Progress Report II

Functioning of the ISS Act 2017

CTIVD no. 62

[adopted on 14 May 2019]

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence and
Security Services

CTIVD no. 62

PROGRESS REPORT II

Functioning of the ISS Act 2017

Table of contents

Review Committee
on the Intelligence and
Security Services

CTIVD no. 62

PROGRESS REPORT II

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 there is a balance between the General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service's (MIVD) far-reaching, necessary investigatory powers to protect national security and 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, in part on the express request of parliament and the government[1], 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.

Progress report I

In December 2018 the CTIVD published its first progress report on the introduction of the ISS Act 2017. The overall view that emerged was that the AIVD and the MIVD still have fundamental steps to take in implementing important parts of the new legislation. Both services lagged behind and ran a high risk of unlawful conduct in certain areas. Vital safeguards for citizens' legal protection still lacked, partly or wholly, implementation in internal policy, work processes and the set-up of technical systems. There were no instruments for the compulsory internal control and partly because of that, effective external oversight by the CTIVD was not yet sufficiently guaranteed. In the short-term, the AIVD and the MIVD had to take concrete measures in their organizations to ensure that the requirements of the ISS Act 2017 would be met in practice.

Focus

As a result of the first progress report, the AIVD and the MIVD have each set up an 'ISS Act board' within their organization, with the intention of addressing the risks established by the CTIVD structurally and in full. The CTIVD closely monitored the ISS Act boards' activities and regularly reflected on those activities. This concerned an assessable time schedule, newly drafted policy and work instructions, the set-up of work processes and technical systems and the plan for a system of compliance and internal control which would also guarantee effective external oversight by the CTIVD. The specific

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).

steps taken by the services are detailed in this second progress report. The report focuses on the following topics:

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** continuously during the processing of data obtained by the use of special investigatory powers, focusing on the application of the duty to assess data as quickly as possible for relevance and to immediately destroy non-relevant data; and
3. the use of the power of **investigation-related interception** including the application of the criterion 'as targeted as possible' and the use of the special investigatory power of **automated metadata analysis** under Section 50 of the ISS Act 2017.

Furthermore, the CTIVD conducted a baseline measurement of the implementation of a general power for which the ISS Act 2017 contains a legal regulation for the first time. This relates to:

4. the use of the **general power** of **automated data analysis** under Section 60 of the ISS Act 2017 in the context of the regular intelligence process of both services;

The CTIVD also conducted four in-depth investigations, of which one has been completed. They concern the following topics:

5. collecting data in as targeted a way as possible by the **application of filters** and processing data in as targeted a way as possible by the **use of the power of selection** in the context of the system of investigation-related interception; and
6. the **cooperation with foreign services**, including the existence and the content of **weighting notes** (completed) and the exchange of **unevaluated data**.

Explanation

In the context of the progress and conducted baseline measurement relating to Section 60 of the ISS Act 2017, the CTIVD assessed marginally whether the legal and pledged policy-related safeguards had been implemented further in the AIVD and MIVD's policy and work processes and in the set-up of their technical systems for data processing. Each assessment is an estimate of the risk of unlawful conduct and is not a decision that unlawful conduct has in fact taken place. The assessment of lawfulness in practice is made in the CTIVD's in-depth investigations and is reflected in the review reports. The appendix to this progress report briefly discusses which method the CTIVD used in its oversight activities into the functioning of the ISS Act 2017. The appendix also provides further explanation of the progress made by both services in implementing the legislation and removing the previously established risks of unlawful conduct. The appendix has not been translated into English.

2 Progress made by the services

2.1 Overall view

The ISS Act 2017 has struck a legal balance between the necessary investigatory powers that may be used by the AIVD and the MIVD in the interest of national security and the safeguards for the legal protection of citizens that are at issue. A similar balance must also be realized in practice. That requires sufficient scope for the operational effectiveness necessary to both services. At the same time, the collection and processing of data must take place within the framework of the Act and the AIVD and MIVD must be in control of the activities conducted as part of their legal duties. The other side of the balance, the requirements set by law, first and foremost serves the legal protection of citizens. That means that the services must be able to vouch for the quality of their data processing and that in doing so they further improve the professionalism of their conduct. National security and legal protection are inextricably linked. The services are tasked with the duty to continuously strike the appropriate balance.

