Review report

On bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

CTIVD no. 70

[adopted on 19 August 2020]

CTIVD
Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence
and Security Services

CTIVD no. 70

REVIEW REPORT

On bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

Inhoudsopgave

Review Committee
on the Intelligence
and Security Services

CTIVD no. 70

REVIEW REPORT

On bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

Summary

Bulk data sets

The General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) are allowed to collect bulk data sets using general and special investigatory powers, such as the hacking power. Bulk data sets are large collections of data, the majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. That means that it mostly concerns data of people who are not the focus of the services. Bulk data sets are of immense value to the performance of the services' tasks, and their value lies, besides in the deeper analysis of recognized threats, particularly in recognizing and identifying unknown targets and threats.

The downside is that collecting and further processing personal data in a bulk data set constitutes a severe privacy infringement. It is therefore important that the fundamental rights of those involved who are not under investigation by the services are sufficiently protected.

The Intelligence and Security Services Act 2017 (ISS Act 2017) does not lay down any specific rule for processing bulk data sets, with the exception of investigation-related interception, or bulk interception. The investigation

Exercising the hacking power is one of the special investigatory powers which the AIVD and the MIVD can employ to collect bulk data sets. This is a special investigatory power with which to explore and enter into a automated device or system and copy the data stored on this automated device or system (Section 45 of the ISS Act 2017).

This investigation focuses on the exercise of the hacking power when collecting bulk data sets and not on the practice as a whole. The investigation concentrates on a number of areas that are new in the ISS Act 2017 and that are important safeguards for legal protection, i.e. the review by the independent Investigatory Powers Commission (TIB), the description of technical risks, the exercise of the 'clean-up obligation' and reporting on the exercise of the investigatory power.[1] The lawfulness assessment by the TIB as such is not part of this investigation.

1 The term clean-up obligation refers to the best-efforts obligation in Section 45(7) of the ISS Act 2017 to remove the technical aids used in a hack, after the hacking power has been used. This topic is examined in more detail below in Section 2.5.

Furthermore, this report looks at how the services deal with the reduction of data in bulk data sets and the related assessment for relevance. Finally, we look at how the AIVD and the MIVD limit the infringement of fundamental rights when further processing bulk data sets obtained through hacking. Both the AIVD and the MIVD use safeguards when accessing and using bulk data sets. These extra safeguards stem from the general obligation to ensure data is processed properly and carefully (Section 18 ff. of the ISS Act 2017) and are an implementation of their duty of care as regards lawfulness and quality of data processing (Section 24 of the ISS Act 2017).

This approach to the topic 'bulk hacks' means that in fact the investigation falls into two parts – the first dealing with the use of the hacking power and the second with the further processing of the bulk data sets collected using that hacking power. This divide is reflected in the two investigative questions central to this report. Consequently, one overall view cannot be properly formulated, as that view is composed of the answers to the individual subsidiary questions and subsidiary topics.

This investigation ties in with other investigations by the CTIVD into the use of general investigatory powers when collecting bulk data, such as report no. 55 about bulk data sets on the internet and the investigation into passenger data.

Investigative questions

The following two questions are the focus of this investigation:

1. *In the period investigated, did the AIVD and the MIVD lawfully use the hacking power when collecting bulk data sets ('bulk hacks')?*

2. *In the period investigated, did the AIVD and the MIVD lawfully further process the bulk data sets obtained by the hacking power?*

The investigation covers the period from 1 May 2018, the date on which the ISS Act 2017 entered into force, to 1 November 2019.

Answer to investigative question 1

The answer to the first main question can be broken up into four subsidiary questions and topics, which are discussed separately below.

Subsidiary question 1: Did the collection of the bulk data sets using the hacking power in the investigation period take place on the basis of an authorization request found to be lawful by the TIB? (Section 2.3)

The introduction of the ISS Act 2017 means that certain special investigatory powers, including the hacking power, can only be used once the authorization granted by the minister is subsequently found to be lawful by the TIB.

The CTIVD established that, of the sixteen operations investigated, data was collected in three operations requested by the AIVD after an authorization request had been rejected by the TIB. This is *unlawful,* as it disregards an important legal safeguard for the lawful use of the hacking power. Soon after the data in these operations had been collected, the AIVD itself established that collecting data following a rejection by the TIB was unlawful. Once it had established that, the AIVD went on to destroy the data in all three operations.

Three months after the ISS Act 2017 entered into force, data was collected in one operation based on an authorization granted by the minister under the ISS Act 2002. With the introduction of the ISS Act 2017 a request for authorization should have been submitted on time to the TIB for assessment. As the AIVD failed to do so, this data was therefore collected *unlawfully*.

The common denominator of the above operations is that a valid authorization to collect data had been granted under the ISS Act 2002 and that this data was collected in the first three months after the ISS Act 2017 had come into force.

Subsidiary question 2: Have the technical risks that could occur when using the hacking power been described in the authorization requests in line with the real-life situation? (Section 2.4)

The law requires the technical risks of exercising the hacking power to be described in requests or in extensions for the use of this investigatory power. The CTIVD established that in the investigation period the risks were generally described as low or non-existent. In practice it has proved difficult to reconstruct the risks of using the hacking power after the fact, as analyzing automated logging is time-consuming and no manual records of assessments of risks were found. Therefore the CTIVD was unable to assess whether the risk description in the requests and extensions was accurate.

Based on its investigation, the CTIVD came to the conclusion that during the investigation period the description of technical risks in the requests had a limited safeguard function. The CTIVD has taken note of the fact that the TIB had already entered into discussions about the substance of the risk description with the services both during and after the investigation period.

The CTIVD has also investigated the procedure which the services follow when it comes to taking and assessing risks. It has concluded that, with due observance of some recommendations, this procedure sufficiently safeguards an assessment of the risks.

Subsidiary question 3: Did the services comply with the clean-up obligation? (Section 2.5)

In the investigated period, the clean-up obligation was observed *lawfully* as the CTIVD did not find any operations in which technical aids had not been removed or in which the report was missing in those cases where the aids had not been removed. However, it was not always clear from the report which aids had been removed at what time and why removal had or had not been possible. That is a failing.

In a number of operations the period between the last approved authorization request for an extension of the hacking power in an ongoing operation and the first clean-up attempt was long. As the technical aids were eventually removed, the legal obligation as such was observed.

Subsidiary question 4: Did the services keep records of the use of the hacking power? (Section 2.6)

Both services, specifically the joint executive Computer Network Exploitation (CNE) department, have *lawfully* implemented the legal obligation to keep records and the relevant recommendations of CTIVD report no. 53. They do so by automated logging combined with a manual log. Keeping records of the use of an investigatory power serves internal control purposes and in addition enables effective external review by the CTIVD. This makes it possible to reconstruct assessments and actions in retrospect.

Answer to investigative question 2

The answer to the second main question can be broken up into two subsidiary questions, which will be discussed separately.

Subsidiary question 1: How do the AIVD and the MIVD deal with the legal requirements relating to the relevance assessment under Section 27 of the ISS Act 2017? (Section 3.2)

Section 27 of the ISS Act 2017 stipulates that data from special investigatory powers, including bulk data sets collected using the hacking power, must be assessed for relevance as soon as possible. Data that has not been assessed as relevant before the deadline of 18 months must be destroyed by the end of that term. Data that has been designated as not-relevant must be destroyed immediately. Given the nature of bulk data sets – consisting for the most part of data of which the relevance cannot be assessed in advance – the relevance assessment based on the criterion 'as soon as possible' is hard to execute in practice.

In the investigated period, the services have in a number of cases partially or comprehensively declared bulk data sets relevant, despite the fact that the vast majority of the data relates to organizations and/or persons who are not the subject of the services' investigation and never will be. As a result, the services are able to retain the data stored in these sets without having to destroy it within the defined destruction term of 18 months, because after being designated relevant, the data falls under the data reduction regime of significance[2].

The CTIVD considers this method of relevance assessment to be an artifice aimed at extending the retention period of the data sets in question. It is, after all, *unlawful* to declare data sets relevant that for the most part contain non-relevant data. The ISS Act 2017 does not offer scope for this. The CTIVD had already included this finding in its third progress report. The CTIVD therefore sees no other options than to recommend destroying the bulk data sets in question immediately, as this ensues from the Act.

