Review Report

On contributions of the MIVD to targeting

CTIVD no. 50

3 August 2016

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence and Security Services

CTIVD no. 50

REVIEW REPORT

on contributions of the MIVD to targeting

Table of contents

CTIVD no. 50

SUMMARY

of the review report on contributions of the MIVD to targeting

Background

The background to this report is the parliamentary debate that has been held in recent years on the potential use of Dutch intelligence for the unlawful use of force by other states. Through this report, the Dutch Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD) intends to provide insight into potential contributions of the Dutch Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) to targeting and the (un-)lawfulness thereof. The CTIVD's investigation was focused on the provision of data by the MIVD to foreign intelligence and/or security services (I&S services) from 1 January 2013 up to and including 31 December 2015 and the provision of data by the MIVD within the context of ongoing and recently concluded military missions.

Targeting and the MIVD

In this report, the term targeting refers to the process that can result in the (lethal) use of force by armed forces in order to achieve a strategic objective within the context of a (military) operation.

The MIVD's role in the context of a targeting process is to provide support. This concerns the provision of data that can contribute to this process. It is the MIVD's task to gather intelligence and to provide this intelligence to other bodies in the interest of national security, e.g. to the Dutch armed forces, to military coalitions in which the Dutch armed forces participate or to foreign I&S services. The MIVD itself is not authorised to use force.

The Dutch armed forces or a military coalition in which they participate can perform a targeting process, resulting in the lethal use of force, in a military operation. It can also happen that foreign I&S services perform this process or pass on the data received to other armed forces. In this way, the MIVD can make a contribution to a targeting process by providing data in various ways, directly or indirectly. This does *not* mean that such provision of data is automatically unlawful. However, this *is* the case when an unacceptable risk of a contribution to the unlawful use of force is being accepted when providing data. The Committee focused its investigation on this aspect.

A need for a clear framework

The above underscores the importance of a clear legal framework for cooperation of the MIVD with military coalitions and foreign I&S services in general and, within that cooperation, for the individual instances of data provision in particular. The Committee determines that the framework used to date by the MIVD is insufficiently focused on the risk that the MIVD can contribute involuntarily, by means of the provision of data, to targeting processes involving the unlawful use of force. This also makes it more difficult for the Committee to review the practice. This report provides a framework as well as guidance to the MIVD for its future actions. The policy of the MIVD must be brought into compliance with the legal framework below.

General assessment of cooperation with foreign intelligence and security services

The first step is for the MIVD to identify, for each foreign (military) I&S service, the risks involved in the cooperation in a so-called weighting note, including the contribution to the unlawful use of force by (the state of) the I&S service in ongoing armed conflicts. By means of the assessment of the cooperation criteria, the MIVD must record in writing which forms of cooperation (nature and intensity) are permitted on what conditions.

Assessment for each individual instance of data provision to foreign (military) I&S services

The second step is for the MIVD to test each individual instance of data provision against this weighting note and against the requirements of necessity, propriety, and due care set by law. In doing so, the MIVD must also take into consideration the extent to which this data can reasonably be used by the recipient party for targeting processes.

The MIVD must record its considerations in writing if it intends to contribute to a targeting process. This also applies when the MIVD does not intend to contribute to a targeting process but when it can be concluded on the basis of general empirical rules and/or the specific facts that the intelligence to be provided can be used for such a process. This can be the case when the state of the concerned foreign I&S service is actively involved in an ongoing armed conflict and the MIVD's provision of data to this service pertains to current data about persons of an armed group involved in that conflict.

In addition, authorisation must first be obtained from the Minister in the case of the provision of unevaluated data. Unevaluated data is data that has not yet been assessed for relevance to the performance of tasks (e.g. large quantities of metadata). The Minister's authorisation must also first be obtained in the exceptional case that personal data is provided to a foreign (military) I&S service that does not (yet) fulfil the cooperation criteria.

Furthermore, the MIVD must impose the following written conditions when providing (evaluated as well as unevaluated) data that can be related to the use of force by the state of the foreign I&S service:
1) the data may not be provided to others without express consent (third-party rule);
2) the data may not be used for purposes that entail a violation of international law.

In conclusion: Following the provision of data, the MIVD must remain alert to indications that this data has nevertheless contributed to targeting processes involving the unlawful use of force and actively enquire into the matter (*feedback loop*). If that is the case, then the results thereof must be included in the reconsideration of the weighting note pertaining to the foreign I&S service in question.

Assessment in the case of the provision of data to military coalitions

A comparable framework applies when providing data to a military coalition in which the Dutch armed forces participate. Moreover, this provision of data must be in conformity with what the government has reported to parliament concerning the nature and intensity of the participation of the Netherlands in the military coalition.

Practice: deliberate contribution to targeting by military coalitions

The Committee has established that the MIVD has purposefully contributed to a targeting process within the scope of two military missions by providing data relevant in that regard to a military coalition in which the Dutch armed forces participate or have participated. The Committee finds that the assessments made by the MIVD for these instances of data provision are in conformity with the legal requirements.

Practice: no deliberate contribution to targeting by or via foreign I&S services

The Committee has not found that the MIVD has purposefully provided data to foreign (military) I&S services for the purpose of targeting processes, outside the framework of military missions in which the Netherlands participates.

Practice: provision of evaluated data within the context of the use of force

The MIVD has nevertheless provided I&S services of states involved in the use of force in certain areas with *evaluated* intelligence related to that use of force, without intending to contribute to a targeting process. This concerned intelligence pertaining to one or more militant groups against which the armed forces of the state involved were fighting, among other instances.

The Committee found that, for individual instances of data provision, the MIVD must take into account, more explicitly than is currently the case, the possibility that these can involuntarily contribute to targeting processes that involve the unlawful use of force and better tailor the conditions for the data provision to that possibility, as indicated above.

Practice: provision of unevaluated data within the context of the use of force

The MIVD has also provided I&S services of states involved in certain regions in the use of force with *unevaluated* intelligence potentially related to that use of force. This concerned e.g. communication data originating from a region where the use of force was taking place. The Committee finds that the decision-making regarding the (un-)acceptability of a risk of contributing to the use of force by means of the provision of unevaluated data must take place explicitly by means of requiring the authorisation of the Minister. This must take into account what is set out in the weighting notes of the MIVD and the requirements imposed on these weighting notes by the Committee. The latter is not (yet) a full part of the MIVD's practice.

Practice: the use of intelligence provided for targeting processes

The Committee does not have concrete indications that the MIVD has accepted an unacceptable risk of a contribution to the unlawful use of force in providing (evaluated and unevaluated) data. However, the Committee cannot exclude that the intelligence provided by the MIVD to foreign (military) I&S services has been used by or via these services for targeting processes resulting in the unlawful use of force. This also applies to intelligence provided to military coalitions. After all, it is not possible for the Committee to investigate what exactly these parties have done with the data received. Nor does the Committee have the legal powers to do so. The Committee cannot answer the question of whether (lethal) force has been used as a result of data provided by the MIVD. In general, the foreign recipients of this data are not accountable in that regard. In its investigation at the MIVD, the Committee itself has not encountered concrete indications that data provided to foreign intelligence and security services (except for military missions in which the Netherlands participated) has been used for the (lethal) use of force.

Finally

Not even the application of the legal framework described above as preferable will in practice exclude the risk that data provided by the MIVD to foreign (military) I&S services is used for the unlawful use of force, without this being the intent of the MIVD. It can, however, significantly reduce the risk of this happening.

This report has **no** secret appendix.

CTIVD no. 50

REVIEW REPORT

on contributions of the MIVD to targeting

1 Introduction

The Dutch Review Committee on the Intelligence and Security Services (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten, CTIVD) has investigated contributions of the Dutch Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst, MIVD) to targeting. Even though targeting is an integral part of military action, it is in general a highly charged term due to the connection made with concepts such as *targeted killing* and *targeted strike*. These concepts are often connected with so-called *drone strikes*: targeted attacks on persons or objects by means of armed unmanned aircraft.[1] Drone strikes are also designated as "extrajudicial executions" and violations of international law by human rights organisations and in the media.[2] However, that assessment is not always easy to make in practice.

The potential use of Dutch intelligence for the unlawful use of force by other states has been discussed regularly in the Dutch House of Representatives in recent years.[3] With this report, the CTIVD intends to provide insight into:

- What targeting is
- The legal framework applicable to the MIVD's contributions to targeting;
- The potential contributions of the MIVD to targeting;
- The (un-)lawfulness of this.

The Committee has done so by means of the following investigative questions.

---

1 These are sometimes also referred to as unmanned aerial vehicles (UAVs).

2 See *Will I be next?* US Drone Strikes in Pakistan, Amnesty International 2013, available via www.amnesty.nl 2013; *Between a Drone and Al Qaeda*, Human Rights Watch 2013, available via www.hrw.org; S. Derix en H. Modderkolk, 'Doden met 'onze' data- mag dat?', *NRC Handelsblad* 10 March 2014; J. Gruiters, 'Blijf weg van inzet drones in Somalië', *Trouw* 5 April 2014; See also S.A. Ross, 'MPs call for guidance on prosecuting UK spies over US drone strikes: Tory and Labour MPs ask DPP to clarify how police should handle intelligence-sharing allegations after Snowden documents raised questions about GCHQ role', *The Guardian* 7 July 2015; C. Fuchs en T. Wiegold, 'Tod durch Nähe: Wurden Informationen deutscher Militärs von amerikanischen Killerkommandos missbraucht?', Die Zeit 8 January 2015. Otherwise: P. Ducheine & F. Osinga, '(On)duidelijkheid bij Drones', 68 *Internationale spectator* 2014-9, pp. 41-43; I. Roox, 'Ja, dit mag' (interview Prof. J. Wouters), *De Standaard* 14 November 2015.

3 See *Appendix to the Proceedings II* 2012/13, no. 843; *Appendix to the Proceedings II* 2013/14, no. 1710; *Appendix to the Proceedings II* 2015/16, no. 1177; *Parliamentary Documents II* 2013/14, 30806, no. 24, pp. 29 & 37-38; *Parliamentary Documents II* 2013/14, 33750-X, no. 57; *Parliamentary Documents II* 2013/14, 33750-X, no. 67, p 6; *Parliamentary Documents II* 2014/15, 29924, no. 115, pp. 20; *Parliamentary Documents II* 2013/14, 33750-V, no. 21.

Investigative questions

- What is targeting?
- What is the legal framework for contributions to targeting by the MIVD by way of data provision?
- Has the MIVD provided data in current and recently concluded military missions for the purpose of contributing to targeting and how does this relate to the legal framework?
- Besides the above-mentioned missions, has the MIVD provided foreign I&S services with data that can have contributed to targeting and how does this relate to the legal framework?

Framework-providing review report

The CTIVD has opted for a review report that provides a framework guiding the MIVD in its future actions and that makes possible an assessment of the practice in past years. The CTIVD does not assess the political desirability or lack thereof of possible contributions to targeting by the MIVD. This is not part of its oversight task. The emphasis of this report is on establishing a sound framework for contribution by the MIVD to targeting, including the legal boundaries in this respect.

Structure of the report

In **Chapter 2**, to achieve a good understanding of targeting, the CTIVD will first deal with the question of what targeting precisely entails and the MIVD's potential role in that regard. In **Chapter 3**, the CTIVD will explain the legal framework. The assessment of (potential) contributions of the MIVD to targeting will follow in **Chapter 4**. The CTIVD ends its report with conclusions and recommendations in **Chapter 5** and **Chapter 6**, respectively.

This report has three appendices. In **Appendix I**, the CTIVD discusses how it has performed its investigation. In **Appendix II**, attention has been devoted to the relevant international legal standards in addition to the legal framework in Chapter 3. A glossary has been included in **Appendix III**.

This report has **no** secret appendix.

2 The significance of targeting and the MIVD's role in that regard

2.1 Introduction

Targeting is a comprehensive term.[4] It is important for the Committee's investigation to give serious thought to the question of what targeting entails precisely and to what extent and in what manner the MIVD can contribute to that. The Committee answers these questions in this chapter.