In its first progress report of December 2018, the CTIVD established that both services had a backlog in implementing legal safeguards. The Minister of the Interior and Kingdom Relations and the Minister of Defence who are politically responsible for the AIVD and the MIVD respectively, concurred.[2] There was an imbalance. The AIVD and the MIVD seriously addressed the risks identified by the CTIVD and have taken specific steps to mitigate them. The services are fully aware of the necessity for this. Most of the high risks from the first progress report have now been reduced to average or limited risks.[3] The AIVD and the MIVD have worked hard but they are not there yet. The services have partly caught up on the backlog they had when the legislation entered into force. The CTIVD will continue to monitor the progress closely and will report again in the coming progress reports.

In the first quarter of 2019, the AIVD and the MIVD have established, in accordance with the pledge from both Ministers[4], an assessable time schedule indicating what they aim to complete and when, as regards the implementation of the legislation. This provides a guide for what can be expected from both services. The time schedule to 1 May 2019 has largely been achieved. However, there is a differentiated picture in the progress that each service has accomplished. That is partly because of the difference in approach and partly because of the fact that the AIVD is able to act more decisively compared to the MIVD.

The AIVD focused its efforts on rectifying the shortcomings in its policy and work instructions as quickly as possible based on the CTIVD's findings in its first progress report. These consisted in part of amendments on paper that needed to be put into effect in specific work processes and the set-up of technical systems. It will take some time before this is completed, but the AIVD's ICT infrastructure seems to provide sufficient support to achieve this. The CTIVD will continue to review this in the coming period.

2 *Parliamentary Documents II* 2018/19, 34588, no. 80.
3 The appendix to the second progress report explains in greater detail the definitions of high, average and limited risks.
4 *Parliamentary Documents II* 2018/19, 34588, no. 80.

The MIVD took a wider approach and mainly sought to better identify its own work processes and use that as a basis on which to make structural improvements. That approach does not show concrete results as quickly. In addition, there are restrictions in the technical implementation of legal requirements, such as data reduction and internal control, in the short term, because of the MIVD's supporting ICT infrastructure. That requires a modernization of the infrastructure, which is a longer-term process. Although the CTIVD understands that this will take time, it feels it is important that concrete results are made visible in the meantime. The ISS Act 2017 has now been in force for a year and it is therefore imperative that the requirements set by law are complied with in the shortest possible time.

2.2 Progress regarding the duty of care

The AIVD and MIVD's legal duty of care of lawfully processing data means that both services must themselves continuously monitor the way in which they process data. They must ensure compliance with the law themselves and continue to do so. That requires the use of instruments that provide them with a central view on the functioning of processes and systems of data processing and that enable them to identify risks and take measures promptly. A well set-up duty of care not only contributes to compliance but also serves the professionalism and operational integrity of both services. In its first progress report, the CTIVD established that there was no set of instruments in place at the AIVD or the MIVD for the duty of care.

AIVD

The AIVD set to work very energetically. It established an overall framework of standards in which data protection by design and by default[5] are guiding for the measures to be taken. Instruments such as risk analyses and audits were also implemented and are already used in practice for internal control. The AIVD has made good progress on imbedding the duty of care within the organization. This is done on the basis of a clear control structure that should ultimately enable the AIVD itself to exercise continuous control over the data processing that occurs within the service.

Indication of risk
In view of the progress achieved in a short period and the concrete implementation given to the instruments by conducting risk analyses and audits, the CTIVD has scaled down the risk **from high to limited**. To maintain this risk indication or reduce it to 'no risk', it is important that the AIVD continues along the same lines.[6]

MIVD

The MIVD made a good start on setting up the duty of care. Decisions were taken regarding the policy framework to be applied, the control structure to be set up and the corresponding instruments, but implementation has been limited. At the beginning of May 2019, a policy framework was established which included the general principles of data protection (including data protection by design and by default) that serve as the starting point for measures to be taken in the context of the duty of care. The decision was taken to organize the duty of care based on a control structure similar to that of the AIVD, with corresponding instruments such as risk analyses and audits.