Subsidiary question 2: To what extent do the AIVD and the MIVD fulfil the procedural safeguards for the further processing of bulk data sets collected via a hack? (Section 3.3)

The services use their own additional safeguards not explicitly laid down in the law, to access and use the collected bulk data sets. These are included in general published policy and are an interpretation of the general requirement of proper and careful processing of data and the services' duty of care for the lawfulness and quality of data processing (Sections 18 and 24 of the ISS Act 2017). Although these safeguards have not been set out in overall policy for bulk data sets collected using the hacking power, it is existing practice for the services to work with an 'outer box/inner box' procedure where it comes to bulk data sets collected using the hacking power. This procedure provides for a division of job roles and an authorization procedure (Internal Check) to access the data. The CTIVD finds the division of job roles and this authorization procedure, with due observance of the comments and recommendations, to be a sufficient implementation of the requirements of proper and careful data processing that the law sets.

In conclusion

The lack of a more specific legal regime for bulk data means that ultimately the CTIVD can only assess the lawfulness of the safeguards taken by the services against the general requirements that apply to all data processing, such as Section 18 of the ISS Act 2017.

2 Data within this data reduction regime may be stored until it has lost its significance for the task of the service.

Although the general principles for data processing form a starting point for the lawfulness assessment in this report, they do not, in the CTIVD's view, offer a sound legal framework for the processing of bulk data sets and the exercise of a lawfulness review on it. It is therefore advisable to turn to a more inclusive legal regulation of bulk data sets that does sufficient justice to the protection of citizens' fundamental rights and the operational value of bulk data sets for the services.

Structure of the report

The report has the following structure:

- Section 2 contains the findings and conclusions about the policy, work instructions and practice of the AIVD and the MIVD concerning the use of the hacking power when collecting bulk data sets ('bulk hacks') in the investigated period. The applicable legal assessment framework is discussed in greater detail in Appendix II to this review report. Each section presents the essence of this assessment framework.
- Section 3 contains the findings and conclusions about the policy, work instructions and practice of the AIVD and the MIVD concerning the further processing of bulk data sets collected using the hacking power. The applicable legal assessment framework is discussed in greater detail in Appendix II to this review report.
- Section 4 looks briefly at the problems around bulk data sets and the ISS Act 2017.
- The conclusions of the investigation are set out in Section 5.
- Finally Section 6 lists the recommendations per phase and per service.

The report has the following appendices:

- Appendix I: Investigation plan and methodology
- Appendix II: Legal framework
- Appendix III: Definitions

This report has a classified appendix, in which the nature and course of the operations referred to in Section 2.3 are discussed in more detail. The appendix also contains a further explanation of the relevance assessment method described in Section 3.2. The classified appendix has eight pages and does not include any reports of unlawful conduct that have not been included in the public review report.

CTIVD no 70

REVIEW REPORT

On bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

1. Introduction

Using the hacking power to collect and further process bulk data sets

The General Intelligence and Security Service (AIVD) and the Military Intelligence and Security Service (MIVD) have the special investigatory power to enter automated devices and systems, also known as the hacking power (Section 45 of the ISS Act 2017). The Privacy Impact Assessment (PIA), conducted in the run up to the current ISS Act 2017, referred to the hacking power as 'the most intrusive power imaginable'. Although this investigatory power already existed in the precursor (the ISS Act 2002) to current legislation, the greater role of computers and the introduction of smartphones and similar devices in daily life have made it 'even more intrusive'.[3] During hacks, not only is data obtained in the course of transmission, but also, in particular, stored data which is obtained retrospectively.

Although the hacking power must be targeted at a specific automated device or system, the investigative power does not regulate which data may be copied after the hack. Thus legislation leaves a lot of scope to obtain large amounts of data using this investigatory power. This includes what is known as 'bulk data sets'. A bulk data set is a large collection of data, the vast majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. Given the nature and volume of data to be acquired, an estimate can often be made in advance that the majority of the bulk data will contain data that is not relevant to the services' performance of tasks.[4] However, from an operational or technical perspective it may nonetheless be necessary for the services to collect these bulk data sets. This is because the work of the intelligence services involves recognizing threats to national security in time, including exposing as yet unknown threats. Bulk data sets are of immense value to the performance of the services' tasks, particularly to recognizing and identifying unknown targets and threats. The ISS Act 2017 therefore provides scope for this.[5]

Background to the investigation

Because a bulk data set contains large amounts of personal data, the vast majority of which concern organizations and/or people who are not the subject of investigation by the services, nor ever will be, collecting and further processing it constitutes a severe interference of privacy.

3 *Parliamentary Documents II* 2016/17, 34 588, no. 3 (Appendix 787332 external advisory opinion PIA), p. 107; *Parliamentary Documents II* 2016/17, 34 588, no. 3 (MVT), p. 75.
4 Review report 39 on the lawfulness of the investigation on social media by the AIVD (2014) p. 13, *Parliamentary Documents II* 2013/14, 29 924, no. 114 (appendix), accessible on www.ctivd.nl.
5 See the legal assessment framework to this investigation included in Appendix II, Section 3.3.

The fundamental rights of those involved who are not under investigation by the services must therefore be sufficiently protected. This investigation is consistent with other CTIVD investigations into the use of the general investigatory power when collecting bulk data, such as report no. 55 on bulk data sets on the internet and the investigation into passenger data.[6]

What are the safeguards?

In general the law stipulates that data should be processed properly and carefully. Furthermore, a subject of case law including at European level is the development of safeguards for collecting and processing bulk data sets.[7] In contrast to bulk data obtained by investigation-related interception, the ISS Act 2017 does not have a more detailed regime for processing bulk data sets.[8]

One of the main safeguards for the legal protection of citizens in the ISS Act 2017 when processing data collected using special investigatory powers is the requirement of continuous data reduction. A key element is the obligation to assess the data for relevance as soon as possible and to destroy non-relevant data (Section 27 of the ISS Act 2017). However, this proves hard to carry out in practice where bulk data sets are concerned. Because of the nature and size of these data sets, little or no relevance assessment can be carried out on the data in advance. In addition, data that has not been assessed at the end of the 18-month term must be destroyed, whereas bulk data sets can, precisely because of their specific characteristics, be of value to the services' investigations for a significantly longer period.[9]

As well as the ISS Act 2017, the services apply certain additional safeguards to the bulk data sets obtained by the hacking power when accessing and using this data. These safeguards are an interpretation of the general requirement of proper and careful processing of data.

What have we reviewed?

The CTIVD finds it important that it identifies and conducts a lawfulness assessment of certain parts of the practice of using the hacking power to acquire bulk data sets. The CTIVD opted to restrict the current investigation to a number of elements in the law that are new.[10] These elements are laid down in the law to provide more legal protection and to mitigate certain concerns that exist in society about the exercise of this investigatory power. In specific terms this means: the requirement to conduct a lawfulness assessment by the Investigatory Powers Commission (TIB) of an authorization given by the minister to use the hacking power, the requirement to describe the technical risks in the authorization request and the obligation to clean up the technical aids after the hacking power has been exercised. These elements are assessed in this investigation. The lawfulness assessment by the TIB as such is not part of this investigation.

Furthermore, following the recommendation in report no 53, the CTIVD again looked at the keeping of records on the exercise of the hacking power, including the automated records of actions. These elements also provide a safeguard in connection with the collection of large amounts of data and the careful conduct of the services in that respect, although the functioning is not limited to that.

---

6 See review report no. 55 (published February 2018) about the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties, *Parliamentary Documents II* 2016/17, 29 924, no. 155 (appendix); the investigation into passenger data (review report no 71).

7 See Section 3.3 of the legal framework (Appendix II).

8 The legal system of investigation-related interception is categorized in three stages for interception, optimization and use/analysis of data, each subject to a separate lawfulness assessment by the TIB and the safeguard of a division of roles and/or positions pursuant to Sections 48 to 50 of the ISS Act 2017.

9 VGR III, no. 66 (published 3 December 2019), p. 9, *Parliamentary Documents II* 2019/00, 34 588, no. 85 (appendix).

10 CTIVD has already widely reviewed the exercise of the hacking power in its review report no. 53 (published in April 2017) on the use of the hacking power by the AIVD and the MIVD, *Parliamentary Documents II* 2016/17, 29 924, no. 149 (appendix), available at www.ctivd.nl. The corresponding legal framework includes an extensive description of this investigatory power under the ISS Act 2002.

The CTIVD also investigated how the rights of the persons involved are protected in the further processing of data. In this respect, the CTIVD looked at how the recommendations adopted by the ministers from review report no. 55 have been followed up. This investigation also offers the chance to further elaborate on the criticism voiced about the relevance assessment of bulk data sets in the third progress report on the functioning of the ISS Act 2017. Lastly, the report assesses to what extent the services, in implementing the requirement of proper and careful processing of data and their duty of care, have safeguards in place to protect the rights of people or organizations whose data is processed in bulk data sets.

