Progress Report

Functioning of the ISS Act 2017

CTIVD no. 59

[adopted on 27 November 2018]

CTIVD
Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence and
Security Services

CTIVD no. 59

PROGRESS REPORT

Functioning of the ISS Act 2017

Table of contents

Review Committee
on the Intelligence and
Security Services

CTIVD no. 59

PROGRESS REPORT

Functioning of the ISS Act 2017

1 Introduction

Context

On 1 May 2018, the Intelligence and Security Services Act 2017 (ISS Act 2017) entered into force. This piece of legislation has generated much debate in politics and society as a whole over the past years. Central to this debate is the question whether the investigatory powers of the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) to protect national security are balanced with the safeguards for the legal protection of citizens, such as the right to privacy and the general principles of personal data protection. The Review Committee on the Intelligence and Security Services (CTIVD) sees it as its core duty to provide an ongoing insight into that balance.

From 1 May 2018, the CTIVD has focused its oversight activities on the functioning of the new Act, in particular on the topics that received most attention in the political and public debate. That debate specifically stressed the importance of effective oversight on the use of a number of investigatory powers and compliance with legal and pledged policy safeguards. This was followed up with pledges from the government to the Senate and the House of Representatives to request the CTIVD to report on certain topics soon after the Act entered into force. By letter of 25 April 2018, the Minister of the Interior and Kingdom Relations sent the CTIVD the requests for accelerated oversight arising from the parliamentary debate of the act[1].

The independence of the CTIVD includes the freedom to choose the topics it wishes to investigate. The topics of the letter referred to above correspond to a large extent with the key points the CTIVD put forward itself during and after the parliamentary debate on the act and which it considers relevant and prioritizes on the basis of its legal task of oversight.

1 Request from the Minister of the Interior and Kingdom Relations regarding motions and pledges ISS Act 2017, dated 25 April 2018, *Parliamentary documents II* 2017/18, 34588 no. 1 (appendix).

Focus

In the past six months, the CTIVD focused on the following topics[2]:

1. The existence of the pledged range of instruments for the services' **duty of care** to **lawfully process data** and the functioning of those instruments;
2. How **data is reduced responsibly** during the use of special investigatory powers, focusing on the implementation of the duty to assess data as quickly as possible for relevance and to immediately destroy non-relevant data;
3. The use of the investigatory power of **investigation-related interception** including the application of the criterion 'as targeted as possible' and the usefulness and need for the maximum retention period of three years;
4. The use of the investigatory power of **automated data analysis** in the context of investigation-related interception;
5. How the process of **internal complaints handling** and **reports of misconduct** is set up within the services;
6. The **cooperation with foreign services**, including the existence and the functioning of weighting notes as well as the exchange of **unevaluated data**.

Methodology

In those areas where the services' investigatory powers are new or where the legal and pledged policy-related safeguards for the legal protection of citizens left room for interpretation, the CTIVD conducted a **baseline measurement**. In its baseline measurements, the CTIVD assessed marginally whether the legal and pledged policy-related safeguards had been implemented further in the services' policy and work processes as well as in the set-up of the technical systems for data processing. All safeguards incorporated in the ISS Act 2017 and the policy-related commitments made before and after the referendum on the ISS Act 2017 should be implemented internally at the AIVD and the MIVD. In some cases a random check was conducted to gain insight into the application in practice.

Another point of assessment was whether the functioning of the internal data processing processes is continuously checked internally as intended by the Act and whether effective external oversight by the CTIVD is possible. Effective oversight means that the CTIVD is able to focus on each process of data processing by the AIVD and the MIVD, in terms of set-up, application and results. Simply having unrestricted access to data is not enough. That would mean that the CTIVD would have to manually assess the data fact by fact and expand its staff capacity disproportionally to be able to do so. That is neither feasible nor desirable. The data processing at both services must be subject to internal control mechanisms, which are obligated by law and on which the CTIVD can in part base its oversight.

The outcome of a baseline measurement is a **risk assessment** regarding lawfulness. The assessment identifies where there are risks for unlawful conduct by the services and gives direction to the subsequent oversight activities of the CTIVD. Each assessment is an estimate of the risk of unlawful conduct and not a decision that unlawful conduct has taken place. Where risks are established, the CTIVD will indicate what is lacking and why. These assessments are not based on what the CTIVD feels is advisable, but are founded in a legal or pledged policy-related safeguard for the legal protection of citizens.