2.2 The definition of targeting

There are different definitions of targeting in circulation. The Committee derives its definition from the description of the term "targeting process", as used by the North Atlantic Treaty Organization (NATO) as well as by the Dutch armed forces.[5] Based on this definition, targeting can be understood as *a process used by armed forces that can result (through selection of targets) in the use of force to achieve a certain tactical or strategic objective in the context of a military operation, among other outcomes*. As becomes manifest below (paragraph 2.4), this process and the use of force can also be performed by parties other than armed forces.

In the case of the use of force, an example is the use of lethal force against members of an armed group in order to weaken its offensive power. The use of force can also pertain to taking a person prisoner to limit the threat constituted by that person or to destroy an object for the purpose of terminating its use by an armed and organised group.

A term often giving rise to debate is *targeted killing*. This term relates to intentional and planned attacks using lethal force against one or more specific persons.[6] Whenever this report refers to the use of lethal force, it therefore pertains also to *targeted killing*.[7]

However, a targeting process can also result in actions that do not involve the (lethal) use of violence. For example, the dissemination of information for the purpose of influencing the opinions or ideas of certain persons.[8]

---

4 The term is also used in the context of (untargeted) interception of communication (*targeted/untargeted interception*). This meaning of the term is beyond the scope of this review. For this subject, see the legal appendix of 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.

5 *A cyclical process performed by armed forces in which targets are being selected and linked to suitable solutions in the context of military operations, taking into account the operational needs and own possibilities.* See Joint Doctrine Publicatie 5 (JDP-5), Commandovoering, Ministerie van Defensie (2012), p 128 (among others); Doctrine Publicatie 3.2 (DP 3.2), Landoperaties, Commando Landstrijdkrachten (2014), p 6-4; These Doctrine Publications are available via www.defensie.nl. For a definition of the term in an international context, see: P.R. Pratzer, 'The Current Targeting Process' in: Ducheine, Schmitt & Osinga, Targeting: *The Challenges of Modern Warfare*, Den Haag: T.M.C. Asser Press 2016, pp. 79-80.

6 See *Advies inzake bewapende drones* (advice July 2013, no. 23), Den Haag: Commissie van Advies Volkenrechtelijke Vraagstukken (CAVV) 2013, pp. 24-25; Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions, Philip Alston, VN Doc. A/HRC/14/24/Add.6, 28 May 2010, paras. 7-10.

7 *Targeted killing* is frequently associated with the use of armed unmanned aircraft (also referred to as drones). *Targeted killings* can, however, also be performed with other means of force (e.g. handguns, ballistic missiles, bombers, etc.).

8 See P.A.L. Ducheine, 'Non-kinetic Capabilities: Complementing the Kinetic Prevalence to Targeting' in: Ducheine, Schmitt & Osinga, Targeting: *The Challenges of Modern Warfare*, Den Haag: T.M.C. Asser Press 2016 pp. 201-230.

Due to the fact that the social and political-administrative discussion concerns targeting (processes) that involves the use of lethal force, the Committee has decided to focus its investigation on the **contributions of the MIVD to targeting processes in so far as this can give rise to the use of force, by armed forces or foreign I&S services, against persons and objects in the context of a (military) operation** (see appendix I).

2.3 Steps within a targeting process

The exact steps of a targeting process vary. They depend on the operation or mission in the context of which targeting is taking place, among other aspects. The crucial steps in the process are in any case: the selection of targets important to achieve successfully an objective of the operation or mission concerned and the assessment of which actions are lawful in that regard.[9] Intelligence plays an important part in this assessment. After all, intelligence plays a part in determining whether eliminating or capturing a target is lawful and contributes to achieving a mission's objective.

2.4 Which actors are involved in targeting?

In general, a targeting process involves armed forces (military units) that have the task and (national and/or international) powers to execute military operations. The commander of such an operation is in general responsible for the targeting process and the decisions made in that context. However, targeting is not reserved exclusively for armed forces. It can also happen that foreign I&S services, depending on the task and (national) powers assigned to them, perform targeting processes involving the use of lethal force. An example of such a service is the American *Central Intelligence Agency* (CIA).[10] This is *not* the case as far as it concerns the Dutch intelligence and security services (AIVD and MIVD). The tasks and powers in the Intelligence and Security Services Act 2002 (Wet op de Inlichtingen- en veiligheidsdiensten 2002, Wiv 2002) or ISS Act 2002 offer no leeway in that regard for the application of force by the MIVD (or the AIVD).[11] The Committee has not found indications that the services have acted outside the boundaries of the ISS Act 2002 in this respect.

2.5 Origin of the intelligence that can contribute to targeting

Intelligence that contributes to a targeting process can be gathered using means available to a military commander. This can be done using military resources or units on the ground, in the air, on and under water, and in (cyber-)space, for instance. In addition, other sources can play a role (e.g. open sources). It is also possible that (military) I&S services such as the MIVD can have gathered data through their investigations that can contribute to a targeting process. A military commander will make the necessary decisions on the basis of all the data that are provided (and that can originate from various sources).

---

[9] See Joint Doctrine Publicatie 5 (JDP-5), Commandovoering, Ministerie van Defensie (2012), pp. 128-130, available via www.defensie.nl.

[10] See 'Remarks of CIA General Counsel Stephen W. Preston at Harvard Law School, April 10, 2012' (www.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/cia-general-counsel-harvard.html), which refers to *Article II of the U.S. Constitution, specific congressional authorisations* and *Presidential Findings "in accordance with the covert action procedures of the National Security Act of 1947* for the legal foundation for the use of force by the CIA, among other foundationswww.cia.gov/news-information/speeches-testimony/2012-speeches-testimony/cia-general-counsel-harvard.html), waarin voor juridische grondslagen voor het gebruik van geweld door de CIA wordt verwezen naar onder meer ."

[11] See also *Parliamentary Documents II* 2000/01, 25 877, no. 72, p 23.

2.6 The MIVD's role in the context of targeting

The primary responsibility in the context of a targeting process resides with the body that makes the final decision about whether or not to act against a certain target. This body is also (legally) ultimately responsible for that decision. Hence, this responsibility resides in the operational domain (of which the bodies that execute the targeting processes - such as the armed forces - are a part) and not in the intelligence domain (of which the MIVD is a part). The MIVD's potential role in a targeting process must be seen as a supportive one, through the provision of data.

This supportive role manifests itself in the first place when the recipients of these data are bodies whose tasks and powers partially involve the use of force. This can be the Dutch armed forces or a military coalition in which the former is participating. In the second place, a contribution can be made to a targeting process when the MIVD provides data to a foreign I&S service with the power to use force or to an I&S service cooperating with foreign armed forces. After all, such a service can pass this data on for targeting processes.

The MIVD can purposefully contribute to a targeting process, by providing data aimed at contributing to decision-making on the use of force against a certain group, persons or objects. However, the service cannot always establish whether data provided for a certain purpose is used for a different purpose by or via a recipient party. In that context, the MIVD can also contribute involuntarily to a targeting process through data provision, therefore without being aware of it.

2.7 Data that can be used for targeting

All kinds of data can contribute to a targeting process. However, there is a specific category of data that is particularly suitable for this purpose, due to its direct applicability, topicality, and accuracy. This data can be used for decision-making by bodies in the operational domain. This could take the form of current data about the identification, location and/or behaviour of a leader of an armed and organised group.

2.8 Conclusion

Targeting pertains to more than just the use of lethal force against enemy targets. The dissemination of information in order to influence ideas can also be part of targeting, for instance. The Committee has focused its investigation specifically on the MIVD's contributions to targeting processes (purposefully or not), in so far as this can result in the use of force by armed forces or foreign I&S services, against persons and objects in the context of a (military) operation.

The role of the MIVD in a targeting process is a supportive one, namely through data provision. The MIVD itself does not have the power to use force on the basis of the ISS Act 2002.

3 The legal framework

3.1 Introduction

The preceding chapter has shown that the MIVD can make a contribution to a targeting process by providing data to foreign I&S services, the Dutch armed forces or a military coalition in which they participate.[12] However, when is a contribution of the MIVD to a targeting process lawful or unlawful? This question cannot be answered easily.

The fact that the provision of data by the MIVD is permitted must be put first. After all, the law does provide opportunities for doing so. This is not changed by the circumstance that this data can be used by others for a targeting process. After all, the use of force as a consequence of a targeting process can be lawful. It can happen that while the MIVD acts in conformity with the law when providing data, the recipient party uses this data for unlawful purposes. In itself, the provision of data can be unlawful if it involves accepting an unacceptable risk that this data provision will contribute to a targeting process involving the unlawful use of force.

The (un-)lawfulness of the use of force is often difficult to establish. After all, this requires knowledge of all the facts and circumstances of the case. These facts and circumstances are often known only to the party that is carrying out the targeting process and the ensuing use of force or that is having it carried out. In addition, the interpretation of international legal standards relevant to the targeting processes is subject to ongoing debate. For example about the answer to the question of under which circumstances a person loses the protection of international humanitarian law[13] and can therefore be attacked.[14]

International legal standards pertaining to targeting processes.

➜ **International Public Law Basis/International Public Law Mandate/Legal Basis**
A targeting process in which force is used by units of a state in or against another state (cross-border armed action) must in the first instance have a basis in international law. In general, this legal basis is referred to as an "international public law mandate" or "**international public law basis**". An international public law basis can consist of the approval of the state in which the use of force is taking place, of Security Council resolutions of the United Nations or of the right to (collective) self-defence. Without an international public law basis, the use of force of a state against or in another state is a violation of international law.

---

12 In the preceding chapter, the Committee has also indicated that the emphasis of its investigation was placed primarily on contributions of the MIVD to targeting processes in the context of decision-making concerning the use of force (see also Appendix I). Therefore, the legal framework is namely focussed on that.

13 See Appendix II, paragraph 2. A different name for this regulatory framework is the "law of armed conflict" or "law of war".

14 See e.g. J. Pejic, 'Extraterritorial targeting by means of armed drones: Some legal implications', *International Review of the Red Cross* 7 May 2015, icrc.org, DOI:10.1017/S1816383114000447; *United Nations, General Assembly, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, A/HRC/16/51 (22 December 2010), p.19-21, available via www.undocs.org/a/hrc/16/51.

➜ **When is the use of force permitted (which regulatory frameworks apply)?**
In addition, the regulatory framework that applies to the use of force itself is important: **international humanitarian law and/or the human rights regime**. These regulatory frameworks determine when the use of force is permitted.

➜ **When does international humanitarian law apply?**
International humanitarian law applies when there is an armed conflict.

➜ **When does an armed conflict exist?**
An armed conflict exists when states use force against each other. An armed conflict can also exist when force is used between one or more states on the one hand and armed groups on the other hand (or among such groups themselves). Not every use of force between one or more states on the one hand and armed groups on the other hand (or among such groups themselves) can be qualified as an armed conflict. This depends on the intensity of the use of force and the degree of organisation of the armed groups.

Hence, the rules of international humanitarian law apply when there is an armed conflict. These rules establish the circumstances under which a person or object can be attacked, among other aspects. As such, objects that are military targets can in principle be attacked, while civilians can only be attacked when they participate directly in hostilities.

➜ **States' use of force outside an armed conflict**
It can also happen that states use force outside armed conflicts. In that case, the rules of international humanitarian law do not apply. The **human rights regime**[15] is in that case applicable in its full extent. In comparison with international humanitarian law, this regime only allows for the use of lethal force in exceptional circumstances. This means that, in principle, it is not permitted to carry out a targeting process, with as outcome the use of force, outside an armed conflict.

See Appendix II for a more extensive description of international legal standards relevant for targeting.