A detailed legal framework to this report has been included in Appendix II.

With this topic, the CTIVD aims to address the criticism and concerns in the social and political debate during the legislative procedure of the ISS Act 2017 about processing bulk data sets. At the time, the debate focused mainly on the investigatory power of investigation-related interception, in particular on the untargeted interception on the cable but, in light of the above, the relevance is clearly much broader.[11] This report by the CTIVD aims to contribute to the evaluation of the ISS Act 2017, in particular to the effect of certain new elements of the hacking power in practice and how bulk data obtained with the hacking power under the ISS Act 2017 is handled.

Investigative questions and investigation period

The CTIVD has conducted an in-depth investigation into bulk data sets collected using the hacking power ('bulk hacks') and their further processing by the AIVD and the MIVD.[12] The emphasis of this investigation is on the system used by the services. To this end, the CTIVD examined parts of all bulk hacks in the investigated period, which means that not all hack operations conducted or all bulk data sets available were included in the investigation. There were eleven operations approved by the TIB, in addition to four rejected operations. One operation was approved in the course of the investigation period and later, on extension, rejected in that same investigation period.

The investigation covers the period from 1 May 2018, the date on which the ISS Act 2017 entered into force, to 1 November 2019.

This investigation by the CTIVD answers the following investigative questions:

- *In the period investigated, did the AIVD and the MIVD lawfully use the hacking power when collecting bulk data sets ('bulk hacks')?*

- *In the period investigated, did the AIVD and the MIVD lawfully further process the bulk data sets obtained by the hacking power?*

The investigation method and scope of the investigation are described in more detail in Appendix 1 to this review report.

11 Here the CTIVD refers to the investigation about the processing of airline passenger data by the AIVD and the MIVD that was announced on 25 September 2019.
12 The investigation was announced on 11 September 2019.

2. Findings on policy, work instructions and practice of the AIVD and MIVD: exercising the hacking power

2.1 Introduction

This section centres on answering the following investigative question:

In the period investigated, did the AIVD and the MIVD lawfully use the hacking power when collecting bulk data sets?

The investigation focused on a number of elements of the hacking power that are new in the ISS Act 2017. The main question is answered based on the following subsidiary questions:

- Did the collection of the bulk data sets using the hacking power in the investigation period take place on the basis of an authorization request found to be lawful by the TIB? (Section 2.3)
- Have the technical risks that could occur when using the hacking power been described in the authorization requests in line with the real-life situation? (Section 2.4)
- Did the services comply with the clean-up obligation? (Section 2.5)
- Did the services keep records of the use of the hacking power? (Section 2.6)

2.2 Nature of the operations

When conducting this investigation, the CTIVD gained an overview of the practice of both services where it concerns operations that can be considered 'bulk hacks'. There are eleven operations approved by the TIB, in addition to four rejected operations. One operation was approved in the investigated period and later rejected on extension.

To better understand this report, it is important that the nature of these operations is described as accurately as possible. However, the sensitive nature of the operations imposes restrictions, making it impossible to list exact amounts, types of data and organizations. In general it can be said that bulk data sets concern large collections of data. In a previous report for example, the CTIVD classified a collection of the email addresses, passwords and names of more than a hundred million people as a bulk data set.[13] In its 2018/2019 annual report, the TIB calls a hack of a company to obtain the data of millions of people an example of a 'bulk hack'.[14] These examples illustrate the possible size of a bulk data set.

The investigation shows that bulk hacks appear in the practice of both services, but are not an everyday occurrence[15] In most cases, the operations conducted in the investigated period are aimed at collecting data abroad that can be relevant to several of the services' teams, for example to get a better picture of targets and their activities such as communication and movement. In addition, the services attach great importance to the bulk data sets obtained in these operations because of their significance for target discovery. That means that the data in these data sets can be used to recognize as yet unknown

13 See review report no. 55 (published February 2018) about the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties, *Parliamentary Documents II* 2016/17, 29 924, no. 155 (appendix), p. 3.
14 TIB 2018/2019 annual report, p. 22, www.tib-ivd.nl.
15 Based on an analysis of the requests for authorization and extension in the investigated period.

targets and thereby identify unknown threats. The data sets therefore contain data that is 'unique and essential' in the services' perspective and that contributes to answering their investigative questions.

Although the operations qualified as bulk hacks differ, they do also have similarities. In broad outlines the operations follow a similar process where it concerns the start phase, execution and further processing of the collected data. In all phases departments of the Joint Sigint Cyber Unit (hereinafter: JSCU) – a joint unit of the AIVD and MIVD – play a central role. For example the use of the hacking power has been assigned to the executive department CNE (Computer Network Exploitation) with its specialized operators. The requesting of authorization to use the investigative power laid down in Section 45 of the ISS Act 2017 has been assigned to another department of the JSCU, which acts as a gatekeeper and supervises the operations that are conducted for the various teams. Data from bulk data sets is generally of interest to more than one of the services' teams. In many cases and in consultation with CNE, this department drafts the authorization requests for 'bulk hacks', which are then approved by the relevant minister following the applicable internal procedure, after which the TIB reviews the authorization granted by the minister for lawfulness.

Nearly all the operations for which authorization was granted in the investigation period are long-term operations which were initiated under the ISS Act 2002 and continued under the ISS Act 2017. That means that within an operation, data could have been collected at various times,, which contributed to the formation, and therefore the updating, of a bulk data set. Some of these bulk data sets compiled over time can consist of millions of unique 'facts' such as technical characteristics. In the cases where a distinction can be made between content and metadata, the sets mainly consist of metadata.

The use of the hacking power in the operations carried out in the investigation period, concerned automated devices or systems of organizations not considered targets by the services but which do have data about people and/or organizations that can be considered possible targets. These organizations are therefore considered non-targets.

Lastly, the investigation period covers both separate operations by the AIVD and the MIVD and joint operations. In that respect, the AIVD and the MIVD are interconnected to a considerable degree in this investigation. In joint-team operations, one of the services generally takes care of the authorization request but the collected data is made available to both services. In those cases the lawfulness assessments pertain to both services but formally relate to the service considered the applicant of the authorization request.

2.3 Authorization requirements

Legal framework

To use the hacking power, the AIVD or the MIVD must request authorization from the relevant minister. This is the Minister of the Interior and Kingdom Relations where it concerns the AIVD and the Minister of Defence where it concerns the MIVD. Once the minister has granted authorization, the TIB conducts its lawfulness assessment. The TIB assesses the substantiation for the requirements of necessity, proportionality, subsidiarity and 'as targeted as possible'. The hacking power may only be exercised after approval by the TIB. In the ISS Act 2017 this independent review by the TIB forms an important new safeguard for the legal protection (see Appendix II on the legal framework, Section 4.1).

Assessment of the practice

The CTIVD looked at the requests for authorization and extension of hack operations leading to the collection of a bulk data set in the period investigated. The CTIVD examined whether bulk data was only collected using the hacking power if there was a valid authorization by the TIB to do so.

The CTIVD established that in three of the sixteen operations investigated, data was collected after an authorization request had been rejected by the TIB. It concerns operations requested by the AIVD for which the relevant minister granted authorization at the end of April 2018 under the ISS Act 2002. At that time a review by the TIB was not yet a legal requirement. In May 2018 the AIVD renewed its authorization request for these operations under the ISS Act 2017 which entered into force on 1 May 2018. A new request was made for this. These requests were subsequently rejected by the TIB at the end of May 2018.

It appears from technical investigation by the CTIVD's IT Unit that data was nevertheless collected in these operations until the end of July 2018. This is due to the fact that the term of the ISS Act 2002 request ran from April to the end of July (three months) 2018 and that the operation was not put on hold after the interim rejection by the TIB.

The CTIVD finds the collection of data after the rejection by the TIB to be unlawful because of a failure to comply with all authorization requirements for the use of the hacking power under the ISS Act 2017.

Further investigation by the CTIVD and the AIVD shows that soon after the data had been collected, the AIVD itself realized that collecting that data after rejection by the TIB was unlawful. The AIVD had at an earlier stage already withdrawn the authorizations to use the data from some of these operations. Once it established that this collection was unlawful, the AIVD went on to destroy the data in all three operations. There are no indications that the unlawfully collected data was used in intelligence products. In the CTIVD's view the AIVD thus exercised sufficient care in dealing with this unlawful collection. The CTIVD specifies the nature and course of these operations in more detail in the classified appendix.