2 Letter from the CTIVD to the House of Representatives, dated 26 April 2018, *Parliamentary documents II* 2017/18, 34588 no. 77.

The CTIVD classifies the risks into the following categories:

- **No risk:** The implementation of the legal framework is sufficient and no inadequacies have been established in policy, processes or their application. Moreover, policy is up to date.

- **Limited risk:** The implementation of the legal framework is sufficient but inadequacies have been established in policy, processes or their application. The inadequacies are of limited substantive or procedural nature and easy to repair.

- **Average risk:** The implementation of the legal framework is insufficient because substantive inadequacies have been established in policy, work processes, systems or their application. These inadequacies could lead to unlawful conduct by the services.

- **High risk:** The implementation of the legal framework is insufficient because of the lack of any policy or processes or because these are in violation of the law or because there is unlawful conduct in their application.

The baseline measurements were conducted for the period 1 May 2018 to 1 July 2018. In October 2018, the CTIVD updated its view of the findings of those measurements and the risks it established in that context. In this context, frequent conversations were held with both services. That means that the current progress report is a reflection of the legal and pledged policy-related safeguards implemented by the AIVD and the MIVD per 1 November 2018. The appendix to this progress report provides a more detailed explanation. The appendix has not been translated into English.

Besides baseline measurements, the CTIVD also conducts **in-depth investigations.** In-depth investigations focus on the application of a part of the law in practice. The outcome of an in-depth investigation is a **lawfulness assessment** and comes with recommendations to prevent any further unlawful conduct. Currently there are two ongoing in-depth investigations. One into the assessment of cooperation criteria in the weighting notes that form the basis for cooperation with foreign services and another into the exchange of unevaluated data with foreign services (see section 3.5).

Reports

The oversight activities into the functioning of the ISS Act 2017 will continue at least until May 2020. With a view to the early evaluation of the ISS Act 2017 intended from May 2020, the CTIVD strongly aims to issue – within two years of the act entering into force – its concluding report on the topics that were raised during the parliamentary debate on the act and that were submitted to the CTIVD for investigation.[3] It will report every six months to the Ministers involved and parliament, addressing the progress of this process and the preliminary conclusions that may be drawn regarding the functioning of the ISS Act 2017.

The findings and conclusions of the lawfulness investigations are adopted each time in a separate review report that is subsequently published. In addition, the CTIVD reflects on its activities of the past reporting year in its annual report.

3 Request from the Minister of the Interior and Kingdom Relations regarding motions and pledges ISS Act 2017, dated 25 April 2018, *Parliamentary documents II* 2017/18, 34588 no. 1 (appendix).

2 Overall view

The implementation of the ISS Act 2017 places heavy demands on the AIVD and the MIVD. Much has been done by both services in the run up to the new act entering into force. A significant part of the AIVD and MIVD's capacity had to go into supportive processes, while at the same time much was expected of the services in operational terms. Even after the new legislation entered into force, the services have been in full swing and they still are.

The AIVD and the MIVD are faced with a new framework for their investigatory powers, some of which they have been exercising for years, and face the challenge of making the newly granted investigatory powers operational as soon as possible. They have a new player in the review regime to contend with – the TIB, that reviews the lawfulness of the authorization granted by the Ministers prior to the use of certain special investigatory powers. They are required to adapt to the oversight body, the CTIVD, that – thanks to direct and full access and the reinforcement of its technical expertise – is increasingly able to penetrate into the technical data processes of both services. In that respect, the area of activity in which the AIVD and the MIVD operate is highly dynamic, where international cooperation and technological developments are prevalent and where there are political and societal forces at play that question the functioning of the ISS Act 2017. That requires vision, control, flexibility as well as empathy and stamina from the services.

The impression that the CTIVD has, a good six months after the new legislation entered into force, is that the services are not there yet. The professionalism of the AIVD and the MIVD in conducting the tasks assigned to them to protect national security is beyond dispute. However, in practice, vital safeguards to protect the rights of individuals are still lacking in part or in their entirety. Policy in the area of data protection is lacking in key parts, such as the implementation of data protection *by design and by default.* Further, the criterion 'as targeted as possible' is not applied in any recognizable form (for example, as targeted filtering as possible within the interception itself and as targeted selection criteria as possible). The reduction of data required by law is still a work in progress, in part because of a flawed supporting IT infrastructure at the MIVD. Finally, too little heed is taken of legal safeguards for the automated metadata analysis (such as prior authorization in all cases and limited access of staff to metadata). Effective oversight on compliance with the obligations set by the legislation is not yet sufficiently possible. The instruments for the legal duty of care to lawfully process data have not been adequately specified and as a consequence, any ongoing compliance audits on important work processes are lacking. There is a backlog when it comes to implementing these legal and policy-related safeguards.