5 Data protection by design means that data protection is included and built in when the processes are set up and the applications and systems are designed. Data protection by default is a related term. It means that standard settings in applications and systems are set up in such a way that they provide maximum data protection. To adjust these, users must take additional actions. Therefore, applying a level of data protection that is lower than the standard settings must be a conscious act each time.
6 Further details are provided in chapter 2 of the appendix to this progress report.

However, to date only tentative steps have been taken to set this up within the service. The MIVD has made investments to further map out its own work processes with the aim of improving them.

Indication of risk
The CTIVD has scaled down the risk **from high to average** given that in the coming six months the MIVD will further implement the decisions taken.[7]

2.3 Progress regarding data reduction

The AIVD and the MIVD must assess the data they collect using special investigatory powers 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. Data collected by investigation-related interception falls outside this regulation, as it is subject to a three-year retention period. In its first progress report, the CTIVD established, among other things, that policy and work instructions were lacking in key areas, the destruction of data had not yet been fully safeguarded and that internal control and therefore effective oversight was out of the question. Where the MIVD is concerned, this was partly caused by an ICT infrastructure that provides limited support.

AIVD

The AIVD worked on drafting new policy and work instructions. In some areas, policy and work instructions are still lacking. The AIVD has committed to providing them before 1 July 2019. Progress was also made with implementing a system of data reduction in the technical systems. The system of data reduction had to be fully operational on 1 May 2019 as on this date the legal one-year term expired within which the relevance of data collected from 1 May 2018 had to be assessed. That seems to be the case. The CTIVD will conduct a technical random check in the coming period to assess the functioning in practice.

A number of previously established average risks have still not been mitigated. This concerns the leeway taken by the services to declare data to be relevant in advance, without prior substantive assessment, and the limited internal control. This implies a real risk that non-relevant data continues to be stored and that data is not always destructed within the required timeframe. As regards the two risks assessed as average – assessing data for relevance as soon as possible and the irreversible destruction of data – progress has been made to the extent that these risks can be scaled down. Assessing data under the ISS Act 2002 for relevance and, where applicable, destroying it, has now been done in part. Where the rest of the data is concerned, an extension of the retention period was given in accordance with the legal regulation, so that data must be either assessed as relevant or be destroyed by 1 November 2019.

Indication of risk
The CTIVD has scaled down the risks regarding the AIVD assessing data for relevance as soon as possible and irreversibly destroying data **from average to limited**. The other risks in the area of data reduction, which were previously established as **limited and average risks,** will persist.[8]

7 Further details are provided in chapter 2 of the appendix to this progress report.
8 A specification for each part of data reduction and a further explanation are provided in chapter 3 of the appendix.

MIVD

The MIVD's policy is largely in place. However, the MIVD has made only limited progress in implementing data reduction. This has to do with the quality of their supporting ICT infrastructure. For the MIVD also, 1 May 2019 is an important reference date for the destruction of non-relevant data and for the requirement that the system of data reduction must be fully operational on that date. However, problems continue with the technical implementation of that system which is meant to support the assessment of data for relevance as soon as possible and the immediate destruction of non-relevant data. Destruction of data on expiry of the retention period has partly been automated. However, internal control on that data reduction process has not yet been accomplished. In April 2019, the MIVD initiated an ICT pilot project aimed at developing a modern data architecture. Restructuring the ICT landscape will take several years and no end date has been set for this process. The previously established average and high risks therefore persist. One exception is assessing the relevance of data as soon as possible, including data collected on the basis of the ISS Act 2002. Just like the AIVD, the MIVD has made concrete progress in this area, in line with the ISS Act 2017.

Indication of risk

The CTIVD has scaled down the risk regarding the MIVD assessing data for relevance as soon as possible **from average to limited**. The other risks in the area of data reduction **continue to be average and high.**[9]

2.4 Progress regarding investigation-related interception

The ISS Act 2017 allows for the possibility to collect personal data in bulk, both from satellite and radio communications and from the cable, in order to process this further. Important safeguards for the legal protection of citizens include the following: that the special investigatory powers, including in the context of investigation-related interception, are applied in as targeted a way as possible and that the acquired data is reduced as quickly as possible to the information that is relevant to both services for investigation-related interception. In its first progress report the CTIVD established, among other things, that the criterion 'as targeted as possible' had not been implemented in any recognizable form, that the process of metadata analysis had insufficient procedural safeguards, that there was no specific policy on data reduction and it was unclear how this was done within the interception system, that internal control on these processes was lacking and that as a result, effective oversight was impossible.