In one of the operations requested by the AIVD, data was collected at the end of July 2018, close to the expiry period of the authorization to use the hacking power granted under the ISS Act 2002 by the Minister of the Interior and Kingdom Relations on 18 April. In the meantime no renewed request was put to the TIB. In the opinion of the CTIVD, the AIVD should have submitted an authorization request to the TIB as soon as possible after the introduction of the ISS Act 2017, as it did in the three operations mentioned above. Furthermore, the CTIVD feels that the sensitive nature of the operation in question was even more reason to submit the request to the TIB as soon as possible. This view is in line with the undertaking of the Minister of the Interior and Kingdom Relations in this respect that as soon as possible after the introduction of the ISS Act 2017, authorization requests should be submitted to the TIB in phases, starting with the sensitive operations.[16] The AIVD eventually requested authorization to use the hacking power as late as August 2018, without stating in its request that data had already been collected in July. This request was subsequently rejected by the TIB.

In this operation the AIVD was able, with the help of login information, to log into a automated device or system and collect a bulk data set there. The CTIVD considers this action to be the exercise of the hacking power, as the service actually entered a automated device or system with the help of login details to copy data stored there. The AIVD explained to the CTIVD that it did not consider this action to be the use of the hacking power. The service therefore invokes a different legal ground for the collection of this data. Although the service had asked for authorization to use the hacking power under

16 Letter from the Minister of the Interior and Kingdom Relations to the House of Representatives regarding undertakings and motions ISS Act 2017 1 May 2018, 25 April 2018.

the ISS Act 2002, it was not the AIVD's intention, according to their explanation, to extend the obtained authorization after 1 May 2018. The fact that a renewed request for the use of the hacking power was eventually made for authorization in August, was linked to changed circumstances, according to the AIVD.

The CTIVD finds the collection of data on the basis of these circumstances to be *unlawful*.

This finding leaves the CTIVD no room to come to any recommendation other than to immediately destroy the unlawfully collected data.[17] Naturally on the understanding that further investigation into the use of the data must remain possible as explained below. Use of the data in the intelligence process must be halted immediately. The CTIVD specifies the nature and course of this operation in more detail in the classified appendix.

As regards the recommendation to destroy the data, the CTIVD states the following: The CTIVD has not further investigated how the unlawfully obtained data was shared by the services, for example in intelligence products or by providing it to partner services. Without this additional information therefore, it is not possible to make a recommendation about how to undo all further sharing of the unlawfully obtained data. The CTIVD has asked both services to identify the sharing of the unlawfully obtained data as soon as possible. The CTIVD will include this information in an independent follow-up investigation into the consequences that sharing the unlawfully obtained data has had. This investigation will address both the infringement of fundamental rights connected with the further processing of this data and the significance of the processing in the context of national security.

Conclusion

The CTIVD established that in three operations requested by the AIVD, data was collected after an authorization request had been rejected by the TIB. This is unlawful. This is a disregard for an important legal safeguard for the lawful use of the hacking power. The AIVD destroyed the data in question after establishing that it had been collected unlawfully.

In one operation requested by the AIVD, data was collected three months after the ISS Act 2017 entered into force, based on an earlier authorization granted by the minister under the ISS Act 2002. Once the ISS Act 2017 entered into force, a request for authorization was not submitted to the TIB for assessment on time. As there was reason to do so, collecting this data was *unlawful*. As a result, the CTIVD recommends that the data must be destroyed immediately, on the understanding that further investigation into the use of the data should remain possible.

17 Moreover, the data set in question is part of the data sets which Section 3.2 refers to concerning a lawfulness decision issued regarding the relevance assessment.

2.4 Technical risks

Legal framework

Section 45(4) of the ISS Act 2017 stipulates, among other things, that an authorization request for exploring or entering an automated device or system of a target, non-target or third party must contain a description of the technical risks associated with the use of the relevant investigatory power (under a). This is in addition to the general requirements that Section 29(2) of the ISS Act 2017 sets for the use of a special investigatory power. It is up to the TIB to assess if this description is adequate and how much weight to give it in the lawfulness assessment.

It can be understood from Section 31 of the ISS Act 2017, which lays down the obligation to keep records of the use of an investigatory power, that the service must keep a record of the technical risks that are associated with the use of that investigatory power, in any case where they deviate from the description in the authorization request.

Weighing the technical risks is important because hacking operations may have widespread societal consequences, for example for the users of an automated device or system.

Legislative history distinguishes various risks. Firstly, the risks linked to the use of known or unknown vulnerabilities in software to gain access to an automated device or system, both for users of the automated device or system on which that software operates and for other users of that software. In addition, third parties could take advantage of these vulnerabilities. Secondly, there are risks in the services introducing technical aids to gain access to a automated device or system. Weighing these risks is also in the services' own interest in order to be able to enter unnoticed.

Assessment of the practice

The CTIVD established that in the requests and extensions of operations in the investigation period the risks were generally described as low or non-existent. From interviews that the CTIVD has held with CNE employees it emerged that it is hard to come to a conclusive risk assessment at the beginning of an operation, before authorization for the use of the hacking power has been granted, because at that time, depending on the preliminary investigation, there is scant information available about the technical environment of the person or organization the use of the hacking power is aimed at. This affects the risk description in the first authorization request of an operation.

As regards the authorization requests to extend operations in the investigation period, the CTIVD established that the description of the technical risks is a snapshot at the time of drafting. That means that the description relates to the technical risks that exist at the time the extension request was drafted and not to the risks that did or did not manifest themselves in the preceding months.

The description in the requests in the period investigated therefore has a limited safeguard function. The CTIVD has taken note of the fact that the TIB had already entered into discussions about the substance of the risk description with the services both during and after the investigation period.

The CTIVD also conducted an investigation into the internal risk assessment within CNE. The picture that CTIVD gets of the implementation practice of hacking operations is that CNE attaches great importance to *operational security*. The associated risks relate mainly to the risk of damage from an operation or a certain action, for example that an operator will be identified by the person or organization the hack is aimed at. The CTIVD understands that these risks have a high degree of interdependence with the risks for the user(s) of the automated device or system the hack is aimed at. Disrupting processes and/

or activities by making changes in the automated device or system inherently runs the risk of being identified. The procedure that the CNE operators use is therefore inherently aimed at minimizing risks.

In an explanation, CNE staff indicated that measures are being taken to assess the risks beforehand as best they could and to avert them during an operation. However, the CTIVD has established that these measures are not mentioned in requests, policy or work instructions.

Risks can occur at various moments in the course of an operation. Operators bear responsibility themselves for the decision to take or not to take a certain risk. It emerged from the interviews the CTIVD held that they are also supposed to report the risk assessments in the course of an operation in the operation log. When in doubt, *operators* can then consult a coordinator who is responsible for the safety of operations, and who is involved in the risk assessment in the context of the four-eyes principle. The CTIVD has not found any written evidence of this procedure in policy or work instructions. It recommends describing this procedure, which sufficiently safeguards a risk assessment, within CNE and including it in policy and/or work instructions.

Random checks

The IT Unit of the CTIVD found in a random check that it is extremely time-consuming to assess the accuracy of the description of the technical risks of using the hacking power, based on the automated logs. For that reason, this procedure is not suitable for effective external review retrospectively. In the context of this investigation therefore, a random check is unsuitable as a means to assess whether the risk description in the requests and extensions was accurate.

Therefore it is all the more important, from the perspective of internal control and external review, to keep a record in the operation log of the internal assessments on whether or not to take certain risks in the course of an operation. In the operations conducted in the period investigated, no assessments relating to risks were found in the logs. It is unlikely that not a single risk occurred in any of the operations conducted.. The CTIVD recommends recording the assessments regarding significant risks in the log of an operation, given the fact that automated logging itself is unsuitable to effectively reconstruct the risks of an operation after the fact.

Conclusion

The description of the technical risks in the requests in the period investigated has a limited safeguard function. The CTIVD has taken note of the fact that the TIB had already entered into discussions about the substance of the risk description with the services both during and after the investigation period.

The internal procedure that CNE follows for taking and assessing risks sufficiently safeguards a risk assessment with due observance of the following recommendations. The CTIVD recommends laying down this procedure, such as the four-eyes principle, in policy and work instructions. The investigation found no assessments of risks in the logs of the operations investigated. The CTIVD recommends recording the assessments regarding significant risks in the log of an operation, given the fact that automated logging itself is unsuitable to effectively reconstruct the risks of an operation after the fact. This hampers effective external review in retrospect.

2.5 Clean-up obligation: Removal of technical aids

Legal framework
Based on Section 45(7) of the ISS Act 2017, the principle applies that a technical aid used to enter an automated device or system, for example malicious software (malware), must be removed if possible after the hacking power exercised has ended. If an automated device was entered through that of a third-party, this obligation not only applies in regard to that third party but also in regard to the target.