The AIVD and the MIVD will still have to take a number of fundamental steps to shape – in practice – the balance required by law between the need to protect our national security and being able to ensure sufficient legal protection for citizens. After all, the use of investigatory powers to protect national security and the legal protection of citizens must go hand in hand. In November 2018, the CTIVD points out that although the services are willing to commit to this, they have not taken any specific steps to do so.

In the following, the CTIVD will discuss the results of the baseline measurements and the accompanying risks perceived. The appendix to this progress report further details the basis for the risks established by the CTIVD.

3 Overall view per topic

3.1 Baseline measurement: duty of care

The duty of care that the AIVD and the MIVD have to ensure data is processed lawfully is a crucial safeguard, both for the protection of data and for the oversight. Certain elements of that duty of care existed in the former ISS Act 2002 and are embedded in the services' data processing processes. Technological developments and the services' new investigatory powers and requirements under the ISS Act 2017 have led to new challenges where it concerns these elements of the duty of care. One new element compared with the former ISS Act 2002 is the duty to promote the quality of the data processing. This element was included in the ISS Act 2017 because the services' data processing is becoming increasingly automated. The duty of care also creates safeguards in relation to the legislation's independence of technology.

The duty of care clearly places demands on the AIVD and the MIVD that are greater than simply implementing the legal requirements for collecting, analysing and using data. In specific terms, the duty of care means that the services have ongoing control of how they process data and that they ensure that this data processing is and continues to be in compliance with the legal requirements. Continuously being in control requires the services to use a number of instruments that provide a central view on the functioning of processes and systems of data processing and enable them to identify risks and take measures promptly. Without these instruments, without a clear structure for the duty of care, it is not possible to exercise sufficient internal control over the data processing and any effective external oversight is out of the question.

In December 2017, the Minister of the Interior and Kingdom Relations and the Minister of Defence pledged that 'when the legislation enters into force, an adequate set of instruments safeguarding the protection of data will be available, allowing the CTIVD to immediately use this in its oversight activities'.[4]

The CTIVD has established that on 1 May 2018 (and on 1 November 2018) there was no set of instruments in place at the AIVD or the MIVD for the duty of care. Both services are now taking steps to set this up. Work is in full swing but there is no question of any instruments available or working adequately in any recognizable form. The AIVD is working hard to develop a set of instruments. It is as yet impossible to assess how this is being set up and if the application of these instruments will allow the CTIVD to exercise effective oversight. The MIVD now has a policy framework for data protection. A system for internal control is not included in policy and is still at a developmental stage.

It is crucial that the instruments for the duty of care are developed and implemented in as short a timeframe as possible. This requires a planning which reflects the importance of the duty of care. This planning has not been provided as yet. For the time being, the CTIVD is proceeding on the assumption that in its second progress report in May 2019 there will be an existing and adequately functioning set of instruments for the duty of care.

4 Letter from the Minister of the Interior and Kingdom Relations and the Minister of Defence to the House of Representatives, dated 15 December 2017, *Parliamentary documents II* 2017/18, 34588 no. 69.

The lack of ongoing internal control of the data processing by the services themselves is the principal element linking the results in all the baseline measurements conducted by the CTIVD.

Indication of risk
The CTIVD considers the risk of unlawful conduct in data processing by the AIVD and the MIVD to be **high**.[5]

3.2 Baseline measurement: data reduction

The requirement to permanently reduce data is the cornerstone of privacy protection in the ISS Act 2017. In short, the AIVD and the MIVD must assess the data they collect using special investigatory powers – such as targeted interception, hacking, requesting stored data, etc. – as quickly as possible for relevance. Non-relevant data must be destroyed immediately and irreversibly. Data not assessed for relevance must be destroyed within a year of acquisition.

There are some crucial elements of the requirement to reduce data which should be further detailed in policy and the work processes of both services.