Progress by the AIVD and MIVD

Both services have improved their policy and work instructions, including on the application of the criterion 'as targeted as possible' and on data reduction in the interception system in the wider sense. Work instructions are still lacking in some areas. These are important in order to guide the application in practice, including the filtering of data on acquisition. Moreover, the policy must for a large part still be implemented in the services' technical systems. Metadata analysis[10] is defined in accordance with the Act. In practice, a balance must now be sought between the day-to-day workability and the legal protection of citizens when applying metadata analysis. Specific policy and work instructions are still required to provide direction. In the autumn, the CTIVD will conduct a second random test of the application of metadata analysis.[11] In addition, the services have made improvements in safeguarding the division of positions and roles.

9 A specification for each part of data reduction and a further explanation are provided in chapter 3 of the appendix.
10 This relates to the power to apply automated data analysis on metadata obtained from investigation-related interception, under Section 50 of the ISS Act 2017.
11 A first random test was conducted at the end of 2018 and is discussed in chapter 5 of the appendix.

A key issue is designating data selected by 'targeted' selection criteria as relevant beforehand, without basing this on any substantive assessment of that data. This entails the risk of non-relevant data being stored. In the CTIVD's opinion, this should only occur in exceptional circumstances which need to be properly substantiated and recorded. The CTIVD is currently in talks with the AIVD and the MIVD to discuss under which conditions an assessment for relevance with automated support could be conducted so that sufficient safeguards for the legal protection of citizens are provided. Adequate internal control of the system of investigation-related interception is as yet insufficiently provided for, making effective external oversight impossible. The AIVD and the MIVD are currently working on setting this up.

Indication of risk

The previously established high risks regarding the application of 'as targeted as possible' for metadata analysis and regarding the assessment of relevance in the context of investigation-related interception for the AIVD and the MIVD have been scaled down **from high to average**. As regards the division of positions and roles, the risk for both services is scaled down **from average to limited.**[12]

12 A specification per segment of investigation-related interception and a further explanation are provided in chapter 4 of the appendix.

3. Baseline measurement of automated data analysis under Section 60

Automated data analysis under Section 60 of the ISS Act 2017 covers a wide range of data processing activities that are automated and part of the AIVD and MIVD's daily activities. These include simple search sessions but also complex techniques such as profiling. Authorization from the Minister concerned and subsequent review by the TIB do not apply. This is in contrast to the use of the special investigatory power of automated analysis of metadata obtained by investigation-related interception (see section 2.4 and chapter 5 of the appendix).

The use of automated data analysis techniques may imply a variety of risks. Algorithms are able to analyse data much faster and more consistently than humans, but may generate an incorrect or skewed outcome. The extent of the risk related to automated data analysis depends, among other things, on the complexity of the algorithm and on the data used in the analysis. The services must have the tools to identify and mitigate these risks, in order to have continuous control over this type of data processing.

The ISS Act 2017 provides a specific legal basis for automated data analysis for the first time. The associated package of safeguards relates to the entire lifecycle of automated data analysis techniques – from development or acquisition (for example a purchased technology) to the contribution the result makes to day-to-day decision making. In a baseline measurement, the CTIVD assessed how the AIVD and the MIVD implemented these safeguards in their policy and in the processes.

How do the AIVD and the MIVD interpret the concept of automated data analysis?

The CTIVD has drawn up a legal framework on what the interpretation is of automated data analysis according to the law. The AIVD and the MIVD have endorsed this framework in broad outlines. However, the scope of the term automated data analysis has not yet sufficiently taken shape in the services' policy and work instructions. Thus the AIVD and the MIVD have failed to sufficiently regulate these activities. That means that there is a risk that data processing activities now mistakenly not considered to be automated data analysis are not subject to necessary safeguards.

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

How do the AIVD and the MIVD check the functioning of automated data analysis techniques?