The aim is to prevent abuse of the technical aids used by the service that could lead to large-scale damage to the owner and/or users of the automated device or system.

A best-efforts obligation was selected in this case because in certain cases the removal of malware could disproportionally harm the third party or the compelling operational interests of the services. In the event that the technical aid cannot be removed, this must be recorded.

Assessment of policy and work instructions

The policy of both services states that there is a best-efforts obligation to remove the technical aids when ending a hacking operation, unless this would cause disproportionate disadvantage to the person or organization the hack is aimed at or the services' compelling operational interests. If the technical aids are not removed, this should be recorded in a report. Policy places no further requirements to this report. The AIVD does have a document in which some minimum requirements for the report have been defined, for example, reasons must be given for the decision not to remove the technical aids, in addition to describing which technical risks it will cause to users and third parties to maintain these technical aids. The CTIVD supports these principles and recommends that both services set them down in their policy and/or work instructions. The information that CNE records in its manual log when a clean-up action was successful should also be listed, such as a description of the technical aids removed and the time of removal. Lastly, policy should include when the hacking power is deemed to have ended and by what time a clean-up action should have taken place. The principle should be that a clean-up action is carried out as soon as possible.

A brief supplement to the policy has been included in an internal CNE page. It specifies that two weeks before the end of the authorization period, automatic notifications will be sent to the *operator* responsible for the operation, and to the processor of the intelligence team in question. These notifications are then sent until the technical aid has been cleaned up or until the use of the hacking power has been extended. The CTIVD has established that this system is applied in practice.

Assessment of the practice

The CTIVD's IT Unit investigated whether, in the investigation period, the technical aids used were removed from completed bulk hacks. The unit also investigated if and how a report was drafted in those cases where the aids had not been removed.

The investigation shows that in all operations identified by the CTIVD, the clean-up obligation was fulfilled and that in all other cases, a report was drawn up. In one of the investigated operations, the report was very brief and it was unclear when the clean-up action had taken place and which technical aids were involved. That is a failing.

The investigation also shows that in a number of cases the period between the last approved authorization request for an extension of the hacking power in an ongoing operation and the first clean-up attempt was very long (about 12 months). These cases concerned operations in which repeated, unsuccessful, attempts had been made to obtain authorization for an extension.

Where these operations are concerned, the CTIVD states that the best-efforts obligation to clean up arises the moment the use of the hacking power ends. When authorization is not obtained, the legal basis for the further use of the hacking power comes to an end, at which point the use must stop and the best-efforts obligation to clean up should begin. By opting for a best-efforts obligation, the law offers scope to refrain from removing the technical aids, because of compelling operational interests or because removal will cause disproportionate disadvantage to the person or organization the hack is aimed at. This substantiation must, in the CTIVD's view, be included in the report and therefore in the log of the relevant operation. This assessment should be made at each rejection of authorization, as a rejection is in principle a reason to remove the used aids. In the operations in question during the period investigated, the CTIVD did not find any such assessments in the log, with the exception of the ultimate clean-up action. As the technical aids were eventually removed, the legal obligation as such was observed.

Conclusion

In the investigated period, the clean-up obligation was carried out lawfully as the CTIVD did not find any operations in which technical aids had not been removed or in which the report was missing in those cases where the technical aids had not been removed.

However it was not always clear from the report which technical aids had been removed at what time and why removal had or had not been possible. That is a failing. The CTIVD recommends stipulating in the work instructions what minimum requirements the report must fulfil, both in cases where the technical aids are cleaned up and in cases where they are not.

In a number of operations the period between the last approved authorization request for an extension of the hacking power in an ongoing operation and the first clean-up attempt was long. As the technical aids were eventually removed, the legal obligation as such was observed.

In operations where access is maintained because of an intended extension of the operation, a report must be drawn up each time the authorization is rejected. The report must show why the technical aids were not cleaned up and what the corresponding risks are.

2.6 Reporting

Legal framework

Section 31 of the ISS Act 2017 stipulates that a record must be kept of the use of an investigatory power, also referred to as reporting. This includes recording the decisions made when exercising the hacking power. Records that must be kept on the investigatory power to hack include newly identified or substitute automated devices or systems of a target, non-target or third party. Records must also be kept on the assessment of the technical risks linked to the exercise of the investigatory power in the case concerned. In its review report no. 53 of April 2017, the CTIVD recommended that the services start logging (i.e. start the continuous automated and comprehensive recording of data) the hacking power exercised and the related technical actions taken.[18] The ministers adopted this recommendation at the time.

Keeping records of the use of an investigatory power serves internal control purposes and in addition enables effective external review by the CTIVD. This makes it possible to reconstruct assessments and actions in retrospect.

Assessment of policy and work instructions

The general policy of both services concerning this obligation to keep records (reporting) on an investigatory power exercised is limited to a general description of this legal obligation, namely that recording should take place. There is both policy and a description of the applicable procedures for individual special and general investigatory powers.

However, none of the documents relating to Section 45 of the ISS Act 2017 include any specific details of record-keeping or the manner of keeping records of the exercise of this investigatory power. The same applies to a further detailing of the recommendations from CTIVD report no 53 with respect to keeping records by automated logging. As regards that last point, the CNE department does have a more detailed elaboration on an internal web page intended for its own staff. In practice, it appears that both automated and manual records are kept.

The CTIVD recommends setting out in policy and/or work instructions which minimal automated logging the operators must set up and which events they should record manually in the log of an operation.

Assessment of the practice

In practice, it appears that both automated and manual records are kept. automated logging results in a log file in which the actions of CNE operators are recorded by automated means for each computer system. This concerns the operators' own systems used to conduct operations. Because there are only minimum requirements for the automated logging, differences in logging can occur for each operator.

In addition to automated logs, CNE operators also keep a manual log of each operation, in which they record significant events and activities over the course of an operation, such as obtaining or losing access, the manual collection of data and the registration of incidents. Examples of these events are described in the aforementioned internal CNE page.

The CTIVD established for all bulk hack operations conducted in the investigation period that there was both automated logging and a manual log and that there was a conclusive explanation in other cases.

18 CTIVD review report no. 53 (published in April 2017) on the use of the hacking power by the AIVD and the MIVD, *Parliamentary Documents II* 2016/17, 29 924, no. 149 (appendix), available at www.ctivd.nl.

No real discrepancies were found between automated logging and the manual log, which means that important events from the automated logging could be found in the manual log and that the events included in the manual log could be linked to the automated logging.

However, the manual logs of operations were not uniform, with operators using different working methods where it concerns the level of detail. The CTIVD was able to establish that the general quality of the manual logs has increased significantly over time. In addition, an analysis of automated logging brought to light differences in this type of logging. This complicated the search of log files. This finding underlines the importance of keeping a manual log for each operation, because it provides a relatively fast overview of the course of an operation.

Despite the differences, the quality of the automated logging where it concerns completeness, availability and traceability, is such that in combination with the manual log it is suitable for internal control and effective external review.

Conclusion

Both services, specifically the joint executive CNE department, *lawfully* implement the recommendations from CTIVD report no. 53 and the obligation to keep records by automated logging and a manual log.

For automated logging, the CTIVD recommends working towards a standardized and uniform set-up in the short term including the minimum requirements.

The CTIVD further recommends drafting work instructions to keep manual operation logs in a uniform manner, which should at least include a description of which activities and decisions are to be recorded and with what level of detail.

3. Findings on policy, work instructions and practice of the AIVD and MIVD: safeguards for the further processing of bulk data sets

3.1 Introduction

This section centres on answering the following investigative question:

- *In the period investigated, did the AIVD and the MIVD lawfully further process the bulk data sets obtained by the hacking power?*

The main question can be specified based on the following subsidiary questions:

- How do the AIVD and the MIVD deal with the legal requirements relating to the relevance assessment under Section 27 of the ISS Act 2017? (Section 3.2)
- To what extent do the AIVD and the MIVD fulfil the procedural safeguards for the further processing of bulk data sets collected via a hack? (Section 3.3)

Bulk data sets are large collections of data, the majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. As stated above in this report, bulk data sets are of immense value to the performance of the services' tasks, to recognizing and identifying known and in particular unknown targets and threats. The downside is that collecting and further processing personal data in a bulk data set constitutes a severe privacy infringement. It is therefore important that the fundamental rights of those involved who are not under investigation by the services are sufficiently protected.

When a bulk data set is copied, this necessarily entails that the data of persons or organizations who are not, nor ever will be, the subject of investigation by the services, is also copied in the interest of gathering intelligence or because of operational risks. This untargeted way of obtaining data must be corrected when the bulk data sets are processed further. Therefore, collecting and processing are interrelated where it comes to how targeted the use of the hacking power is.