1. When is data considered relevant and when is it not?
The services have a broad definition of relevance. The CTIVD understands this, given the importance of it for the intelligence process. However, it does consider it necessary that additional substantiation is provided about why data was judged to be relevant, if an objective assessment of the data in all reasonableness does not directly lead to the conclusion that it is relevant. This must be laid down in policy.

Indication of risk
The CTIVD assesses the risk in this area for both services as **limited**.[6]

2. How long is the assessment period?
It is part of the intelligence process that in many cases the assessment for relevance is conducted within three months. However, this does not always apply. Certainty as to what should be considered 'assessing for relevance as soon as possible' in which cases is still lacking in policy and work instructions of both services, allowing for a shift of the timing of the assessment. Significant also is the fact that provisions have not yet been made for a regulation to determine the relevance of unassessed data collected under the ISS Act 2002, other than that 'old data' which has not been assessed for relevance must be destroyed on 1 May 2019. The legal requirement of an assessment 'as soon as possible' of the relevance of data must also have effect here.

Indication of risk
The risk for both services is estimated as **average**.[7]

5 Further details are provided in section 1 of the appendix to this progress report.
6 Further details are provided in section 2 of the appendix to this progress report.
7 Further details are provided in section 2 of the appendix to this progress report.

3. How is data reduced?

Adequately implementing the legal requirement of data reduction requires a sound system of data reduction that is not only reflected in the services' policy and work processes, but that is also properly embedded in a technological sense. In addition, its functioning must be checked internally and allow for effective external oversight by the CTIVD. The latter means that the CTIVD must be able to trace on what basis data was assessed as relevant and must be able to check that non-relevant data was destroyed immediately and non-assessed data within the time limits. That kind of system for data reduction is highly complex and not easy to create. It also requires a sound ICT infrastructure.

The AIVD has developed a system for data reduction that is well-supported from a technological point of view. Assessing for relevance can be done with automated support or by hand. However, the assessment for relevance using automated support has not been sufficiently outlined yet. As yet, the AIVD has not documented clearly in which cases it is permissible to assess for relevance using automated support and how this method compares with relevance assessment by hand. Moreover, there are no internal checks whether the relevance of data is traceable. Effective oversight is therefore not yet possible.

The MIVD lacks a sound ICT infrastructure as a basis for a thorough data reduction system. Assessing for relevance is mainly done by hand. Data lineage (the origin and course of data) is incomplete and internal control of the assessment for relevance cannot be achieved at this time. In many cases, the assessment for relevance cannot be traced to a sufficient extent and effective oversight is out of the question. An adequate technical solution for data reduction is a prerequisite for the MIVD to be able to achieve lawful data reduction. This should be implemented as soon as possible and not spread out over several years as appears to be the suggestion currently.

Indication of risk
The risk for the AIVD is estimated as **average**. The CTIVD assesses the risk for the MIVD as **high**.[8]

4. What guarantees are there that data is irreversibly destroyed when so required by law?

Given the volume of data it is absolutely essential when destroying data within the time limits that there is a supporting ICT infrastructure in place to handle this. This seems to be the case for the AIVD and the set-up of the systems appear to provide for the timely destruction of data. To date, the option of declaring data as non-relevant is not yet available in many of the applications used. Nor is there any internal control. As yet, the CTIVD is therefore unable to properly assess the destruction of data. The MIVD's ICT infrastructure and incomplete data lineage insufficiently safeguard the lawful destruction of data and make internal control and external effective oversight impossible.

Indication of risk
The risk for the AIVD is estimated as **average**. The CTIVD assesses the risk for the MIVD as **high**.[9]

8 Further details are provided in section 2 of the appendix to this progress report.
9 Further details are provided in section 2 of the appendix to this progress report.

3.3 Baseline measurement: Investigation-related interception of satellite and radio communications

The ISS Act 2017 has tightened the legal framework for bulk interception of satellite and radio communications and created the option to apply bulk interception on the cable as well. This new investigatory power caused considerable political and public debate in the Netherlands, which centred on the perception of 'trawling'. The AIVD and the MIVD are currently working hard on making investigation-related interception on the cable operational. At this stage, therefore, it is too early to conduct a baseline measurement for this investigatory power. For this reason, the CTIVD is focusing on the use of investigation-related interception of satellite and radio communications. The outcome of the baseline measurement is discussed for the AIVD and the MIVD jointly.