The check on the functioning starts at the development or acquisition of the technique. It is important that, during the development process, the necessary steps are built in to create an algorithm that will process data within the framework of the law. The development phase includes and is followed by the validation: the check on the algorithm's functioning. This process of development and/or validation must be conducted and recorded thoroughly. In addition, there must be safeguards that the end users in the services' operational teams have sufficient knowledge of the functioning of the techniques to be able to correctly interpret the outcome of the automated data analysis. The checks on the functioning of the techniques do not end the moment an automated data analysis technique is put into use within the organization, but must instead be part of an ongoing process in which the end users' feedback is also incorporated.

In broad outlines, the AIVD's policy provides a basis for the safeguards referred to above. However, this policy has not yet been specifically implemented in work instructions for every department working on the development or testing of the algorithms' functioning. The MIVD has not yet regulated the check on the functioning of automated data analysis techniques in its policy and only marginally in its work instructions. Both services therefore run the risk of inadequate monitoring and control of the functioning of the automated data analysis techniques used.

Indication of risk
The CTIVD assesses the risk for the AIVD as **average** and for the MIVD as **high**.

Which safeguards are in place for the use of automated data analysis techniques in investigations?

The law regulates that data processing, which includes automated data analysis, must have a specific purpose and must be necessary for the implementation of the ISS Act 2017. In addition, the requirements of proper conduct (including proportionality), due care and an indication of reliability or source apply. For automated data analysis specifically, this means that certain deliberations should take place before an automated data analysis technique can be used in an investigation. The content of those deliberations depends on the investigation interests and the functioning of the automated data analysis technique to be applied – to what extent does this technique infringe the privacy of the people whose data will be used? Furthermore, it is important that the level of reliability of the underlying data and the outcome of the automated data analysis are apparent.

In light of the risks related to the use of algorithms, the law prohibits facilitating or taking measures on the basis of automated data analysis outcomes only. In other words, the law prohibits automatic decision making. Translated to the practice of the AIVD and the MIVD, this prohibition means that operational decisions and actions that have substantial consequences for people or groups of people may not be exclusively based on the outcome of an automated data analysis but must first be assessed by a person.

The AIVD and the MIVD have not implemented these legal requirements in any specific form in their policy or work instructions. That lack of implementation leads to a high risk of staff using automated data analysis for their investigations without making the necessary deliberations beforehand and not knowing to what extent they may base operational decision making on the outcome without additional verification.

Indication of risk
The CTIVD assesses the risk for the AIVD and the MIVD as **high**.

4 Current situation of in-depth investigations

4.1 Investigation-related interception of satellite communications

During the parliamentary debate on the ISS Act 2017 and in the run-up to the subsequent advisory referendum, public debate centred mainly on the expansion of the existing 'bulk interception powers' of satellite and radio communications to cable (such as internet traffic through cables in the ground). The application of the criterion 'as targeted as possible' and compulsory continuous data reduction are important safeguards for the legal protection of citizens in the process of investigation-related interception. In the first progress report of December 2018, the CTIVD established a high risk for the implementation. That compelled the CTIVD to prioritize the assessments of the lawfulness of the filters applied and the use of the power of selection in the context of investigation-related interception in practice.

Investigation into the application of filters

The filters used during interception determine which data may be stored by the services to be processed further and which may not. The filters must be applied in an as targeted way as possible. In other words, the filters determine whether the interception is 'untargeted' or 'investigation-related'. The AIVD and MIVD's new policy for filtering in the context of investigation-related interception is generally in line with the legal assessment framework that the CTIVD drew up for the investigation. Both services endorse the principles of the assessment framework. For example, filtering must remain within the boundaries of the Integrated Security and Intelligence Order and the investigation assignments based on it, the 'as-targeted-as-possible' requirement is a guideline for filtering, the immediate destruction of non-relevant data is described, filtering is viewed as an elementary part of responsible data reduction and the necessity of reducing data is recognized where it concerns special groups of people such as lawyers and journalists. Notwithstanding the above, the services' policy only sketches in outlines how filtering should be conducted. Work instructions must be detailed further if they are to provide concrete guidelines for the application of filtering in practice (see also section 2.4 and chapter 4 of the appendix).