This section looks at the services' system when further processing bulk data sets that have been collected using the hacking power.

The legal safeguard that applies to further processing is a limited retention period within which the data sets must be assessed for relevance. The first part of this section illustrates the problems that arise with this requirement, followed by a description of the services' policy and practice.

The second section looks at the additional safeguards not explicitly laid down in the law, which the services subject themselves to when processing the collected bulk data sets further. This is an implementation of the general requirement of proper and careful data processing and the duty of care for the lawfulness and quality of data processing (Sections 18 and 24 of the ISS Act 2017). The CTIVD examined these restrictions in greater detail and assessed policy, work instructions and daily practice.

3.2 Data reduction

Legal framework

The further processing of bulk data sets collected using the hacking power is regulated mainly by Section 27 of the ISS Act 2017, as the hacking power under Section 45 sets no further requirements to this. Section 27 stipulates that data obtained by a special investigatory power, such as the hacking power, must as soon as possible be assessed for relevance to the investigation for which it was collected.

If it has been established that data is not relevant to that investigation or any other ongoing investigation by the services, that data must be destroyed immediately. There is a maximum term of one year (with a six-month extension if necessary) in which the relevance assessment must take place. Data that is assessed as non-relevant at the end of that term, must be destroyed immediately.

Data declared relevant falls under the data reduction regime based on significance. This follows from Section 20 of the ISS Act 2017. That section stipulates that data which has no, or no longer has any, significance in light of the purpose it is processed for, must be removed.

Section 27 is a major legal safeguard for further processing of data from special investigatory powers. The provision prevents non-relevant data from remaining available to both services for a long period of time.

As the ISS Act 2017 does not distinguish between bulk data sets and other data, Section 27 of the ISS Act 2017 applies in full to these data sets because they originate from a special investigatory power.

Bulk data sets are distinguished from other collections of data, because they consist mainly of data relating to organizations and/or people who are not the subject of investigation by the services, nor ever will be. However, therein lies the value of these data collections to identify known and particularly unknown targets and threats.

Based on evolving knowledge and understanding and using the data from bulk data sets, new connections can constantly be made in the context of ongoing investigations. This applies to various teams within the services, who each in their own way value the data from bulk data sets based on their own investigative questions and who repeatedly search the data sets throughout the retention period That means that it is difficult, if not impossible, to assess the relevance of the data in a bulk data set beforehand. Relevance can differ from investigation to investigation and from day to day. This is an issue for both the services, which the CTIVD also recognizes.

Assessment of policy and work instructions

Both the AIVD and the MIVD have a policy to reduce the data from bulk data sets obtained through special investigatory powers, with the exception of investigation-related interception. This policy describes how the relevance assessment of the bulk data sets is made. That policy contains three safeguards that are used. In summary, this includes (1) a higher level of authorization and the additional requirement to give reasons when determining relevance, (2) continuing to apply safeguards after relevance has been determined (see Sections 3.3 and 3) and a periodic evaluation of the data once it has been declared relevant (and thus falls under the data reduction regime based on significance). An important detail is that this policy states that the relevance assessment of a bulk data set not only pertains to the data collected but also to any future data added to the bulk data sets through an ongoing operation. The implementation of this policy in practice has resulted in unlawful conduct,

as explained in more detail below. For that reason the CTIVD has not made a separate lawfulness assessment of the policy.

Assessment of the practice

In its third progress report on the functioning of the ISS Act 2017 (Dec. 2019) the CTIVD had already noted that the retention period under Section 27 of the ISS Act 2017 and the requirement 'to make a relevance assessment as soon as possible' is not feasible in practice for bulk data sets. The simple fact is that they contain too much data. In addition, because of their specific characteristics, bulk data sets are of value to the services' investigations for a significantly longer period.[19] At the end of the maximum retention period of 18 months, the law requires that the data not assessed on relevance be destroyed.. In practice, the services do not always observe that requirement when it comes to bulk data sets collected using special investigatory powers.[20] Although in a few cases bulk data sets were destroyed in their entirety, in other cases only parts of the data sets – if that – were destroyed.. This included data from countries not contributing to ongoing investigations by the services. As data should be collected in an as targeted way as possible, the CTIVD feels that a reduction should have been made directly after collection.[21] In addition it must be noted that a bulk data set is still considered a bulk data set, even after part of it has been destroyed and as such it mainly consists of the data of people that should not be the focus of the services' attention.

In other cases, the bulk data sets as a whole were declared relevant without destroying parts of them. As a result of this, the services are able to retain the data stored in these sets without a final destruction term and destruction after 18 months is therefore no longer at issue, because after being designated relevant, the data falls under the data reduction regime based on significance. This is based on Section 20 of the ISS Act 2017. That section stipulates that data which has no, or no longer has any, significance in light of the purpose it is processed for, must be removed. However, the bulk data sets should never have fallen under that data reduction regime. In its classified appendix, the CTIVD takes a further look at this practice by discussing the bulk data sets declared relevant in this way.

The CTIVD considers this method of relevance assessment to be an artifice aimed at extending the retention period of the data sets in question. It is, after all, *unlawful* to declare data sets relevant that for the most part contain evidently non-relevant data.

The ISS Act 2017 does not offer scope for this. The CTIVD had already included this decision in its third progress report.[22] This assessment applies equally to automatically decl aring any future data in a bulk data set relevant. As the CTIVD stated in its third progress report, it does not follow from this decision that the bulk data sets in question should be destroyed.

This is because the CTIVD understands that bulk data sets have significant operational value. In its decision at the time, the CTIVD intended to send a clear message to the services and the ministers that a solution must be sought for the situation. In the absence of such a solution, the CTIVD now sees no other option than to recommend the immediate destruction of the bulk data sets in question. This ensues from the Act.

---

19 VGR III, no. 66 (published 3 December 2019), p. 8, *Parliamentary Documents II* 2019/00, 34 588, no. 85 (appendix).

20 As noted in the third progress report (p. 10), the AIVD decided in April 2019 to extend the retention period of bulk data sets collected under both the ISS Act 2017 and the ISS Act 2002 with the legal term of six months. That made 1 November 2019 the deadline on which the data sets had to have been assessed for relevance or have been destroyed. As the MIVD uses the data as well, the service endorsed this decision. In the run up to 1 November 2019, the AIVD analyzed the value of the data sets based on quality and the nature of the data and the use of the data in the intelligence process. That analysis contributed to the decision whether or not to destroy a data set partially or completely.

21 This requirement of as targeted as possible is laid down in a policy rule (*Parliamentary Documents II* 2017/18, 34 588, no 76) (appendix) pending a legislative amendment (*Parliamentary Documents II* 2018/19, 35 242, no 2).

22 VGR III, no. 66 (published 3 December 2019), p. 8, Parliamentary Documents II 2019/00, 34 588, no. 85 (appendix).

Conclusion

The ISS Act 2017 offers no scope for declaring manifestly non-relevant data relevant. This methodology used by the services in the investigated period was already assessed as *unlawful* in the CTIVD's third progress report.

The CTIVD recommends destroying the bulk data sets in question immediately.

3.3 Safeguards for the further processing of bulk data sets

Legal framework

Section 18 of the ISS Act 2017 stipulates that data should only be processed for a certain purpose and only in as far as necessary for the AIVD and the MIVD to properly perform their tasks. In addition data processing by the services must be done properly and with due care.

As regards the processing of bulk data sets, that last requirement means that the following principles have been taken into account: a distinction between data relating to targets and data relating to organizations and/or people that are not nor ever will be the subject of investigation by the services, including in any case the measure that the data of this last category is not immediately accessible to staff (exceptions notwithstanding).

In addition, safeguards must be set up that regulate the access by staff to the data (authorization process). The automated recording of data search requests arises from the duty of care for data processing under Sections 18 and 24 of the ISS Act 2017.

The CTIVD also focuses on the follow-up of relevant recommendations in report no. 55 on bulk data sets on the internet, in as far as adopted by the ministers.

Assessment of policy and work instructions

The investigation shows that neither service has an overall policy on further processing the bulk data sets obtained using the hacking power. In the policy documents found there is only scant reference to bulk data sets. Following CTIVD report no. 55, both services have admittedly published their policy on their website but that only lists general principles and does not offer an opinion on whether this applies to all bulk data sets or only the data sets made available on the internet by third parties.[23] They have said that new policy on handling bulk data sets is in the making, although the CTIVD has not yet read this.