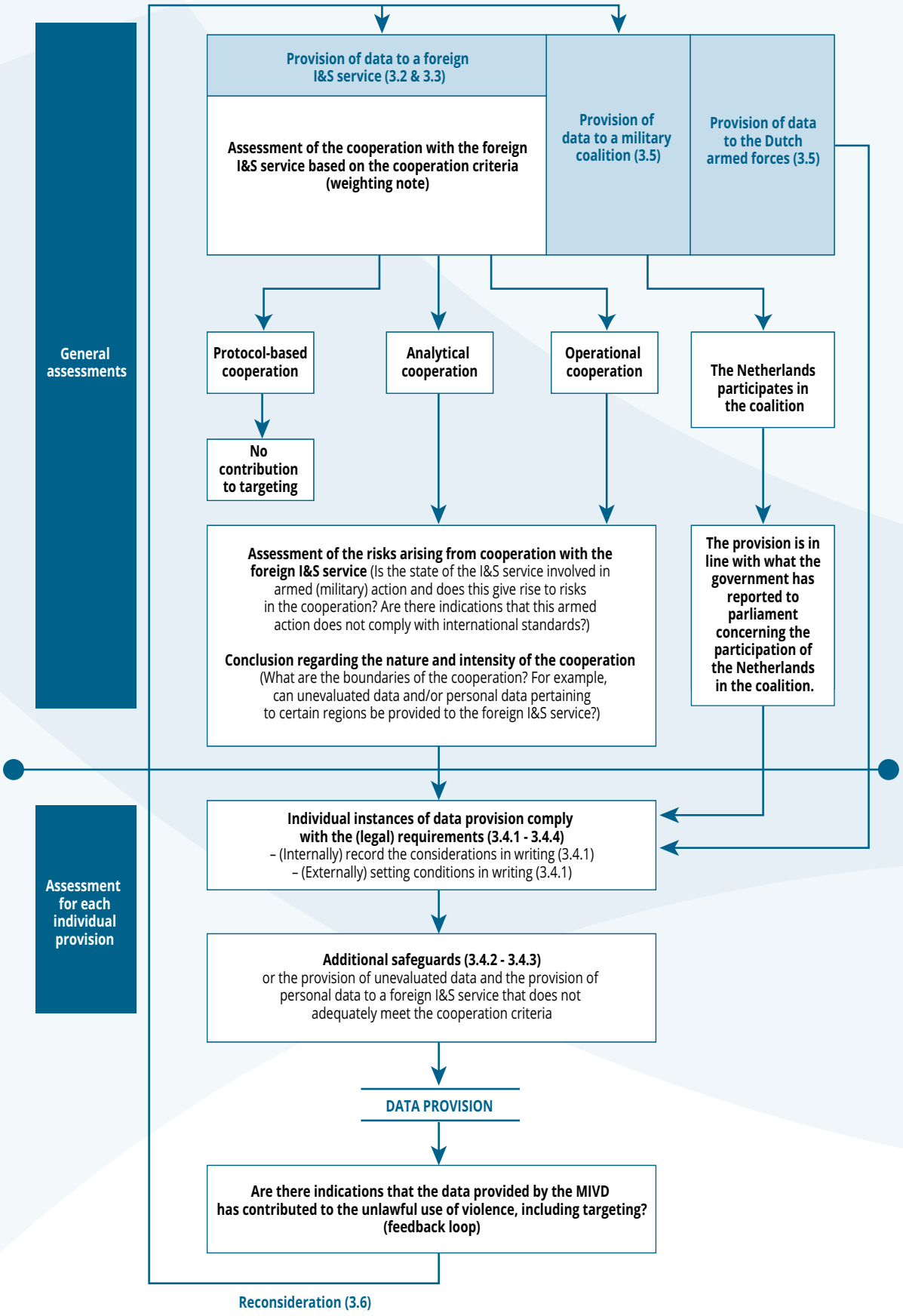
In view of the aforementioned, it is important to set out what can be reasonably expected of the MIVD from a legal perspective to prevent that a contribution is made, directly or indirectly, through data provision, to the unlawful use of force by others.

The Committee finds that these are rules pertaining to:

a) The general assessment of whether, and to what extent, the party to whom data is being provided can be cooperated with.
b) Assessments that must be made for each individual data provision.

[15] For example, standards of the European Convention on Human Rights (ECHR) and the International Covenant on Civil and Political Rights (ICCPR). See Appendix II.

This can be shown in a diagram as follows.



3.2 General assessment of cooperation with foreign intelligence and security services

The provision of data by the MIVD to a foreign I&S service is a form of cooperation. The ISS Act 2002 (and the legislative history) require that the MIVD first assesses, **before entering into a cooperative relationship**, whether this service qualifies for cooperation on the basis of **the cooperation criteria** and, if so, to what extent.[16]

The MIVD records the assessments made on the basis of these criteria in a **weighting note**[17], that constitutes the **framework for the cooperative relationship** with the foreign I&S service involved. The following are the cooperation criteria:

a) **Respect for human rights and democratic anchorage**
b) **Professionalism and reliability**
c) **Advisability in the context of international commitments**
d) **Enhancing the performance of tasks**
e) **Reciprocity**
f) **Legal powers and (technical) possibilities**
g) **Level of data protection**

These criteria are explained in more detail below.

a) Respect for human rights and democratic anchorage

In the context of the criterion of respect for human rights, a review takes place, for instance, of whether the service's state has ratified international human rights treaties and, if so, whether these human rights treaties are being observed in practice. Another important aspect is whether the foreign I&S service itself is or has been associated with human rights violations. Whether a service is sufficiently democratically anchored depends on a number of factors, such as the overall political system of the state in question and the position of the service within that system and (independent) oversight of it.

b) Professionalism and reliability

The extent to which a foreign I&S service can be regarded as professional and reliable depends largely on the experiences gained by the AIVD and the MIVD through the cooperative relationship with the service in question. When entering into a cooperative relationship, such views and experiences can be exchanged with other (friendly) I&S services. Moreover, the professionalism and reliability of a service are important factors when deciding to which extent the cooperative relationship can be intensified. In doing so, attention must be devoted to the extent to which a foreign I&S service respects the third-party rule.[18]

---

[16] See CTIVD Review Report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix).

[17] This is the document in which the MIVD records the assessment of the extent to which a foreign I&V service meets the cooperation criteria and which forms of cooperation are permitted.

[18] This rule states that data obtained by I&S services can only be passed on when authorised by the I&S service providing those data.

c) Advisability in the context of international commitments

For this criterion, the MIVD must consider whether the cooperation is advisable or not based on Dutch foreign policy and international commitments arising, for example, from membership of an international organisation or international treaties ratified by the Netherlands. The legislative history of the ISS Act 2002 shows that cooperation with certain foreign services can take on an additional dimension that requires explicit political decision-making. According to the legislator, it is imperative that such a situation be submitted to the relevant Minister for a decision and is not to be assessed solely by the head of the MIVD.[19]

d) Enhancing the performance of tasks

When entering into and maintaining a cooperative relationship with a foreign I&S service, the extent to which the cooperative relationship benefits or can benefit the performance of tasks by the MIVD (e.g. of ongoing investigations) must be examined.

e) Reciprocity

Cooperation with foreign I&S services takes place according to the principle of *quid pro quo* or reciprocity. This basic principle can be summarised as: "One good turn deserves another", and forms the basis for international cooperation in the world of I&S services. According to the legislative history of ISS Act 2002, requests for information from foreign I&S services must in principle be dealt with positively. This serves to continue to ensure that these services will do the same for information requests of the MIVD. This reciprocity therefore serves the national security, albeit indirectly. However, the principle of reciprocity has its limits, namely: there where the interests protected by the MIVD and the proper performance of tasks by the MIVD stand in the way.

f) Legal powers and technical possibilities

The MIVD must make sufficient efforts to identify the legal powers and gain as much insight as possible into the (technical) possibilities of the foreign I&S service.

g) Level of data protection

In the context of the assessment of whether personal data or unevaluated data[20] can be provided to the foreign I&S service, the MIVD must make efforts to identify the level of data protection (such as for storage and destruction) of the foreign I&S service.

Depending on the extent to which a foreign service meets the cooperation criteria, the MIVD establishes whether the cooperation will be protocol-based, analytical and/or operational. This means, respectively, maintaining contacts (protocol-based), the exchange of data that provides an insight into the current level of knowledge of the service (analytical) and forms of cooperation that provide insight into the methods or sources of the service or where joint operations or the exchange of personal data are involved (operational).

---

[19] *Parliamentary Documents II* 1999/2000, 25 877, no. 8, p 102.

[20] CTIVD Review Report no. 49 on the exchange of unevaluated data by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix). This is data that has not yet been assessed for relevance to the performance of tasks by the MIVD, such as large quantities of metadata. Evaluated data has been assessed for relevance to the performance of tasks. Where the committee does not explicitly refers to evaluated or unevaluated data, it is referring to both evaluated and unevaluated data.

The result of the assessment based on cooperation criteria must also clarify the risks that can be engendered by the cooperation and the forms (intensity) of the cooperation, including the exchange of personal data[21] and unevaluated data (see also paragraph 3.4.3), that are permitted and under which conditions.

In this manner, the weighting note indicates the boundaries of the cooperation between the MIVD and the foreign I&S service involved. The starting point is for the MIVD to stay within these boundaries in its cooperation with the foreign I&S service concerned. This can be deviated from only in exceptional cases (e.g. due to a compelling operational interest). The legislative history of the ISS Act 2002 provides an example of this, namely the provision of data that is inevitable to prevent terrorist attacks on innocent victims.[22]

The Committee refers to its Review Report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD for a more extensive description of the legal framework for the implementation of the cooperation criteria (among other aspects).[23]

3.3 General assessment of cooperation with foreign intelligence and security services in the context of targeting

As already explained above, the weighting note must show the risks that can be engendered by the cooperation and the conditions under which certain forms of cooperation (such as the provision of personal data and unevaluated data)[24] are permitted. This means that the MIVD must also assess whether (the state of) the concerned foreign I&S service is involved in the use of force in the context of armed conflicts or a comparable use of force and, if so, whether this can give rise to risks related to data provision, in the sense that the use of this data can lead to a violation of international legal standards. An example of such a risk is the existence of indications that there is no international public law basis for the use of force by the concerned state or that the applicable regulatory frameworks (e.g. international humanitarian law) is insufficiently complied with. The *track record* of the concerned state is also important. Does the state apply e.g. the same interpretations of relevant international legal standards as the Netherlands does? Is there adequately effective supervision and accountability? In addition, the history of cooperation between the MIVD and the concerned I&S service is important. Can it be assumed that the service will abide by the conditions for data provision set out by the MIVD?

Depending on the outcome of the above-mentioned considerations, a condition can be included in the weighting note stipulating that no data or only data that is subject to additional conditions can be provided by the MIVD to the concerned I&S service where it concerns data that can support the use of force due to their topic.

---

[21] According to the ISS Act 2002, personal data is data relating to an identifiable or identified individual natural person.

[22] *Parliamentary Documents II* 25877, no. 59, p 16.

[23] See CTIVD Review Report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), pp. 5-14 (appendix), available at www.ctivd.nl.

[24] Unevaluated data is data that has not yet been assessed for relevance to the performance of tasks (e.g. large quantities of metadata).

In practice, not all cases will lend themselves to a straightforward determination of whether there is an armed conflict and an international public law basis for the use of force by another state.[25]

The states involved will in general think that there is an armed conflict and that there is an international public law basis for the force used by them. States (even friendly ones) can disagree among themselves in that regard.[26] The Committee therefore deems it advisable for the MIVD to seek legal advice on this issue in the event of uncertainty. For example, from the Legal Affairs Department of the Dutch Ministry of Defence and/or via this ministry from the Dutch Ministry of Foreign Affairs if necessary. The same applies to the question of whether a state is adequately observing the applicable regulatory frameworks when using force against another state and/or militant groups.

The consequence of the foregoing is that, in the cooperation with foreign I&S services, the general assessments must already include the assessment of the risk that the MIVD's cooperation will contribute to targeting processes involving the unlawful use of force. It can be necessary already at this stage to restrict the boundaries within which the cooperation with the I&S service can take place. For example, because there is an unacceptable risk that the data provision, directly or indirectly, will contribute to the unlawful use of force.