The investigation assesses how filtering was in fact conducted regarding the various flows of satellite and radio interception. The CTIVD assesses whether the previously established high risks did indeed manifest themselves. The investigation covers the period from 1 May 2018 to 1 February 2019. It focuses on filtering interception of satellite and radio communications but is also significant for the investigation-related interception on the cable. The results will be published in a review report in the summer of 2019.

Investigation into the use of the power of selection

The power of selection entails learning the contents of intercepted communication and assessing it for relevance. Data is selected based on selection criteria such as telephone numbers, IP addresses and email addresses. A selection may also be made based on keywords. When selecting, the requirement 'as targeted as possible' has different lines of approach. The CTIVD explains this in more detail in the legal framework it uses in the investigation. That includes the following elements: 1) Authorization from the Minister involved must be requested for the selection of data from a person, organization or a topic. This is assessed by the TIB. The services must substantiate why the selection cannot be more targeted and must describe the 'object' of the selection as specifically as possible. 2) It must be possible to link the selection criteria that are subsequently used to a person, organization or topic. A targeted link, for example, is a telephone number or email address belonging to a certain person. 3) The services must substantiate the choice for a certain type of selection criterion and indicate its origin. A keyword has a broader scope than a technical characteristic, such as a telephone number, and is therefore less targeted. The services subscribe to these elements and implement them in their policy.

One of the things the CTIVD examines in its investigation is whether the selection criteria used by the AIVD and the MIVD were as targeted as possible. It assesses this on the basis of the elements referred to above. The CTIVD also assesses how both services decide if the selected data is relevant and if non-relevant data is destroyed promptly. In its first progress report of December 2018, the CTIVD established a high risk of unlawful conduct when selected data was designated as relevant in advance without this data being assessed on its content (see section 2.4 and chapter 4 of the appendix). The investigation looks at whether the risk – wrongly storing non-relevant data – manifested itself in practice. The CTIVD is investigating five operations to obtain a clear picture of the use of the power of selection. The report is expected to be published in the summer of 2019.

4.2 International cooperation

Investigation into weighting notes of lead group partner services (completed)

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.[13] 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. The review report was published on 6 February 2019.

The investigation showed that the weighting notes of the AIVD and the MIVD were completed in time but were not up to standard in terms of content. The quality of the weighting notes must be improved if they are to provide a clear insight into the risks that are connected with cooperation with the foreign service in question. The Minister of the Interior and Kingdom Relations and the Minister of Defence adopted the recommendations and indicated that the revision of the investigated weighting notes would be completed by 1 July 2019. The CTIVD will review this.

Investigation into the provision of unevaluated data

The CTIVD is currently conducting an investigation into the provision of unevaluated data by the AIVD and the MIVD to foreign intelligence and security services. This investigation was started in the autumn of 2018.

The CTIVD has drawn up a legal assessment framework for the provision of unevaluated data based on the ISS Act 2017, legislative history, previous review reports and the subsequent conclusions and recommendations adopted by the Minister(s). This assessment framework was discussed with the AIVD and the MIVD and endorsed by them. The CTIVD also analysed and assessed the services' policy. It established that policy was largely in line with the legal regulation and in that sense provided sufficient guidance to lawfully provide unevaluated data. However, in several areas policy is lacking or the policy has shortcomings. For example, it is important that the services record the best-efforts obligation that technical characteristics of lawyers and journalists are removed from unevaluated data before this data is provided and that they specify in which cases this applies to Dutch characteristics in general. The AIVD also lacks policy and work instructions to centrally record the provision of unevaluated data, so that there is no up to date overview of this. The MIVD also lacks work instructions and an overview of the data provided. Both services have pledged to supplement or correct their policy and work instructions in the short term.

13 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 investigation further focuses on the procedure and the practice of the AIVD and the MIVD regarding the provision of unevaluated data in the period 1 May to 31 December 2018. It identifies the unevaluated data provisions and their nature and scope. The question will then be addressed whether this was done lawfully. Particular focus will be placed on the duty of both services to report to the CTIVD on the exchange of unevaluated data. The findings and conclusions of this investigation will be published in a review report that is expected to appear in the summer of 2019.