The following legal and policy-related safeguards are important:

1. Has the process of authorization been adequately set up?

Both services have a general policy where it concerns investigation-related interception and use formats to draw up requests for authorization. Broadly speaking, the general policy and the formats provide the services' staff with sufficient guidance to submit requests for authorization to use special investigatory powers in the process of investigation-related interception. Both services submitted various requests in the period 1 May to 1 November 2018. All authorization requests ruled to be lawful by the Review Board for the Use of Powers (TIB) included all the elements required by law. In its baseline measurement, the CTIVD sees no reason to assess if the requests comply with legal requirements from a substantive viewpoint. That is for the TIB to assess.

Indication of risk
The CTIVD sees **no** risk of unlawful conduct by either of the services.[10]

2. Is the criterion 'as targeted as possible' being applied?

'As targeted as possible' pertains, in accordance with a motion proposed by member of Parliament Recourt and the Policy rules published by the ministers, to the use and application of all special investigatory powers. It therefore also relates to the special investigatory powers that may be used in the various stages of the system of investigation-related interception, such as automated metadata analysis and selection. That means that the criterion must not only be substantiated in the requests for authorization to use the investigatory power, but must also be given effect in the application of that use in practice. Failing that, the criterion is nothing more than an empty shell. In specific terms, the application of this criterion means that, for example, filtering the data to be intercepted, assigning selection criteria and using a profile for metadata analysis must all be 'as targeted as possible'. What 'as targeted as possible' means in this context must in principle first be detailed by the AIVD and the MIVD and subsequently assessed by the CTIVD. 'As targeted as possible' should thus be applied in all stages of the interception system.

10 Further details are provided in section 3 of the appendix to this progress report.

The criterion 'as targeted as possible' has not been implemented in the services' policy or work processes in any recognizable form. Neither services' policy, work instructions or actual work processes make clear how 'as targeted as possible' should be implemented in practice. It seems that since 1 May 2018 the criterion has hardly been applied at all in the different stages of the interception process, while it could – and should – have a guiding effect.

Indication of risk
The CTIVD finds that the risk for both services is **high**.[11]

3. Are there sufficient safeguards in place for automated data analysis?

The AIVD and the MIVD must request authorization for the automated analysis of metadata obtained through investigation-related interception (metadata analysis) when that analysis is aimed at the identification of persons or organizations. The policy and work processes of both services do not adequately support the lawful application of the automated analysis of metadata from investigation-related interception. The CTIVD established that for the period 1 May to 1 July 2018 the process lacked adequate procedural safeguards. Furthermore, no system of internal control had been set up.

The CTIVD subsequently decided to discuss the topic in greater depth in a legal uniformity meeting with the TIB. In that context, further consultations were conducted with the department of the Interior and Kingdom Relations, the department of Defence and with the AIVD and MIVD. Although this resulted in a noticeable, positive development at the services, there is still a fundamental difference of opinion on the legal definition of automated analysis of metadata between the TIB and CTIVD on the one hand and both services and departments on the other. The TIB and the CTIVD published their concluding point of view in a legal uniformity letter on 26 October 2018 addressed to the Minister of the Interior and Kingdom Relations, the Minister of Defence and both heads of service. On 23 November a corresponding version of the legal uniformity letter was sent to the Senate and the House of Representatives and published on the websites of the TIB and the CTIVD. The legal uniformity letters of the TIB and the CTIVD serve as a framework for the services where it concerns the implementation of that legislation, from the principle of a reasonable interpretation of the law.

In October and November 2018, the CTIVD further conducted a random check of the actual application of automated metadata analysis by both services. The results of this random check are now known. The CTIVD will first give the services and the departments the opportunity to respond to the findings before these are made public.

Indication of risk
The CTIVD assesses the risk of unlawful conduct for both services as **high**.[12]

11 Further details are provided in section 3 of the appendix to this progress report.
12 Further details are provided in section 3 of the appendix to this progress report.

4. Are there sufficient safeguards for the selection of data?

By using selection criteria to select data, the content of this data is made accessible for staff in the operational process. Determining the selection criteria is an internal assessment and must be substantiated. The services have each drawn up extensive policy regarding the selection of substantive communication. The legal requirements have been correctly laid down in it. However, the policy and work instructions of both services need to be supplemented where it concerns the internal authorization of selection criteria and to a lesser extent the removal of selection criteria. A criterion must be removed for example in the case where it yields insufficient relevant data.