3.4 Assessments of individual instances of data provision

The preceding paragraph shows that the MIVD can provide data to a foreign I&S service, depending on the form of cooperation permitted in the weighting note (and associated conditions). The legal basis in that regard is formed by Article 36 of the ISS Act 2002 (provision in the context of the proper performance of tasks) and Article 59 of the ISS Act 2002 (provision in the interest of the foreign I&S service).[27]

3.4.1 Legal requirements: data processing

According to the ISS Act 2002, data processing entails "*each action or a series of actions pertaining to data*."[28] This also means the provision of data. The ISS Act 2002 imposes requirements on data processing (including therefore data provision).

These requirements entail that each individual data provision must take place for a specific purpose and only to the extent that it is necessary for the proper implementation of the Act (Article 12 (2)), among other requirements. On the one hand, this means that the purpose must fit in with the framework of the Act. On the other hand, there must be a reasonable expectation that the provision of data will contribute to achieving that purpose.

---

[25] According to the government, there must always be an international public law basis for the deployment of the Dutch armed forces (*Parliamentary Documents II* 2006/07, 29 521, no. 41). In addition, the deployment of the Dutch armed forces abroad, in the context of a coalition or not, involves political decision-making in which the parliament is informed and consulted (informally) (par. 3.5).

[26] See e.g. *Appendix to the Proceedings II* 2012/13, no. 843 (answers of the Minister of Foreign Affairs to questions of Van Bommel (SP) and Van Dijk (SP) about the lawfulness of and accountability for *targeted killings*). In his answers, the Minister indicates that there is a difference of opinion between the USA and many other states, including the Netherlands, about the applicability of the laws of war and the right to self-defence in connection with the use of *drones*, among other aspects.

[27] For a more extensive description of the legal framework for data provision (and data processing in general) in this context, the Committee refers to the legal appendix to its review report 22b on cooperation between the MIVD and foreign I&S services (*Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl).

[28] Article 1 (f) of the ISS Act 2002.

Furthermore, the ISS Act 2002 requires that data provision takes place with due care (Article 12 (3) of the ISS Act 2002). This primarily relates to the safeguard that the data provided by the MIVD can be corroborated by data underlying those data. Furthermore, the data must bear an indication of the degree of reliability of the data or a reference to the source or the documents from where the data have been derived (Article 12 (4) of the ISS Act 2002).

Finally, the provision of data by the MIVD must be proper (Article 12 (3) of the ISS Act 2002). The propriety test is especially important in the context of targeting, due to the potentially drastic consequences that can arise from the data provision. The term propriety in any case entails an assessment being made between the purpose that the data provision intends to achieve and the (potentially) negative consequences thereof for the persons to whom (or objects to which) the data pertains: the so-called proportionality test. Here, a distinction must be made between data provision aimed at contributing to a targeting process and data provision that serves another purpose.

The purpose of data provision aimed at contributing to a targeting process (purposeful contribution) is to provide the decision-makers in a targeting process with relevant information. In the context of the necessity test, the MIVD will have to consider for each data provision whether that data provision for a targeting process (in view of the tasks) is in the interest of national security *and* remains within the boundaries of cooperation specified in the relevant weighting note(s). In the context of the propriety test, the MIVD will subsequently have to consider whether the consequences of such a contribution (a person is e.g. selected as a target partially as a result of the data provision) are in proportion to the purpose of the data provision (provision of intelligence to the decision-makers in a targeting process). This is the case at one end of the spectrum when e.g. the data to be provided pertains to objects that or persons who can potentially be designated as targets that can be lawfully attacked in the context of a military operation.[29] In that case, such a data provision contributes to the lawfulness of the use of force under international humanitarian law, provided the provision meets the requirement of due care. After all, qualitatively sound intelligence can contribute to establishing the degree of certainty of whether a target can be designated as a military objective within the meaning of international humanitarian law.[30] At the other end of the spectrum, the propriety test can result in the MIVD refraining from data provision. For example, because the data originates from an unreliable source and cannot be verified or is not supported by other data.

The Committee finds that the assessments made by the MIVD, in the context of the legal requirements for data provision aimed at contributing to a targeting process, must be recorded internally in writing.

When the MIVD's explicit objective for the data provision is *not* a contribution to a targeting process, the aforementioned considerations apply just as much when there is a real possibility (risk) that this data provision will contribute to a targeting process, on the basis of general empirical rules and/or the facts and circumstances of the specific case, as well as in view of the nature of the data provision.

This risk is especially present when the data to be provided pertain to a topic of which it is known that it is related to the ongoing use of force by the state of the I&S service to which the data are being provided *and* the Netherlands itself is not involved in that use of force.[31] The Committee finds that, for

---

[29] A target that can lawfully be attacked is e.g. (in the case of an armed conflict) a person who can be attacked in accordance with international humanitarian law (see Articles 35-58 of the Additional Protocol to the Geneva Conventions of 12 August 1949 relative to the Protection of Victims of International Armed Conflicts adopted in Bern on 8 June 1977 (Protocol I). See also Appendix II, paragraph 2.

[30] See Appendix II, paragraph 2.3.

[31] This risk is present to a lesser extent when the Netherlands itself is involved in the use of force. As such, according to the government, there must always be an international public law basis for the deployment of the Dutch armed forces (*Parliamentary Documents II* 2006/07, 29 521, no. 41) as well as insight in the scope and nature of the applicable power to use force.

such provisions of data, the MIVD must always attach the written condition for the recipient party that this data may not be used for purposes that entail a violation of international law.

It is not unusual to attach external conditions to the provision of data.[32] According to (Article 37 of) the ISS Act 2002, in all cases of data provision to foreign I&S services, the MIVD must set as a condition that these services may not pass on the data received to others (the so-called third party rule). Foreign I&S services may only pass on data they received from the MIVD to other parties, such as armed forces, when the Minister of Defence or the director of the MIVD has granted permission to do so.

While setting conditions does not guarantee that the data received from the MIVD will be used exclusively for lawful purposes, the Committee is of the opinion that professional and reliable I&S services can be expected to a certain extent to respect these conditions. This element is reflected in the general assessment of the nature and intensity of a cooperative relationship with a foreign I&S service (see paragraph 3.2). After all, the cooperation criteria of reliability and professionalism result in the MIVD assessing, prior to and periodically during the cooperation, the extent to which the concerned I&S service is sufficiently reliable and the extent to which it will respect agreements.

3.4.2 Legal requirements: provision of personal data

The ISS Act 2002 also has a number of specific provisions on the provision of data. As such, additional requirements apply in any case to the provision of personal data. This must be done in writing if the recipient is authorised to take measures against the person or organisation in question as a result of that data provision. Furthermore, a record must be kept of the provision of personal data by the MIVD.[33] Finally, in principle and as a result of the general assessments (see paragraph 3.2), personal data can only be provided to a foreign I&S service when operational cooperation is permitted according to the weighting note. The weighting note must also show the circumstances under which the MIVD can provide such data to the concerned foreign I&S service. In the exceptional case that it is deemed necessary to provide personal data to a foreign I&S service that does not adequately meet the cooperation criteria, the Committee finds it important that the authorisation of the Minister is obtained prior to the provision of personal data.[34]

3.4.3 Safeguards for the provision of unevaluated data

The aforementioned (legal) requirements also apply to the provision of unevaluated data. In the case of such data provision, the theme or geographical region to which the data exchange will pertain is agreed upon with the foreign I&S service. However, the assessments in that regard are not always easy to make, in comparison with the provision of evaluated data. These assessments do not have the same depth as they often concern large quantities of data that has not yet been assessed for its relevance to the performance of tasks by the MIVD. The provision of unevaluated data also implies that the MIVD does not know exactly which data is being provided. Moreover, the intended goal of such data provision is often general in nature. However, the (legal) requirements described above must be applied as much as possible.

---

[32] See also Born, Leigh & Wills, *Making International Intelligence Cooperation Accountable*, Printing Office of the Parliament of Norway 2015, p 113-114.

[33] Article 42 of the ISS Act 2002.

[34] See CTIVD Review Report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), p 10.

Following a motion adopted in the Dutch House of Representatives in 2014[35] on the interception by the NSA and the role of the Netherlands in this activity, the Minister of the Interior and Kingdom, partly on behalf of his colleague from the Ministry of Defence, has indicated that the authorisation of the Ministers will be required from now on for sharing unevaluated data.

The provision of unevaluated data can only take place with foreign I&S services that qualify for this form of cooperation. This means in any case that the relevant weighting note must show that operational cooperation with the concerned foreign I&S service is a possibility and that there is therefore a significant degree of confidence in the foreign I&S service.

In its review report (no. 49) on the exchange of unevaluated data by the AIVD and the MIVD, the Committee has stated that is important for the Minister to review whether the assessment laid down in the weighting note is correct.[36] The Minister also assesses whether the exchange of unevaluated data fits in with the framework laid down in the weighting note.

The possibility of the MIVD contributing to a targeting process by providing unevaluated data to a foreign I&S service emphasizes the importance of the weighting note properly specifying whether (the state of) the concerned foreign I&S service is involved in the ongoing use of force and, if so, whether cooperation can therefore give rise to risks. An example of such a risk is the unintentional contribution to targeting processes involving the unlawful use of force.

3.4.4 The role of the weighting note in individual instances of personal data provision

The aforementioned shows that the weighting note is the foundation for every data provision. The risks named in the weighting note pertaining to the cooperation with the concerned foreign I&S service must be taken into consideration for every provision of data. It must be assessed whether it concerns a situation in which a risk discussed in the weighting note is applicable and whether the data provision remains within the boundaries of cooperation established in the weighting note. If that is not the case, data provision can (as mentioned earlier) only take place when a compelling operational interest outweighs the risks of this data provision.

3.5 Provision to the Dutch armed forces and/or military coalitions

As apparent from the text of Article 36 of the ISS Act 2002, data can also be provided to parties other than foreign I&S services in the context of a proper performance of tasks. When the MIVD makes a contribution to a targeting process, this entails data provision to the Dutch armed forces or a military coalition in which they participate. For that matter, this is the **only legal basis** for the provision of data to the Dutch armed forces or a military coalition in this context. In addition, data provision to the Dutch armed forces or a military coalition is fully subject to the (legal) requirements regarding data provision described above.

When the Dutch armed forces, whether in a coalition or not, are deployed in the context of a military mission abroad, this is generally preceded by a political decision-making process, in which the

---

[35] *Parliamentary Documents II* 2013/14, 33 820, no. 2, p 6.

[36] CTIVD Review Report no. 49 on the exchange of unevaluated data by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), p 29.

government informs and informally consults with the parliament.[37] This involves a so-called article-100 procedure (named after Article 100 of the Dutch Constitution) or a comparable procedure.[38]

The letter with which the government informs the parliament of the deployment of the armed forces in the context of the article-100 procedure is referred to as the **article-100 letter**. In that case, the government's decision to deploy the Dutch armed forces is made based on the so-called Assessment Framework[39] for the consultation with parliament. The focal points of this assessment framework include the international public law basis and military aspects, such as the manner and purpose of the use of force by the coalition and the protection of the civilian population, as well as political considerations concerning the participation of the Netherlands in the coalition and the limitations in that regard. In general, an article-100 letter will not deal explicitly with the potential role of the MIVD. When the deployment of the armed forces falls outside the scope of Article 100 of the Constitution, the government will inform parliament as soon and extensively as possible.[40]

The aforementioned shows that a deployment of the Dutch armed forces in the context of a coalition will involve a governmental decision about which information is provided to parliament. The Committee finds that the provision of data to a military coalition in which the Netherlands participates must be in agreement with that what the government has reported to parliament about the participation of the Netherlands.

3.6 Feedback loop

If the MIVD provides evaluated or unevaluated data related to the use of force by (the state of) the recipient party, then it must pay attention to the (un-)lawfulness of that use of force also after the data has been provided. When there are suspicions that data provided have contributed, directly or indirectly, to the unlawful use of force (reports from human rights organisations or the media can be indicators of such use), then the MIVD must actively investigate whether the data provided has potentially contributed to that use (a so-called *feedback loop*). If there are concrete indications of such unlawful use, then this must be taken into account in (the extent of) the cooperation with the concerned party through reconsideration.