Despite the lack of policy, there is an established practice. The CTIVD established that the authorization requests for operations that qualify as bulk hacks do refer to the applicable safeguards. The text of the requests refer to CTIVD's report no. 55 in which the CTIVD assessed the 'outer box/inner box structure' regarding the processing of bulk data sets with personal data offered on the internet by third parties as lawful.[24] The services have stated that this structure is also applicable as a safeguard to bulk data sets obtained using the hacking power, which means that an authorization procedure must be followed to transfer data from the 'outer box' to the 'inner box'. Including the safeguards in the authorization requests does not, in the view of the CTIVD, mean that this has been recorded in policy.

23 The 'AIVD and MIVD policy on the acquisition and processing of bulk data sets' was published on the websites aivd.nl and defensie.nl on 1 May 2018.

24 Review report of the CTIVD no. 55 (published February 2018) about the acquisition by the AIVD and the MIVD of bulk data sets offered on the internet by third parties, p. 21, accessible on ctivd.nl.

The CTIVD recommends both services to substantiate in policy how bulk data sets are handled, irrespective of the authorization by which they were obtained, thus including data sets obtained by the use of the hacking power. The services should come to a central policy that unambiguously sets out which safeguards apply, where responsibility for compliance has been assigned and how these safeguards manifest themselves in practice.

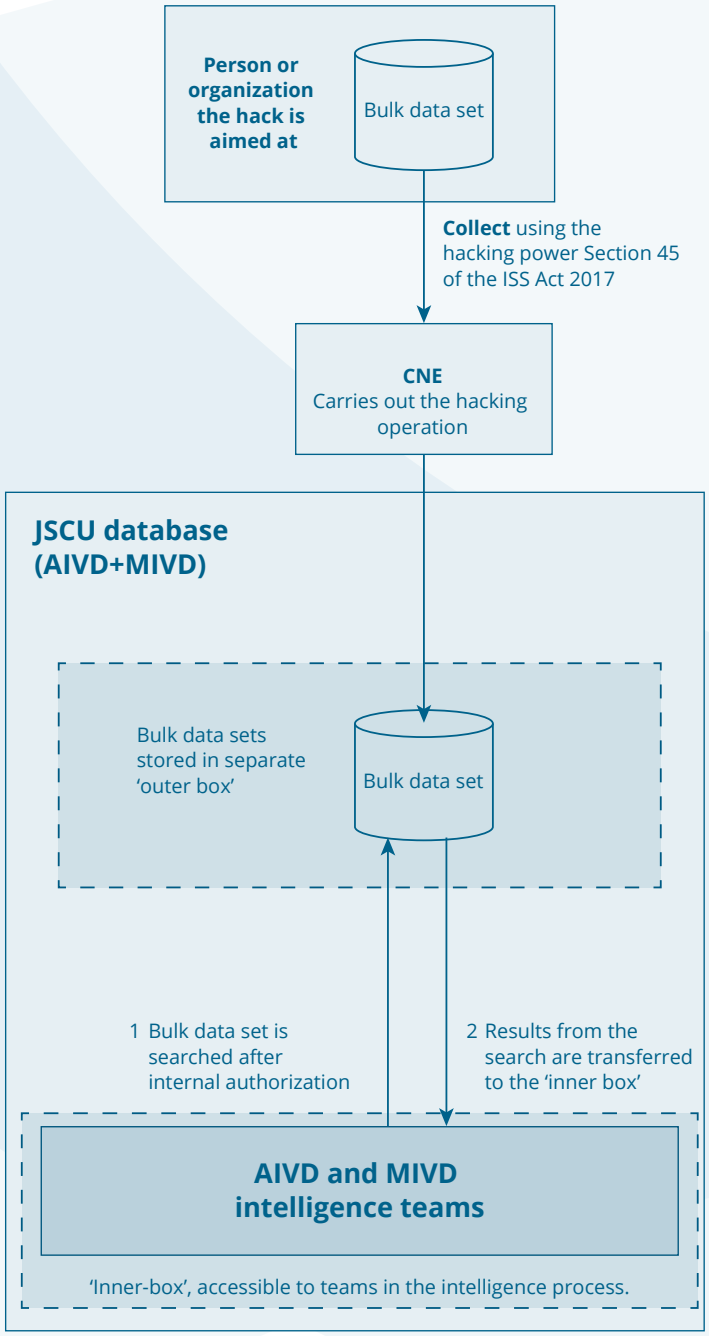
Assessment of the practice

In practice, the AIVD and the MIVD use certain safeguards. This is referred to as the outer box/inner box procedure. The procedure means that the obtained bulk data sets are not immediately accessible to the intelligence process (and thus to the different intelligence teams) but that after collection they are first placed in an outer box.[25] This is based on a division of job roles, and therefore the data is only accessible to authorized staff members. This is ensured by an authorization model. A second aspect of the outer box/inner box procedure is that the data may only be transferred from the outer box to the inner box after authorization, at which it becomes available to the wider intelligence process. The purpose of the procedure is to separate data in the bulk data sets. This is ensured by an authorization procedure.

In the subsequent part of this section, we will look at the authorization model used (division of positions) followed by the authorization procedure. The CTIVD will discuss the system of the outer box/inner box procedure as set out by both services in the Internal Check procedure. Alternative applications of the procedure are not included in the investigation, except those discussed at the end of this section.

25 The outer box is not a separate IT environment but an authorization regime on JSCU's central database. This barrier is enforced by using an authorization policy based on which access to data sources is possible.

Figure 1 diagram of the collection and processing of bulk data sets



Description of the division of job roles

The outer box in which the bulk data sets are stored is accessible to a limited group of service staff. Both services have set out in policy which categories of job roles have access.

In addition to JSCU staff who are responsible for the technical management of data, data-analysts for example may be granted access to the outer box. These data-analysts may also be part of an intelligence team. They are permitted to search the outer box without additional authorization, for example to formulate a query for the intelligence teams. Although the data-analysts' activities in the outer box are recorded by automated means, this generally serves internal-security purposes.

Other staff members within the intelligence teams of both services do not have access to the outer box. Processors are able to see in various applications that a certain search query yields other hits (or

results) but they are unable to see what these results are. To do so they need to follow the Internal Check procedure (see below). This is also referred to as the *hit/no-hit system.*

Assessment of the division of job roles

Data-analysts are authorized for the outer box after having received instructions within the JSCU. Although in practice a periodic check is made of these authorizations, there is no standard procedure with clear responsibilities. The CTIVD recommends setting up such a procedure and laying it down in policy.

The CTIVD considers that the applied authorization model sufficiently ensures that data that relates to organizations and/or persons who are not the subject of an investigation by the services is kept separate, and as such the requirements ensuing from Section 18 of the ISS Act 2017 have been met. This mainly pertains to keeping the data separate from the intelligence process. Concerning the role of data-analysts who are part of a team and who have access to the outer box, the CTIVD stresses that effective distance, including physical distance, is part of the safeguard function of the system of division of job roles and tasks.

Based on Sections 18 and 24 of the ISS Act 2017, automated recording of search requests by data-analysts in the outer box must also serve the purpose of internal and external control.

Description of Internal Check

Both services use an internal procedure to consult data from bulk data sets obtained via a hack. This procedure allows data to be transferred from the outer box to the inner box following a written request for authorization. This is referred to as Internal Check. The CTIVD's investigation underlines this procedure as implementation of the outer box/inner box procedure because it is frequently used and the most standardized. The Internal Check is a form of automated data analysis within the meaning of Section 60 of the ISS Act 2017. The cases in which this specific procedure did not apply are discussed at the end of this section.

Both the AIVD and the MIVD have a description of the Internal Check. The description serves as an instruction for staff. The AIVD procedure facilitates two types of search requests on data in the bulk data sets in the outer box, i.e. a 'limited' search request and a 'broader' search request. The MIVD does not make that distinction. The differences are depicted in the diagram below.

AIVD	**Authorization level**
Check: 'Limited' search request	Head of team
Check: 'Broad' search request	Head of unit
MIVD	**Authorization level**
Internal Check	Director of the MIVD

Thus a limited search request requires a lower authorization level than a broad search request. This is linked to the fact that the limited search request is made based on certain characteristics, for example a number or other technical characteristic. A broad search request differs because it is possible to search the available data sets on the basis of profiles, which enables more complex search requests.

The intelligence teams must substantiate in writing for each authorization request for an Internal Check why the search request is necessary, proportional and subsidiary. In addition, the MIVD must also substantiate why it is as targeted as possible.

