foreign services subject to ministerial authorisation and was adopted on 15 April 2014.
Partner service	A foreign service with which the AIVD or the MIVD has a cooperative relationship.
Personal data	Data relating to an identifiable or identified individual natural person (e.g. a name or a photograph).
Power to select	The power to select (i.e. examine content) non-cable bound communications (e.g. satellite connections) obtained by untargeted interception.
Security service	A service that conducts investigations into persons and organisations that potentially represent a threat to the continued existence of the democratic rule of law, or to security or other vital interests of the State, or to the security and readiness of the armed forces.
Selector	A criterion, for example a telephone number, based on which specific content data can be selected from a large volume of telecommunications data.
Target	A person or organisation that is being investigated by the AIVD or MIVD (Article 13 ISS Act 2002).
Targeted acquisition	Acquisition where the person, organisation or technical characteristic at whom/which the data acquisition is targeted can be specified in advance.
Task performance	The performance of the tasks as described in Article 6 (2) ISS Act 2002 (AIVD) and Article 7 (2) ISS Act 2002 (MIVD).
Technical characteristics	Characteristics traceable to various telecommunication elements, for example a telephone number, an e-mail, an IMEI number or an IP address.
Unevaluated data	Data which has not yet been assessed for relevance.
Untargeted acquisition	Acquisition where the person, organisation or technical characteristic at whom/which the data acquisition is targeted cannot be specified in advance.
Web forum	Digital discussion pages on the Internet. Some web forums require visitors to register in order to obtain access to the site. Usually, visitors can also exchange messages via these sites.
Weighting note	A document specifying the assessment of the extent to which a foreign service meets the cooperation criteria and which forms of cooperation are permitted.

Anna van Saksenlaan 50 | 2593 HT The Hague
T +31 (0)70 315 58 20 | **F** + 31 (0)70 381 71 68
E info@ctivd.nl | www.ctivd.nl