---

37 P.A.L. Ducheine & K.L. Arnold, 'Besluitvorming bij cyberoperaties', *Militaire Spectator* 2015-2, p. 56-70, available via www.militairespectator.nl.

38 According to Article 100 of the Dutch Constitution, the government must in principle inform parliament in advance when it plans to deploy the armed forces to promote or maintain the international legal order, or to provide assistance in the case of an armed conflict. The letter with which the government fulfils this constitutional obligation is referred to as the "article-100 letter". Article 100 does not apply to the Dutch participation in international missions on the basis of Article 5 of the North Atlantic Treaty, Article 42.7 of the Treaty on European Union or Article 51 of the United Nations Charter. However, if such situations also involve promoting or maintaining the international legal order, the government will also inform the parliament in accordance with the article-100 procedure (*Parliamentary Documents II* 2013/14, 29 521, no. 226).

39 This is the practical description of the application of Article 100 of the Constitution.

40 As such, the article-100 procedure will be applied similarly in the case of a deployment of the armed forces in the context of alliance obligations, such as those of NATO and the EU (*Parliamentary Documents II* 2004-05, 27 925, no. 170). For that matter, a separate decision-making and information provision procedure applies for special military operations involving significant political and military risks as well as a necessity for strict confidentiality (*Parliamentary Documents II* 1999-2000, 26 800 x 46, no. 2, p 2).

3.7 Conclusion

In its cooperation with foreign I&S services, the MIVD must first thoroughly assess whether and, if so, to what extent it can cooperate with a foreign I&S service and what the associated risks and conditions must and can be. In doing so, it must also expressly take into account the (un-)lawfulness of a potential use of force by (the state of) the foreign I&S service, in the context of previous or ongoing armed conflicts or a comparable use of force, among other aspects. In this assessment, attention must be devoted to the existence of an international public law basis for the use of force by a state in or against another state (cross-border armed actions) and the compliance with the regulatory frameworks (international humanitarian law and/or the human rights regime). This applies in particular when the Netherlands is not involved in this use of force or, in the case of an armed conflict, when the Netherlands is not a party to the conflict.

Next, the MIVD must apply stringently the legal requirements pertaining to the individual instance of data provision itself. When there are concrete indications that the data provided has contributed, directly or indirectly, to an unlawful use of force (the so-called feedback loop), then the MIVD must reconsider the nature and intensity of the cooperation with the concerned I&S service, as shown by the weighting note.

Data provision to military coalitions in which the Netherlands participates is subject to a comparable framework. In addition, the data provision must be in agreement with what the government has reported to parliament about the nature and intensity of the participation of the Netherlands in the coalition, whether via a so-called article-100 letter or not.

According to the Committee, the legal framework described in this chapter constitutes the key to what can reasonably be expected of the MIVD to prevent data provision from contributing to targeting processes that lead to the unlawful use of force by others. It must therefore be guiding for future actions.

4 The policy and practice

4.1 Introduction

The MIVD frequently exchanges data with foreign I&S services.[41] The content of this data varies. It can concern general intelligence reports about certain themes or trends as well as specific information about persons or organisations.

In addition, the MIVD also provides data to the Dutch armed forces or military coalitions in which they participate. In general, the data concerns information that can contribute to the safety of coalition troops or the successful continuation of a military mission.[42] As indicated earlier in Chapter 2, all types of data can in principle contribute to a targeting process.

In a number of close and long-term cooperative partnerships with foreign I&S services, the MIVD provides structural data that has not (yet) been assessed for its relevance to the performance of the tasks by the MIVD itself. This is so-called unevaluated data.[43] The MIVD does not know exactly which information is being provided in the case of such data. For this reason, this data is often also designated as "raw data" or "bulk data". This can pertain to the content of all communications and or the corresponding metadata.[44] Which unevaluated data is provided by the MIVD depends on the topics concerning which I&S services have decided to work together within a cooperative partnership. The exchange of unevaluated data does not necessarily entail the provision of the content of all communication sessions and all corresponding metadata to foreign I&S services. The provision of unevaluated data can e.g. pertain exclusively to telephone numbers and times of telephone calls in a certain region.

It is important for the MIVD to provide (evaluated or unevaluated) data if this limits the risk to Dutch national security interests. These interests include in the first instance the safety and effectiveness of Dutch military personnel or coalition troops during missions.

In this chapter, the Committee examines the practice in view of deliberate and unintentional contributions by the MIVD to a targeting process. First, the Committee will discuss and assess the relevant policy. It will subsequently examine the relevant practice.

4.2 Policy

The MIVD has drawn up a (general) policy in respect of international cooperation. In this policy, it is made clear that, before cooperating with a foreign I&S service, a weighting note must be drawn up in which is included if and, if so, to what extent the service in question meets the cooperation criteria. The note must also describe the themes on which will be cooperated and what the authorisation framework looks like at the service that is a potential cooperation partner, among other aspects. The weighting

---

41 See CTIVD Review Report no. 22b on the cooperation of the MIVD with foreign I&S services. *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl.

42 See e.g. CTIVD Review Report no. 44 on two operations performed by DISS (MIVD) to support the Dutch efforts to combat piracy in the Horn of Africa, *Parliamentary Documents II* 2015/16, 29 521, no. 305 (appendix), available at www.ctivd.nl.

43 In this context, see also CTIVD Review Report no. 49 on the exchange of unevaluated data by the AIVD and the MIVD, Parliamentary Documents II 2015/16, 29 924, no. 142 (appendix) and 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), paragraph 5.4. Both are available at www.ctivd.nl.

44 This is data about communication sessions (such as the concerned telephone numbers, the starting and ending times of a call, and data about the transmission mast)

notes must be re-assessed at least once every two years. A change in the cooperation, current events or political decision-making can give rise to an earlier modification. The policy also deals with the internal authorisation structure. It determines which executive is authorised to grant authorisation for certain forms of cooperation and when authorisation must be obtained from the director and/or the Minister, among other aspects.[45]

Furthermore, the policy also covers the provision of data in respect of armed conflicts. To briefly summarise, this policy stipulates that additional requirements apply if the MIVD deems it *likely* that data can be used directly for military actions in an armed conflict, including executing a targeting process. Those requirements entail refraining from data provision in principle if the Netherlands finds that there is no international public law basis for the participation of the recipient in that armed conflict and deems it *likely* that the recipient is using the data for the purpose of the use of force in the context of that armed conflict. When in doubt, the advice of the MIVD's legal department must be sought regarding the question of whether and, if so, which data can be provided. This question is then submitted to the director of the MIVD to decide on the matter.

Finally, the MIVD has a specific (*ad hoc*) policy pertaining to the provision of evaluated data for the purpose of contributing to a targeting process (deliberate contribution) in the context of two military missions in which the Dutch armed forces are participating or have participated (see paragraph 4.3).

Regarding the (general) policy on international cooperation of the MIVD, the Committee has observed in its review report on the implementation of cooperation criteria by the AIVD and the MIVD that it is in conformity with the regulation as laid down in the ISS Act 2002.[46] However, the Committee reached additional conclusions. As such, it concluded that the policy is not extensive enough where it pertains to the exchange of unevaluated data and the cooperation with foreign I&S services that do not meet the cooperation criteria. Moreover, more attention must be devoted to the powers and (technical) possibilities of the foreign I&S services. Furthermore, the policy fails to mention the level of data protection as a topic to be addressed in the weighting notes.

In addition, in its review report on the exchange of unevaluated data by the AIVD and the MIVD, the Committee has concluded that the MIVD has not defined in its policy what must be understood by the term "unevaluated data" and when authorisation must be obtained from the Minister. The Committee deemed it important for the AIVD and the MIVD to adopt a structured policy in the area of unevaluated data.[47] Moreover, the Committee deemed it necessary that the authorisation of the Minister for the exchange of unevaluated data must be tied to an authorisation period of e.g. one year.[48]

The MIVD does not devote explicit attention in the weighting notes to the use of force by (the state of) the foreign I&S service. In view of the legal framework discussed in Chapter 3, the Committee finds that the MIVD must assess whether (the state of) the foreign I&S service in question is involved in the use of force in the context of armed conflicts or in a comparable use of force outside those conflicts and, if so, whether this can give rise to risks in connection with data provision. The Committee recommends that the MIVD clearly shows in its policy and the weighting notes that this assessment must be made for each foreign I&S service. This is currently not the case.

---

45 For a more extensive description of the MIVD's policy on international cooperation, see CTIVD Review Report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), pp. 24-34 (appendix), available at www.ctivd.nl.

46 CTIVD Review Report no. 48 on the implementation of cooperation criteria by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), p 27, available at www.ctivd.nl.

47 CTIVD Review Report no. 49 on the exchange of unevaluated data by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), pp. 17-18 available at www.ctivd.nl.

48 Idem, p 25.

In addition, the Committee finds that the policy on data provision in respect of armed conflicts is too limited. It makes the following recommendations in that regard:

- The policy does not devote attention to the provision of data that can contribute directly to the use of force by states against militant groups outside armed conflicts.[49] In that case, international humanitarian law does not apply. The legal framework in Chapter 3 and Appendix II to this report shows that executing a targeting process resulting in the use of force in such situations is lawful only in exceptional cases. The Committee recommends devoting attention in the weighting notes to such use of force (if the Netherlands is not involved). The same applies to the degree of compliance with international humanitarian law by a party in an armed conflict in which the Netherlands itself is not a party.

- The policy does not provide an answer to the question of when the MIVD deems it likely that the recipient party is using data for the use of force in the context of an armed conflict. The Committee recommends a (more) concrete implementation thereof.

The Committee finds that the policy of the MIVD is currently insufficiently focused on the risk that the MIVD can contribute involuntarily, by means of the provision of data, to targeting processes involving the unlawful use of force. This made it more difficult for the Committee to review the practice.

4.3 Practice: provision of data in the context of military missions

In view of the tasks of the MIVD, the service frequently provides data in the context of military missions in which the Dutch armed forces participate. In the course of its investigation, the Committee found two military missions in which the MIVD provided data for the purpose of contributing to a targeting process. This concerns an already-concluded mission: the *International Security and Assistance Force* (ISAF) in Afghanistan, and a mission that is still ongoing: Operation *Inherent Resolve* (the fight against the Islamic State in Iraq and Syria (ISIS)).

4.3.1 Contribution to the targeting process during the ISAF mission

In the period that the Dutch armed forces were present in the Afghan province of Uruzgan (*Task Force Uruzgan, 2006-2010*), the MIVD nominated persons for inclusion in the list of targets to be attacked by the ISAF coalition, in addition to the usual intelligence support for the armed forces. The MIVD's purpose was to support a Dutch ISAF unit in eliminating leaders of enemy groups in Afghanistan.

In this context, the MIVD had adopted a specific internal procedure. According to this procedure, the approval of such a nomination required the consent of (consultation) bodies formed within the MIVD and of the director of the MIVD. The nomination was subsequently presented to the Secretary General of the Dutch Ministry of Defence, who in turn received legal advice from the legal affairs department of that ministry. If the Secretary-General also approved the nomination, the MIVD would send a more extensive version of the nomination to the commander of a Dutch ISAF unit in the area of operations. The latter could introduce the nomination in the selection process for targets to be attacked by the ISAF. The decision-making procedure with regard to the actual selection and attack of a target was an ISAF matter and was outside the purview of the MIVD.

---

[49] For example, in 2007, the Dutch government found that the situation in Afghanistan could in general not be labelled as an armed conflict between the ISAF and enemy groups present there, but that there could potentially be "a participation limited in time and scope in an armed conflict". *(Parliamentary Documents II* 2007/08, 27 925, no. 287, pp. 144-145).

The MIVD kept files on the nominated targets. The MIVD would decide to nominate a target for inclusion in the above-mentioned ISAF list depending on the estimated impact of an attack on that target. The nomination contained information about the background and the role of the target, the grounds for justification of the attack, and its intended effect. The more extensive version of the nomination sent to the commander of the ISAF unit also contained an overview of the relevant intelligence. On the basis of that overview, the MIVD itself would (also) review whether the target could be designated as a lawful military objective.