Indication of risk
The CTIVD assesses the risk for both services as **limited**.[13]

5. Is responsible data reduction being implemented?

In the investigation-related interception process, data is reduced in stages. The complexity of that process is greater than the requirement to reduce data obtained by the use of other special investigatory powers, described above in section 3.2. The AIVD and the MIVD as yet have not sufficiently implemented the responsible reduction of data collected by investigation-related interception of satellite and radio communications. No specific policy has been established for data reduction within the interception system. Both services fail to sufficiently recognize the ongoing obligation in the interception process to destroy non-relevant data. It is unclear how the assessment of the relevance of data takes place after this data has been selected based on the selection criteria. As yet there is no recognizable and structured form of internal control on the destruction of data. The maximum retention period of three years has been guaranteed from a technical point of view, meaning that the intercepted data is destroyed within three years. However, there is no internal control mechanism to check this. The CTIVD cannot yet form an opinion on the usefulness or need of the three-year retention period given the limited amount of time that has lapsed. This will require further investigation in time.

Indication of risk
The CTIVD assesses the risk as **high** for both services.[14]

6. Has the division of positions and roles been safeguarded where this is required?

A division of positions and roles means that only certain staff are allocated the power to access the contents of certain data and are assigned specific roles that do not apply to others (position and role based access control). This division of positions and roles is described in more detail in the services' policies and ensures a specific and apparent division between staff (including on the 'need to know' principle). In practice, the division is more diffuse. In addition, the division of positions and roles concerns the access to the content of communication in accordance with the legal requirement in that respect. A similar legal requirement is lacking for access to metadata. However, the division of positions and roles can be a safeguard in strengthening the lawful application of metadata analysis. A division of positions and roles for access to metadata has only marginally been set up. Moreover, there is no internal control mechanism that relates specifically to the division of positions and roles. This is, however, of importance.

Indication of risk
The CTIVD assesses the risk of unlawful conduct for both services as **average**.[15]

13 Further details are provided in section 3 of the appendix to this progress report.
14 Further details are provided in section 3 of the appendix to this progress report.
15 Further details are provided in section 3 of the appendix to this progress report.

3.4 Baseline measurement: complaints and reports of misconduct

The internal policy regulations of both services for handling complaints and reporting misconduct had not been completed on 1 May 2018. This has now been done. The regulations are clear, up to date, complete and in line with the applicable legal framework. The internal policy regulations are sufficiently specific and provide staff with adequate guidelines to properly handle complaints and reports of misconduct. Sufficient information is provided both within the services and outside (on their websites) about how complaints and reports of misconduct are handled by the services. The AIVD and MIVD websites also refer correctly to the CTIVD.

Indication of risk
The CTIVD finds that there is **no** risk for either service.[16]

3.5 In-depth investigation into international cooperation

Investigation into weighting notes of lead group partner services
At the end of 2017, the Minister of the Interior and Kingdom Relations and the Minster of Defence assured parliament that the weighting notes for the lead group of international partners would be ready when the ISS Act 2017 came into effect.[17] The lead group consists of European security services participating in the Counter Terrorism Group (CTG) and foreign intelligence and sigint services participating in certain cooperative relationships in the area of sigint. The CTIVD conducted an investigation into these weighting notes. That investigation has been concluded. The review report was drafted on 17 October 2018 and sent to both Ministers and heads of service on 24 October 2018. The response of the heads of the services were received on 14 and 15 November 2018. The responses from both Ministers are expected before 17 December 2018. The review report will subsequently be adopted by the CTIVD and again be submitted to both Ministers for dispatch to parliament. The CTIVD expects to be able to do so early 2019.

Investigation into exchange of unevaluated data
The CTIVD is currently conducting an investigation into the exchange of unevaluated data by the AIVD and the MIVD with foreign intelligence and security services. This investigation was started recently. It identifies which exchange of unevaluated data has taken place since 1 May 2018 and answers the question if this was lawful. Particular focus will be placed on the duty of both services to report to the CTIVD on the exchange of unevaluated data. The CTIVD expects to be able to publish the review report in the Spring of 2019.

16 Further details are provided in section 5 of the appendix to this progress report.
17 Letter from the Minister of the Interior and Kingdom Relations and the Minister of Defence to the House of Representatives, dated 15 December 2017, *Parliamentary documents II* 2017/18, 34588 no. 69.