Support of foreign services

In the context of its current in-depth investigations, the CTIVD found situations in which the MIVD used special investigatory powers to support a foreign service. Supporting foreign services is permitted by law, if authorization from the Minister has been obtained and the applicable legal requirements have also been met. This is regulated in Section 89 (4)-(6) of the ISS Act 2017 and is further explained in the legislative history. If this support involves the use of a special investigatory power by the AIVD or the MIVD, the authorization granted by the Minister must be submitted to the TIB for a lawfulness assessment. The latter was omitted and is therefore unlawful.

The CTIVD discussed this topic in its legal uniformity consultations with the TIB and in meetings with the department of the Interior and Kingdom Relations, the department of Defence and with the AIVD and MIVD. The topic was also addressed in a legal uniformity letter by the TIB and the CTIVD on the scope of the lawfulness assessment of the TIB. This letter was sent to the Senate and the House of Representatives on 23 November and published on the websites of the TIB and the CTIVD.[14] The ministers involved responded in a letter of 19 March 2019.[15] They indicated that the conduct was not consistent with the legal regulations and that the current practice has now been brought into line with these regulations.

14 *Parliamentary Documents II* 2018/19, 29924, no. 174.
15 *Parliamentary Documents II* 2018/19, 29924, no. 179.

5 Future

Progress reports

The oversight activities into the implementation 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 to start 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.[16] The CTIVD reports to the Ministers involved and to Parliament at least every six months. The third progress report will be adopted in November 2019 and the fourth in May 2020.

Baseline measurements

Baseline measurement of investigated-related interception on the cable

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 reason, the CTIVD is focusing on the use of investigation-related interception of satellite and radio. As soon as investigation-related interception of the cable has become operational, the CTIVD will conduct a baseline measurement of the implementation of legal safeguards in that respect. These results will be published in the subsequent progress report in November 2019 or May 2020.

Random checks

Random check of the functioning of the data reduction system

1 May 2019 was a significant date for the services, because on this date the legal one-year term expired to assess the relevance of data collected from 1 May 2018 with the use of special investigatory powers (except investigation-related interception). From 1 May 2019 the system of data reduction therefore had to be fully operational. The CTIVD will conduct a technical random check in the coming period to assess this in practice.

Random check of metadata analysis under Section 50

In the autumn of 2019, the CTIVD will conduct a second random test of the application of metadata analysis under Section 50 and of the functioning of an adequate internal control mechanism. The AIVD aims to have this completed before 1 August 2019. The results of the random check will be included in the progress report of either November 2019 or May 2020.

Random check of automated data analysis under Section 60

A random check of the use of automated data analysis is important to assess the extent of the risks in the implementation. This is a supplement to the baseline measurement by the CTIVD that focused on the policy and work instructions of both services. The CTIVD aims to conduct this random test before the end of 2019.

In-depth investigations

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 the evaluation to be conducted two years after the legislation entered into force, further investigation into the use 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.

16 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).

The CTIVD places emphasis on this theme. The investigation will be initiated before the summer of 2019 and is expected to result in a review report at the end 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 power which also allows for the processing of large amounts of data. The investigation will focus on the processing of travel data by the AIVD and the MIVD. The investigation will also be initiated before the summer of 2019 and is expected to result in a review report at the end of 2019.

Investigation into the weighting notes of the AIVD and the MIVD
The Minister of the Interior and Kingdom Relations and the Minister of Defence have committed to having completed by 1 January 2019 the weighting notes for all other foreign services with which there is a cooperative relationship and who are not part of the lead group of foreign services which were the topic of the CTIVD's review report no. 60. The recommendations from report no. 60 were adopted by the Ministers involved. They indicated that the revision of the investigated weighting notes would be completed by 1 July 2019 at the latest. From July 2019 the CTIVD will investigate whether these two commitments have been fulfilled and whether the substance of the weighting notes is up to standard. The review report on the weighting notes is expected at the beginning of 2020.

Investigation into cooperative activities in practice
In essence, weighting notes are a written justification for the decision to cooperate with a foreign service within certain limits. In the summer of 2019, the CTIVD will start an investigation into the functioning of weighting notes in practice. A key question of the investigation will be whether the AIVD and the MIVD remain within the boundaries of the weighting notes in the specific cooperative activities, such as the exchange of data and joint execution of operations, and whether these cooperative activities also comply with the requirements of the ISS Act 2017. The investigation will also result in a review report at the beginning of 2020.

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

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