The Committee observes that the MIVD provided evaluated (personal) data to the ISAF in accordance with the procedure described above. This pertained to nominations of persons who belonged to an enemy group.

- *Assessment*

As stated above, the Netherlands was part of the ISAF coalition. There was also an article-100 letter of the government with regard to the ISAF. The Committee finds that the aforementioned contribution by the MIVD to the targeting process is in line with the content of the article-100 letter in question.[50]

In 2012, the Committee explored the contribution of the MIVD to the elimination of targets in Afghanistan. It studied the procedure adopted by the MIVD and the nominations, among other aspects. At the time, the Committee presented its findings ensuing from this exploration to the director of the MIVD.

The Committee finds that the MIVD established an extensive procedure and thereby endeavoured to proceed with as much care as possible when contributing to a targeting process. Nevertheless, the Committee points out that it was not always easy for it to trace nominations back to their underlying data in the case of the nominations presented to the director of the MIVD and the Secretary General. In that regard, the Committee pointed out to the MIVD the necessity of establishing adequate files, in line with the requirements of propriety and due care. Furthermore, the Committee found the reporting on the decision-making and assessments pertaining to these nominations to be too limited. However, the more extensive version of the nomination, which was provided to the Dutch ISAF commander, made clearer to the Committee which intelligence had served as a basis for formulating the nomination. The Committee observes that these more extensive versions were not presented to the director of the MIVD and the Secretary General for decision-making.

The Committee finds that the purpose of the concerned instances of data provision is in line with the tasks performed by the MIVD, especially in view of the involvement of the Dutch armed forces in the military mission. The Committee also finds that the requirement of necessity has been fulfilled in view of the threat to the mission and military coalition presented by the nominated targets. Regarding the weighing of interests in the context of the propriety test, the Committee observes that only those targets were nominated that could be designated as military objectives that could lawfully be attacked (in accordance with the directives of the ISAF). The Committee already indicated in the legal framework that a weighing of interests in the context of the propriety test fulfils the requirement of due care, when in the case of a deliberate contribution to the targeting process the MIVD assesses prior to the data provision whether the person to whom the data pertains can be designated as a military objective that can be attacked lawfully (see paragraph 3.4.1). According to the Committee, the nomination provided to the Dutch ISAF commander meets the requirement of due care. It is sufficiently clear which data has served as a basis for formulating the nomination. However, according to the Committee, more

[50] *Parliamentary Papers II* 2007/08, 27 925, no. 279.

attention should have been devoted to the clarity of the reporting on the (internal) decision-making in respect of the nominations and related assessments.

The investigation of the Committee shows that the MIVD was well aware of all aspects involved in the actions of the military coalition. Close contacts were maintained with Dutch ISAF units in the area of operations, as a result of which the service remained informed of the decision-making within the ISAF regarding nominated targets. These contacts did not give cause to reconsider the provision of data to the military coalition. According to an internal evaluation report of the MIVD, there has not been any use of force by the ISAF against the nominated targets as a result of these instances of data provision.

The Committee concludes that the instances of data provision it investigated in this context took place in conformity with the legal requirements.

4.3.2 Contribution to the targeting process of Operation Inherent Resolve (fight against ISIS in Iraq and Syria)

In the context of the efforts of the military coalition (including units of the Dutch armed forces) in the fight against ISIS in Iraq and Syria, the MIVD provides structural intelligence reports about (potential) targets, so that their content can be taking into account in the targeting process of the coalition. These reports are provided directly to the Dutch representatives (of the Dutch Ministry of Defence) at the operational headquarters of the military coalition. The headquarters decides whether and to what extent it will use these messages for the targeting process in the context of carrying out the mission. The MIVD's purpose for these instances of data provision is to contribute to an effective fight against ISIS and to gain access to additional flows of information that can be important to identifying the threat aimed at the Dutch (military) contribution in Iraq. The contribution in the context of this mission differs from the contribution to the ISAF described above. For example, the MIVD does not make extensive nominations or maintain files specifically for that purpose in the context of the fight against ISIS.

For the purpose of providing these reports, the MIVD has established and presented a specific procedure to the Dutch Minister of Defence, who has approved it. This procedure provides for additional safeguards, such as a mandatory prior review by the legal department of the MIVD as well as additional reports. In the context of this procedure, the MIVD reviews whether the data to be provided pertains to a legitimate military objective (among other aspects). In this manner, the MIVD tries to prevent as much as possible that Dutch intelligence contributes to actions of the coalition that violate international law, including international humanitarian law. The data provision is restricted to data that is important in the context of the defence of Iraq against attacks by ISIS. This is due to the international public law basis for the use of force against ISIS in Syria, namely: the right to collective self-defence, for the defence of Iraq against armed attacks from Syria by ISIS against Iraq.

- *Assessment*

As stated above, the Netherlands was part of the military coalition in the fight against ISIS. There is also an article-100 letter of the government with regard to this mission. The Committee finds that the MIVD's contribution to the targeting process is in line with the content and purport of these article-100 letters.[51]

The Committee observes that the shortcomings identified in the contribution to the ISAF are no longer present here. As such, it is clear to the Committee which data has served as a basis for the content

[51] *Parliamentary Papers II* 2014/15, 27 925, no. 539 and *Parliamentary Papers II*, 2015/16, 27 925, no. 570.

of the intelligence reports and the reporting is adequate. The requirement of due care is thereby met. Furthermore, the Committee finds that the MIVD is adequately taking into account the legal requirements concerning data provision. The purpose of the concerned provisions is in line with the tasks performed by the MIVD, especially in view of the involvement of the Dutch armed forces in the military mission. Given the interest of the Netherlands in contributing to an effective fight against ISIS and thereby achieving the objective of the mission, the instances of data provision meet the requirement of necessity. In the context of the propriety test, the MIVD ascertains whether the data to be provided concerns a military objective as defined in international humanitarian law. According to the Committee, in doing so, the MIVD adequately weighs the interests in the context of the propriety test.

Moreover, when required, the MIVD devoted attention in the intelligence reports to other relevant information that could be important for the assessment on the basis of international humanitarian law, such as considerations concerning potential collateral damage.

The investigation of the Committee shows that the MIVD keeps itself appraised of the actions of the military coalition in general and the targeting process at the headquarters of the military coalition in particular. For example, the MIVD asks for feedback from the Dutch representatives at the headquarters on the targeting process of the military coalition. This feedback has not given cause to reconsider the provision of data to the military coalition.

The Committee concludes that the instances of data provision it investigated in this context took place in conformity with the legal requirements.

4.4 Practice: provision of data to foreign intelligence and security services

As already stated above, the MIVD frequently exchanges data with foreign I&S services. The Committee observes that the MIVD did *not* provide data to foreign I&S services for the purpose of contributing to targeting processes during the investigation period, except for the data provisions in the context of the military missions described above.

The Committee's interviews with employees of the MIVD show that there is cause to establish specific procedures (see paragraph 4.3) and to present a decision on an intended data provision to the management of the service, respectively, when the content of the data can contribute directly to a targeting process. Current events and incidents, such as the occurrence of *targeted killings* in a region falling under one of the investigation areas of the MIVD, are discussed internally and included in the assessment based on the cooperation criteria.

Furthermore, these interviews show that, in the case of evaluated data, the necessity of the data provision and the potential consequences for e.g. the persons mentioned in the data provision, including the use of force as a result of a targeting process, are weighed for each instance of data provision. However, this is not recorded in writing on a case-by-case basis.

The Committee's investigation furthermore reveals that the MIVD exchanges unevaluated data within a number of topically and geographically oriented cooperative partnerships. The MIVD has been authorised to do so by the Dutch Minister of Defence.[52]

---

[52] CTIVD Review Report no. 49 on the exchange of unevaluated data by the AIVD and the MIVD. *Parliamentary Documents II* 2015/16, 29 924, no. 142 (appendix), pp. 16-17.

The Committee notes that a part of the (evaluated as well as unevaluated) data provided to foreign I&S services concerns topics related to the use of force by (the state of) the foreign I&S service to which the data was provided. This also concerns information about the identification, behaviour, and location of members of groups, of which it is certain that they are actively being combated through use of force by the armed forces of the state of the service to which the data was provided and in which use of force the Netherlands does not participate directly itself. In addition, this concerns unevaluated data, namely communications (or data regarding these) from a region in which this use of force is taking place.

The reasons for the provision of such data reside in the MIVD's proper performance of its tasks (Article 36 of the ISS Act 2002). This pertains e.g. to the provision of data for the prevention of activities that can impair the readiness or deployment of the Dutch armed forces or coalition troops in a specific area of operations. This can also concern the provision of data that is only of interest to the foreign I&S service (Article 59 of the ISS Act 2002). These instances of data provision revolve exclusively around the interest of the foreign I&S service in obtaining this data and not around an (ongoing) investigation of the MIVD.

- *Assessment*

The Committee has examined the instances of data provision to establish whether they are related through their topics to the use of force by (the state of) the receiving foreign I&S service.

The Committee finds that the MIVD has drawn up weighting notes in respect of the foreign services with which such data has been shared. These weighting notes provide a comprehensive explanation and a clear picture of the cooperative relationship developed by the MIVD with the foreign I&S services concerned. However, as shown by paragraph 4.2 and the Committee's review report on the implementation of cooperation criteria by the AIVD and the MIVD, the Committee finds that the weighting notes do not meet the applicable requirements as yet.

In an earlier investigation, the Committee has devoted attention to the cooperation between the MIVD and foreign I&S services in general and has reviewed its lawfulness, including the exchange by the MIVD of *evaluated data* with these services. The investigation period was from the beginning of 2007 until the end of 2013. The related review report was published in the middle of 2015.[53] In this investigation, just like in its investigation into the cooperation with foreign I&S services, the Committee also has a positive image of the lawfulness of the provision of evaluated data by the MIVD to foreign I&S services. However, the Committee finds that, in individual instances of data provision, the MIVD must take into account, more explicitly than is currently the case, the possibility that data provision can contribute to targeting processes involving the unlawful use of force. When it can be established that this is a real possibility on the basis of empirical rules and the facts and circumstances, then the assessments resulting from the legal requirements of necessity, propriety, and due care must be recorded in writing when the data is provided. This is not (yet) a part of the MIVD's practice.

As described already above, the MIVD exchanges *unevaluated data* within a number of cooperative partnerships. The Committee finds that the decision-making regarding the (un-)acceptability of a risk that a contribution is made to the use of force by means of the provision of unevaluated data must take place explicitly by requiring the authorisation of the Minister. This must take into account what is set out in the weighting notes of the MIVD, the requirements imposed on these weighting notes by the Committee, and the requirements attached to the individual instance of data provision itself (see Chapter 3). The latter is not (yet) a full part of the MIVD's practice.

---

[53] CTIVD Review Report no. 22b on cooperation between the MIVD and foreign I&S services. *Parliamentary Documents II* 2014/15, 29 924, no. 128 (appendix), available at www.ctivd.nl.

4.5 The use of the data provided by foreign intelligence and security services and military coalitions

During the investigation of the Committee pertaining to the period from January 2013 to December 2015, the MIVD has stated that it has not inferred from contacts with foreign I&S services or from its own investigation, respectively, that data provided to foreign I&S services (except for military missions participated in by the Dutch armed forces) has contributed in specific cases to targeting processes. In its investigation, the Committee has *not* encountered concrete indications of such instances. Neither has the Committee encountered concrete indications that the MIVD has taken an unacceptable risk of a contribution to the unlawful use of force when providing data.

However, the Committee cannot exclude that the data provided by the MIVD to foreign I&S services has nevertheless been used by or via these services for targeting processes (resulting in the lawful or unlawful use of force). Such services are not (publicly) accountable for this. The Committee also does not have the power to investigate what the foreign I&S services have done with the data received. The same applies to the question of what military coalitions have done with the data received from the MIVD.