4 Future

Baseline measurements

Baseline measurement of investigation-related interception on the cable
Early 2019 the CTIVD will conduct a baseline measurement into the way the legal safeguards have been implemented in the cable interception process. It will establish whether, and if so where, the risks of unlawful application of this investigatory power lie in internal policy, work processes, the technical set-up of systems and the internal control of the interception process. These results will be published in a second progress report in May 2019.

Baseline measurement of automated data analysis
The law provides for various sets of regulations where automated data analysis is concerned. The section that relates to the analysis of metadata obtained by investigation-related interception which is aimed at identifying persons and organizations (Section 50, subsection 1 under b of the ISS Act 2017) has been discussed in this progress report and was further implemented in the legal uniformity discussions between the TIB and the CTIVD. At the end of 2018 the CTIVD will conduct a baseline measurement into other forms of automated data analysis that take place based on Section 60 of the ISS Act 2017. These results will also be published in a second progress report in May 2019.

Investigations

Investigation into the application of filters
In February 2018, the CTIVD indicated it would review the filtering of data obtained by investigation-related interception.[18] The application of filters which are 'as targeted as possible' is a significant safeguard in the interception process. These filters determine which data may be stored to be processed further and which may not. The negative results of the recent baseline measurement have led the CTIVD to prioritize the topic of filtering. The investigation will be started immediately and will result in a review report mid-2019.

Investigation into selection
The AIVD and the MIVD are legally permitted to establish internally which selection criteria, such as telephone numbers, IP addresses and key words, will be used to implement the power of selection. The selection criteria do not need to be submitted to either the minister concerned or the TIB and are therefore exempt from prior authorization. The CTIVD will assess whether the selection criteria are applied in as targeted a manner as possible and whether they are sufficiently substantiated internally. After selection, the services must assess the substantive communication on relevance for any ongoing investigation. It is as yet unclear to the CTIVD if and how this assessment is made. The CTIVD follows the principle used in the explanatory memorandum to the Act that information must be assessed on relevance after selection. The investigation will also be started immediately and will result in a review report mid-2019.

Investigation into bulk hacks
Within the CTIVD and at meetings it has with the TIB, the question is often raised whether there are sufficient safeguards for the use and application of hacks with which large amounts of bulk data may be obtained. The TIB has expressly addressed this issue in its response to the draft amendment of the ISS Act 2017. With a view to a possible interim amendment of the ISS Act 2017 or the evaluation to be conducted two years after the legislation entered into force, further investigation into the use

18 Taking stock of ISS Act 2017: workable legislation, p. 5, accessible on www.ctivd.nl.

and application of bulk hacks is important. The use of the hacking power is an important aspect in the broader theme of bulk processing by the AIVD and the MIVD. The CTIVD is acutely aware of this theme. The investigation will be started before the summer of 2019 and is expected to result in a review report in the second half of 2019.

Investigation into travel data
A second topic within the theme of bulk processing by the AIVD and the MIVD concerns the use of the services' general investigatory power which also allows for the processing of large amounts of data. The investigation will focus on how the AIVD and the MIVD handle travel data. The investigation also will be started before the summer of 2019 and is expected to result in a review report in the second half of 2019.

Investigation into weighting notes for other partner services
The Minister of the Interior and Kingdom Relations and the Minister of Defence pledged that by 1 January 2019 the weighting notes would be completed for all other foreign services with which there is a cooperative relationship and who are not part of the lead group referred to above. From May 2019, the CTIVD will investigate whether this pledge been upheld and whether the contents of the weighting notes comply with the legal requirements. In this investigation it will take into account its recommendations regarding the weighting notes for the lead group of international cooperative partners, which will be published early 2019. The review report on the weighting notes for the other partner services is expected at the end of 2019.

Investigation into the functioning of weighting notes in practice
In essence, weighting notes are a written justification for the decision to cooperate with a foreign service within certain limits. In May 2019, the CTIVD will start an investigation into the functioning of weighting notes in practice. A key question will be whether the AIVD and the MIVD remain within the boundaries of the weighting notes in specific cooperative activities, such as the exchange of data and joint execution of operations. The investigation will also result in a review report at the end of 2019.

P.O. Box 85556
2508 CG The Hague, the Netherlands

T +31 (0)70 315 58 20
E info@ctivd.nl | www.ctivd.nl