4.6 Conclusion

The Committee finds that the legal framework used by the MIVD in its policy is to date insufficiently focused on the risk that the MIVD can contribute involuntarily, by means of the provision of data, to targeting processes involving the unlawful use of force. This makes it harder for the Committee to review the practice.

The Committee establishes that the MIVD has in practice contributed a number of times deliberately to a targeting process by providing data to a military coalition participated in by the Dutch armed forces. The Committee finds that the instances of data provision it examined were in conformity with the legal requirements in that context.

The MIVD has provided *evaluated* data that are related to the use of force to I&S services involved in the use of force in the context of armed conflicts or a comparable use of force. This relationship existed, for example, because the data concerned members of a militant group targeted by the use of force. The Committee finds that, in individual instances of data provision, the MIVD must take into account, more explicitly than is currently the case, the possibility that data provision can contribute to targeting processes involving the unlawful use of force.

The MIVD has also provided I&S services of states involved in the use of force with unevaluated data potentially related to that use of force. For example, because the data concerns communications (or data regarding these) from a region in which this use of force is taking place. The Committee finds that the decision-making regarding the (un-)acceptability of a risk that a contribution is made to the use of force by means of the provision of unevaluated data must take place explicitly by requiring the authorisation of the Minister. This must take into account what is set out in the weighting notes of the MIVD and the requirements imposed on these weighting notes by the Committee. The latter is not (yet) a full part of the MIVD's practice.

During the investigation of the Committee pertaining to the period from January 2013 to December 2015, the MIVD has stated that it has not inferred from its own observations, contacts with foreign I&S services or from its own investigation, respectively, that data provided to foreign I&S services (except for military missions participated in by the Dutch armed forces) has contributed in specific cases to targeting processes. In its investigation at the MIVD, the Committee has *not* encountered

concrete indications of such instances. Neither has the Committee encountered indications that the MIVD has taken an unacceptable risk of a contribution to the unlawful use of force when providing data.

However, the Committee cannot exclude that the data provided by the MIVD to foreign I&S services has been used by or via these services for targeting processes (resulting in the lawful or unlawful use of force). After all, such services are not (publicly) accountable for this. The Committee also does not have the legal power or the possibility to investigate what the foreign I&S services have done with the data received. The same applies to the question of what military coalitions have done with the data received from the MIVD.

5 Conclusions

In this review report, targeting refers to the process that (through selection and prioritisation of objectives) can result in the use of force by armed forces in order to achieve a strategic objective in the context of a (military) operation (the targeting process).

A contribution by the MIVD to a targeting process can consist of the provision of data to foreign I&S services, to the Dutch armed forces or to a military coalition in which the latter participates. The MIVD provides data for a specific purpose. However, the MIVD is not always aware of the recipient's precise purpose for the data it provides. Therefore, the MIVD can make a deliberate as well as an involuntary contribution to a targeting process.

The Committee has opted for a review report that provides a framework guiding the MIVD in its future actions and that makes possible an assessment of the practice in past years. This means that the emphasis of this report is on establishing a framework for contribution by the MIVD to targeting, including the legal boundaries in this respect. For that purpose, it has also assessed the standing policy of the MIVD and its implementation. Naturally, the Committee has not assessed the political desirability or undesirability of lawful contributions of the MIVD to targeting processes. This is not part of its oversight task. The Committee's investigation was focused on the provision of data by the MIVD to foreign intelligence and/or security services (I&S services) from 1 January 2013 up to and including 31 December 2015 and the provision of data by the MIVD within the context of ongoing and recently concluded military missions.

First, it must be understood that the possibility that a provision of data can contribute to targeting processes does *not* necessarily mean that the MIVD is acting unlawfully. However, this is the case when the MIVD accepts an unacceptable risk of a direct or indirect contribution to the unlawful use of force when providing data.

Therefore, the MIVD must in the first instance thoroughly assess whether and to what extent it can cooperate with a foreign I&S service and, if so, what the associated risks and conditions can be. This is recorded in a weighting note. In doing so, it must also expressly take into account the (un-)lawfulness of a potential use of force by (the state of) the foreign I&S service, in the context of previous or ongoing armed conflicts or a comparable use of force. In doing so, attention must be devoted to the existence of an international public law basis for the use of force by a state in or against another state (cross-border armed actions) and the compliance with the regulatory frameworks (international humanitarian law and/or the human rights regime). This applies in particular when the Netherlands is not involved in this use of force or, in the case of an armed conflict, the Netherlands is not a party to the conflict.

Next, the MIVD must apply stringently the legal requirements pertaining to the individual data provision itself. The data provision must remain within the boundaries specified in the weighting note (nature and intensity of the cooperation) and meet the requirements of necessity, propriety, and due care. If there are concrete indications that the data provided, directly or indirectly, has contributed to the unlawful use of force (the so-called *feedback loop*), then this must be taken into account in the weighting note pertaining to the cooperation with the concerned I&S service through reconsideration.

Data provision to military coalitions in which the Netherlands participates is subject to a comparable framework. In addition, the data provision must be in agreement with that what the government has reported to parliament about the nature and intensity of the participation of the Netherlands, whether via a so-called article-100 letter or not.

According to the Committee, the legal framework described in this review report constitutes the key to what can reasonably be expected of the MIVD to prevent the cooperation with a foreign I&S service or a military coalition from contributing to the violation of international law, including the unlawful use of force by others. The Committee finds that the MIVD's policy is to date insufficiently focused on the risk that the MIVD can contribute involuntarily, by means of the provision of data, to targeting processes involving the unlawful use of force. This also makes it more difficult for the Committee to review the practice. The standing policy of the MIVD must be brought in line with the legal framework described by the Committee.

The Committee establishes that the MIVD has in practice contributed a number of times deliberately to a targeting process by providing data to a military coalition participated in by the Dutch armed forces. The Committee finds that this took place in conformity with the legal requirements. One of the military coalitions to which data have been provided was the ISAF coalition. According to an internal evaluation report of the MIVD, there has not been any actual use of force by the ISAF as a result of these instances of data provision.

The Committee has *not* found that the MIVD has purposefully provided data to foreign I&S services for the purpose of targeting processes, outside military missions in which the Netherlands participates itself. The investigation of the Committee did show that the MIVD has provided evaluated data to I&S services involved in the use of force in the context of armed conflicts or a comparable use of force, in which these data have a relationship with that use of force. The data concerned e.g. members of a militant group targeted by that use of force. The MIVD has also provided I&S services of states involved in the use of force with unevaluated data potentially related to that use of force. For example, because the data concerned communications (or data regarding these) from a region in which this use of force is taking place.

The Committee does not have concrete indications that the MIVD has accepted an unacceptable risk of making a contribution to the unlawful use of force by providing this data.

However, the Committee finds that, for individual instances of data provision, the MIVD must take into account, more explicitly than is currently the case, the possibility that provision of data can involuntarily contribute to targeting processes that involve the unlawful use of force and better tailor the conditions for the provision of data to that possibility.

During the investigation of the Committee pertaining to the period from January 2013 to December 2015, the MIVD has stated that it has not inferred from contacts with foreign I&S services or from its own investigation, respectively, that data provided to foreign I&S services (except for military missions participated in by the Dutch armed forces) has contributed in specific cases to a targeting process. In its investigation, the Committee has *not* encountered concrete indications of such instances.

However, the Committee cannot exclude that the data provided by the MIVD to foreign I&S services has nevertheless been used by or via these services for targeting processes resulting in the unlawful use of force. In general, such services are not (publicly) accountable for this. The Committee also does not have the legal power to investigate what foreign I&S services have exactly done with the data received. The same applies to the question of what military coalitions have done with the data received from the MIVD.

Not even the application of the legal framework described in this review report as preferable will in practice exclude the risk that data provided by the MIVD to foreign (military) I&S services is used for the unlawful use of force, without this being the intent of the MIVD. Applying the legal framework can, however, reduce significantly the risk of this happening.

6 Recommendations

1. The Committee recommends that the MIVD bring its standing policy for the provision of data to foreign I&S services and to military coalitions, respectively, in line with the legal framework described in this review report.

2. The weighting notes must, among other things, show the risks that can be engendered by the cooperation with foreign I&S services and the conditions under which certain forms of cooperation (such as the provision of personal data and unevaluated data) are permitted. This means that the MIVD must also assess whether (the state of) the concerned foreign I&S service is involved in the use of force in the context of armed conflicts or a comparable use of force. If that is the case, it must evaluate whether the data provision can give rise to risks in the sense that it can imputably lead to a violation of international legal standards, including the unlawful use of force.

3. In practice, not all cases will lend themselves to a straightforward determination of whether there is an armed conflict or an international public law basis for the use of force by another state. The states involved will generally believe that the force they use is lawful. The Committee therefore deems it advisable for the MIVD to seek legal advice on this issue in the event of uncertainty. For example, from the Legal Affairs Department of the Dutch Ministry of Defence and/or via this ministry from the Dutch Ministry of Foreign Affairs if necessary.

4. When the MIVD intends to contribute to a targeting process, then the assessments made in that regard in the context of the legal requirements must be recorded in writing. When the MIVD's explicit objective for the data provision is *not* a contribution to a targeting process, then the assessment must nevertheless be recorded in writing when there is reasonably a real possibility (risk) that this data provision will contribute to a targeting process, on the basis of general empirical rules and/or the facts and circumstances of the specific case.

5. When the (evaluated or unevaluated) data to be provided pertains to a topic of which it is known that it is related to the ongoing use of force by the state of the I&S service to which the data is being provided *and* the Netherlands itself is not involved in that use of force, then the written condition that this data may *not* be used for purposes that entail a violation of international law must be attached, in addition to the third-party rule.

6. The deployment of the Dutch armed forces in the context of a coalition involves a governmental decision about which information is provided to parliament. The provision of data to a military coalition of which the Netherlands is a part must be in agreement with what the government has reported to parliament about the nature and intensity of the participation of the Netherlands, whether via a so-called article-100 letter or not.

7. When there is a suspicion that data provided has contributed to the unlawful use of force by the state of the recipient party (reports from human rights organisations or the media can be indicators of such use), then the MIVD must actively investigate whether the data provided has potentially contributed to that use (a so-called *feedback loop*). If there are concrete indications of such unlawful use, then this must be taken into account in (the extent of) the cooperation with the concerned recipient party through reconsideration.

Appendix I: Investigation plan and methodology

What did the Committee investigate?

The Committee has investigated the lawfulness of contributions by the MIVD to targeting processes.

Due to the scope of the term targeting process and the fact that the social and political-administrative discussion concerns targeting in the sense of the unlawful use of force, the Committee has decided to focus its investigation specifically on the provision by the MIVD to foreign I&S services of data that due to its topic, whether or not in combination with intelligence from other sources, can contribute to decision-making regarding (military) actions to be executed by the use of force.[54] This in the context of the use of force by (the state of) the party receiving the data.

In this context, the Committee has focused on data provision by the MIVD to foreign I&S services from 1 January 2013 up to and including 31 December 2015. In addition, it has focused on data provision by the MIVD to bodies other than I&S services, in the context of ongoing and recently concluded military missions.

The Committee cannot assess to what extent the data provided by the MIVD has effectively been used by foreign parties for targeting processes. After all, the Committee does not have the legal power to further investigate data processing by these parties.[55]

How has the Committee performed this investigation?

In the first instance, the Committee has investigated the legal framework based on a review of literature and various interviews with experts.

Furthermore, the Committee has examined various media reports and parliamentary documents that cover the *targeted killings* attributed to the United States and the potential involvement of the MIVD in that regard.[56]

In addition, based on a review of literature and interviews with employees of the MIVD and other officials of the Dutch Ministry of Defence, the Committee has formed a picture of the practice surrounding the processing of data that can contribute to a targeting process.

Next, the Committee further assessed instances of data provision that fell under the above-mentioned focus, on the basis of searches in the systems of the MIVD and interviews with MIVD employees. The Committee has not performed an exhaustive investigation due to the vast amount of data. Instead, the Committee has focused on data as described in paragraph 2.7. From this data, it has selected and further examined instances of data provision that 1) took place in the aforementioned investigation period, and that 2) are related to the use of force by the state of the recipient foreign I&S service or military coalition.

---

[54] In this context, the Committee takes the terms 'actions to be executed with force' to mean: the use of force aimed at destroying or eliminating objects or at killing (a group of) persons or eliminating them in any other way (by e.g. taking them prisoner).

[55] In the context of its oversight task, the Committee is only authorised to investigate the manner in which what has been prescribed by or pursuant to the ISS Act 2002 or the Security Screening Act (Wet Veiligheidsonderzoeken) has been executed (Article 78 of the ISS Act 2002).

[56] See notes 2 and 3.

In 2012, the Committee brought to the attention of the MIVD[57] an exploration into this topic in respect of the deployment of the Dutch armed forces in Afghanistan and the findings dating from the same year. The Committee has taken these findings into account in this investigation.

(Parts of) draft versions of this report have been submitted to a few members of the Knowledge Network of the Committee.[58] In addition, unclassified parts of these draft versions have been presented to external experts.

External legal experts consulted:
- Brigadier General Prof. Dr P.A.L. Ducheine
- Prof. Dr T.D. Gill

Timeline of the investigation

22 May 2015	Announcement of the investigation.
4 May 2016	Review Report drafted.
29 June 2016	(Classified) reaction of the Dutch Minister of Defence to the drafted review report.
3 August 2016	Review Report adopted.

[57] By means of explorations, the Committee aims to gain broad insight into the key activities of the AIVD and the MIVD. The services inform the Committee about important events and developments. The Committee itself also identifies the activities of the AIVD and the MIVD. By keeping itself appraised of the developments within the AIVD and the MIVD, the Committee can make a justified choice of investigation topics.

[58] The CTIVD set up a knowledge network at the end of 2014. The Knowledge Network advises the CTIVD on relevant developments and collaborates critically with the Committee in (the selection of) investigations.

Appendix II: Relevant international legal standards

1 Introduction

The execution of a targeting process and the use of force that can result from that process are bound by rules. The law sets boundaries for what is allowed in this area. Data of the MIVD can play a role in a targeting process, as described by the Committee in Chapters 2 and 3 of this review report. The MIVD can have at its disposal data that, when provided, can contribute to decision-making on whether or not to use force to eliminate certain targets.

In Appendix I (Investigation plan and methodology), the Committee explains that its focus was primarily on contributions of the MIVD to targeting processes in the context of decision-making concerning the use of force. Consequently, this is also the focus of the legal framework in Chapter 3 and this appendix.

2 International law standards pertaining to the targeting process

2.1 Introduction

International law standards can have an influence on the MIVD's performance of its tasks. One of the principles of the ISS Act 2002 is that the MIVD is bound by law in the performance of its tasks (see Article 2 of the ISS Act 2002). This does not only refer to the ISS Act 2002, but also to the law in the general sense. This includes the legal standards laid down by the Constitution (e.g. the best efforts obligation of the government to promote the international legal order)[59] and international law (the international obligations of the Netherlands that arise from ratified treaties, among other sources).[60]

Whether, and if so, to what extent the use of force as a result of the targeting process is permitted is often connected to the application of such standards. The answer to the question of whether such (direct or indirect) contribution amounts to a violation of these standards is of specific importance in the case of a contribution of the MIVD to a targeting process. In the sub-paragraphs below, the Committee discusses the international legal standards relevant in this context.

2.2 International public law basis for the use of force abroad *(ius ad bellum)*

When executing a targeting process, there is a (military) operation executed by units of one or more states. When such an operation has a cross-border nature or when multiple states are involved, international law prescribes the presence of an international public law[61] basis.[62] This falls under the *ius ad bellum*. This term refers to international legal standards that concern the question of under which circumstances the state can use force against or in another state (or against a non-state entity such as a militant group in another state), among other standards.

---

59 Article 90 of the Dutch Constitution.

60 *Parliamentary Documents II* 2000/01, 25 877, no. 14, p 65.

61 Other names for this are: "legal basis" or "international public law mandate".

62 See e.g the letter of the Dutch Minister of Foreign Affairs accompanying the advice of the external international public law advisor concerning the use of force against ISIS in Syria, which explains what the international public law basis can be of military action over there (*Parliamentary Documents II* 2014-15, 27 925, no. 543). See also T.D. Gill & P.A.L. Ducheine, 'De legitimering van statelijk geweldgebruik na 9/11', in: F. Osinga, J. Soeters, W. van Rossum (reds.), *Nine eleven*: tien jaar later, Amsterdam: Boom (2011), p 216-234.

An international public law basis can be: the consent of the state in which the use of force is taking place, a resolution of the Security Council of the United Nations (Chapter 7 UN Charter) or the right of a state to defend itself (Article 51 of the UN Charter).[63] Decisions to invoke an international public law basis are in general made at the level of the government. When there is no international public law basis for the cross-border use of force by a state, this constitutes a violation of the *ius ad bellum*.

Besides an international public law basis for the use of force by states (that pertains to the question *of* whether a state is allowed to use force outside its territory, among other aspects), the question of when the use of force is permitted is also important. This question is answered by the rules applicable to *the manner in which* (military) operations can take place. This pertains to rules that e.g. establish the manner in which force can be used. These rules can be found in the so-called (international) regulatory frameworks, such as international humanitarian law (also referred to as ius in bello).

2.3 Regulatory frameworks that can apply to the use of force *(including ius in bello)*

Various international regulatory frameworks can apply to the manner in which force is used.[64] When force is used in the context of an armed conflict, then it will be subject to international humanitarian law.[65] This means that, in such a case, international legal standards of international humanitarian law determine in principle what is permitted where it concerns the use of force. For example, the answer to the question of whether an object or person is a military objective that can lawfully be attacked.[66] Under certain circumstances, objects can be attacked when they "by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction (...) in the circumstances at the time, offers a definite military advantage."[67] Civilians enjoy a general protection against dangers arising from military operations. Civilians can also be attacked under certain circumstances, to the extent that and "as long as they participate directly in the hostilities."[68]

---

63 T.D. Gill & D. Fleck (Eds.), *Handbook of the International Law of Military Operations* (2nd ed.): Oxford University Press (2015), pp. 95-252.

64 M.N. Schmitt, *'Targeting in international Law'* in T.D. Gill & D. Fleck (Eds.), *Handbook of the International Law of Military Operations* (2nd ed.): Oxford University Press (2015), pp. 269-306 and N. Melzer, 'Targeted Killings in Operational Law Perspective' in T.D. Gill & D. Fleck (Eds.), *Handbook of the International Law of Military Operations* (2nd ed.): Oxford University Press (2015), pp. 307-331.

65 Other names for this are the "law of armed conflict" or "law of war".

66 See Articles 35-58 of the Additional Protocol to the Geneva Conventions of 12 August 1949 relative to the Protection of Victims of International Armed Conflicts adopted in Bern on 8 June 1977 (Protocol I), among others.

67 Article 52 of the Additional Protocol to the Geneva Conventions of 12 August 1949 relative to the Protection of Victims of International Armed Conflicts adopted in Bern on 8 June 1977 (Protocol I). In general, this provision is considered to be a part of customary law.

68 Article 51 of the Additional Protocol to the Geneva Conventions of 12 August 1949 relative to the Protection of Victims of International Armed Conflicts adopted in Bern on 8 June 1977 (Protocol I). In general, this provision is considered to be a part of customary law.

Armed conflicts can be international armed conflicts or non-international armed conflicts.[69] An international armed conflict exists when states use force against each other. There is a non-international armed conflict when force is used between one or more states on the one hand and organised armed groups on the other hand (or among such groups themselves). However, the existence of a non-international armed conflict requires the intensity of the use of force to be high enough and the armed group(s) must be sufficiently organised. That is why not every use of force between one or more states on the one hand and armed groups on the other hand (or among such groups themselves) qualifies as an armed conflict.

A targeting process that results in the use of force *outside* an armed conflict is permitted only in exceptional cases. After all, the human rights regime is fully applicable in the case of the use of force outside an armed conflict. In comparison with international humanitarian law, this regulatory framework only exceptionally offers leeway for the use of lethal force.[70] This can be the case when the lethal force is absolutely necessary to defend persons against unlawful force, to effect a lawful arrest or to put down a rebellion.[71]

For that matter, it is important to emphasise that the fact that international humanitarian law provides a specific legal framework for armed conflicts does *not* automatically rule out the applicability of the human rights regime in such situations.[72] The entity taking actions in the context of a targeting process will have to establish whether an action to be taken is lawful based on the applicable regulatory frameworks. This legal obligation does not reside with an I&S service that only provides the necessary intelligence in that regard (such as the MIVD), but in general with a (military) commander who has tactical command of combat units.

---

[69] Even though the rules are mostly the same for an international or non-international armed conflict, there are important differences. The prisoner-of-war regime is not applicable in a non-international armed conflict, for instance.

[70] For example, think about standards of the European Convention on Human Rights (ECHR) or the International Covenant on Civil and Political Rights (ICCPR), to wit: Article 2 of the ECHR (the right to life) and article 6 of the ICCPR (idem).

[71] Article 2 of the ECHR.

[72] See E. Pouw, *International Human Rights Law and the Law of Armed Conflict in the Context of Counterinsurgency:* With a Particular Focus on Targeting and Operational Detention, Ministerie van Defensie 2013, Diss. Uva 2013. See also T.D. Gill, *'Some Thoughts on the Relationship between International Humanitarian Law and International Human Rights Law: a Plea for Mutual Respect and a Common Sense Approach'* , *The Yearbook of International Humanitarian Law* 2013, p 251-266.

CTIVD no. 50

APPENDIX III DEFINITIONS

of the review report on contributions of the MIVD to targeting

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.

Analytical cooperation	The exchange of data (that is not personal data and unevaluated data) that provides an insight into the current level of knowledge of the service.
Armed conflict	According to international humanitarian law, there is an armed conflict when states use force against each other (international armed conflict) or when force is used between one or more states on the one hand and one or more organised armed groups on the other hand or between armed groups themselves (non-international armed conflict). The existence of a non-international armed conflict depends on the intensity of the force and the degree of organisation of the armed group(s) involved. Not every use of force by a state against an armed group can therefore be qualified as an armed conflict.
Cooperation criteria	The criteria the service must use in order to assess whether a foreign I&S service qualifies for cooperation.
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, preamble and (f), of the 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 the storage and destruction of data.
Deliberate contribution to targeting	The provision of data for the purpose of contributing to a targeting process.
Evaluated data	Data which has been assessed for relevance to the performance of tasks.
Foreign I&S service	An intelligence and/or security service of another state.
ISS Act 2002	Intelligence and Security Services Act 2002. This law was in force at the time of the investigation by the CTIVD.

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 of the ISS Act 2002 (e.g. interception and surveillance).
Involuntary contribution to targeting	The provision of data without the purpose and without the knowledge of making a contribution to targeting.
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.
Military coalition	A military cooperative partnership consisting of armed forces of multiple states, under the flag or leadership of international organisations such as the NATO.
Operational cooperation	Forms of cooperation that provide insight into the procedure or sources of the service or involving the provision of personal data and unevaluated data.
Personal data	Data relating to an identifiable or identified individual natural person (e.g. a name or a photograph). Article 1, preamble and (e), of the ISS Act 2002.
Protocol-based cooperation	Maintaining contacts with a foreign service.
Quid pro quo	Reciprocity; literally: "One good turn deserves another." Principle in the cooperation between intelligence and security services.
Targeting (process)	A process that can result (through selection and prioritisation of targets) in the use of force by armed forces to achieve a certain tactical or strategic objective, among other outcomes.
Unevaluated data	Unevaluated data is data that has not yet been assessed for relevance to the performance of tasks (e.g. large quantities of metadata).
Use of force	The use of force, in as well as outside an armed conflict, with (military) means such as combat units that are a part of armed forces such as infantry units, military aircraft (manned and unmanned), and long-range missiles.
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 authorised.

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