Assessment of Internal Check

The investigation shows that when the Internal Check has been completed, the results of that search become accessible not only to the team that requested the procedure but also to all other staff who are authorized for certain search applications. At that point, the data is in the inner-box. It makes no difference if the data has been declared relevant or not by the staff member who made the original request. That means that once data is in the inner-box it is available to other intelligence teams who do not need to substantiate the use again. This set-up is considered by the CTIVD to correspond with the legal principle that it must be possible to conduct a relevance assessment on data intended for different investigations.

The recommendation in report no. 55 published in February 2018 – that data should be returned to the outer box by automated means after a period of time (three months) and which was adopted by the ministers – has still not been implemented technically, despite the promise at an earlier stage that implementation was sought. This is *unlawful*.

No central overview is kept of requests for an Internal Check including the corresponding substantiation. The substantiated requests are recorded separately by the teams drafting them. A centralized record is kept of the technical execution of an approved check, including the characteristics underlying the check. However this record does not contain the corresponding substantiation of the original authorization request. The JSCU is not involved in the process of granting authorization, but only in the technical execution of an already approved request.

The CTIVD established that in the course of the investigation period the services have taken steps to provide insight into the search requests of bulk data sets by means of reporting. As requests are now recorded, the requirements set under Sections 18 and 24 of the ISS Act 2017 have been met, in the opinion of the CTIVD. The CTIVD recommends making the further development of reports a top priority as they are a prerequisite for the lawful processing of bulk data sets. Reports are a suitable means of providing insight into the use of a bulk data set and as such they contribute, along with other information, to determining the value of a data set, which is important in the context of data reduction. Furthermore, reports can be helpful in the context of *compliance*, as they enable the services to promptly identify any deviations in the use of bulk data sets. In this way, reports serve to protect data relating to organizations and/or people who are not the subject of investigation by the services, nor ever will be.

Based on these findings, the CTIVD concludes that in principle the authorization procedure for conducting an Internal Check forms a certain safeguard to protect data relating to organizations and/or people who are not the subject of investigation by the services, nor ever will be.

This safeguard would gain more significance at the AIVD if the authorization level places greater distance between the requesting team and the person granting authorization, as is the case at the MIVD, which thus guarantees an objective assessment.

The CTIVD therefore recommends the AIVD to examine for check requests how it can achieve a higher authorization level with greater distance between the requesting party and the authorizing party. The CTIVD also recommends laying down the criterion ‘as targeted as possible’ as a requirement for the substantiation of check requests.

Alternative application of safeguards

The CTIVD established in two MIVD operations that although the outer box/inner box procedures had been declared applicable to collected data, this was not in fact enforced through the Internal Check for a variety of reasons. The data that the MIVD considered to be bulk data sets was managed in the investigation period by a different department of the JSCU, where a division of job roles was enforced by an application they developed themselves. Authorization requests to consult bulk data sets were assessed by the head of the team for which the data was originally collected. The authorizations for searching the data based on *hit/no-hit* also went via this head of team.

The CTIVD agrees with the MIVD's assessment that the data in these operations concerns bulk data sets to which the outer box/inner box procedure should be applied. The investigation shows that the MIVD took steps to apply this procedure, but that it uses a lower authorization level for checks than for the Internal Check. This is a failing, not unlawful conduct, given the observed safeguards and the specific nature of the operations in question.

Conclusion

In the investigation period there was no overall policy for dealing with bulk data sets obtained by the hacking power. The services are working on a new policy for handling bulk data sets, but the CTIVD has not yet been able to see this. The services should come to a central policy that unambiguously sets out which safeguards apply, where responsibility for compliance has been assigned and how these safeguards manifest themselves in practice.

An important safeguard used by the services in practice is the outer box/inner box procedure, which provides for keeping data in the bulk data set separate by means of a division of job roles and thereby ensures that data obtained from those data sets can only be consulted after obtaining internal authorization.

As regards that division of job roles, the CTIVD considers that this is a sufficient implementation of the requirements of proper and careful data processing set under Section 18 of the ISS Act 2017, except for the access that data-analysts who work in an intelligence team have. Where the periodic check of authorizations of data-analysts is concerned, the CTIVD recommends setting up a standard procedure and laying it down in policy.

The CTIVD considers that in principle the authorization procedure used, also referred to as the Internal Check, forms a sufficient safeguard to protect data relating to organizations and/or people who are not the subject of investigation by the services, nor ever will be. The authorization procedure is therefore a sufficient implementation of the requirements set under Section 18 of the ISS Act 2017 of proper and careful data processing. The CTIVD recommends that the AIVD also specifies in its authorization requests for the Internal Check the criterion as targeted as possible and that it examines how a higher authorization level for check requests can be achieved.

Failure to follow the recommendation in report no. 55 regarding the automated return of data to the outer box after a period of time is *unlawful*.

As the Internal Checks are now recorded and the services are working on a system of periodic reports based on this, the requirements set under Sections 18 and 24 of the ISS Act 2017 have been met, in the opinion of the CTIVD. Based on Sections 18 and 24 of the ISS Act 2017, the automated recording of search requests by data-analysts in the outer box must also serve the purpose of internal and external control. The CTIVD recommends making the further development of reports a top priority as they are a prerequisite for the lawful processing of bulk data sets.

The application of the outer box/inner box procedure to bulk data sets from two MIVD operations provides for a lower authorization level for checks than the Internal Check. This is a failing, given the observed safeguards and the specific nature of the operations in question.

4. Bulk data sets and the ISS Act 2017

Based on the findings in the preceding section, the CTIVD considers the following: In the absence of a legal regime for processing bulk data sets not obtained by investigation-related interception, the application of the Internal Check has an important role as a safeguard exceeding the statutory minimum. This procedure must prevent as far as possible the processing of data relating to organizations and/or people who are not the subject of investigation by the services. The Internal Check is a procedure that was already in place under the ISS Act 2002 and which was investigated and found to be lawful by the CTIVD in its report no. 55. However that does not mean that it offers adequate safeguards for processing bulk data in all cases.

The lack of a more specific legal regime for bulk data means that ultimately the CTIVD can only assess the lawfulness of the safeguards taken by the services against the general requirements that apply to all acts of data processing, such as Section 18 of the ISS Act 2017.

In this respect, it is important to note that the law includes a legal regulation for collecting and processing bulk data. This is the regulation for investigation-related interception which was introduced in the ISS Act 2017.[26] It makes provisions for special investigatory powers and related safeguards connected to intercepting, analyzing and further processing of data in the course of transmission.[27] Although collecting this data differs in nature and method from the collected data in bulk data sets in the current investigation, it is quite possible to compare the safeguards of this system with the safeguards belonging to the further processing of these bulk data sets. This comparison, for example with the safeguards for the investigative power to select or for automated data analysis, makes clear that the safeguards for the Internal Check fail – at least by comparison – to keep up. For example where it concerns the requirements for obtaining authorization.

The CTIVD views this discrepancy with concern. Although the general principles for data processing form a starting point for the lawfulness assessment in this report, they do not, in the CTIVD's opinion, offer a sound legal framework for processing bulk data sets and conducting a subsequent lawfulness assessment. It is therefore advisable to turn to a more inclusive legal regulation of bulk data sets that does sufficient justice to the protection of citizens' fundamental rights and the operational value of bulk data sets for the services. Based on the third progress report, the Minister of Defence, at the time also the Minister for the AIVD, announced that the bulk data sets would be a topic within the evaluation of the ISS Act 2017.[28]

26 Sections 48 to 50 of the ISS Act 2017.
27 See the explanation of this system in Appendix I to review report no. 64 (published in October 2019) on the use of the special investigatory power to select by the AIVD and the MIVD, Parliamentary Documents II 2019/20, 29 924, no. 192 (appendix), pp. 2 ff.
28 Letter from the Minister of Defence, also Minister for the AIVD, to the President of the House of Representatives of the States General concerning the submission of the adopted report III, 3 December 2019 and the letter from the Minister of Defence, also Minister for the AIVD, to the President of the House of Representatives of the States General concerning the evaluation of the Intelligence and Security Services Act 2017, 12 November 2019.

5. Conclusions

This investigation by the CTIVD answers the following investigative questions:

1. 1. *In the period investigated, did the AIVD and the MIVD lawfully use the hacking power when collecting bulk data sets ('bulk hacks')?*

2. *2. In the period investigated, did the AIVD and the MIVD lawfully process the bulk data sets obtained by the hacking power?*

The investigation covers the period from 1 May 2018, the date on which the ISS Act 2017 entered into force, to 1 November 2019. The CTIVD investigated all bulk hacks that occurred in the investigation period. There are eleven operations approved by the TIB, in addition to four rejected operations. One operation was approved in the course of the investigation period and later, on extension, rejected in that same investigation period.

Answer to investigative question 1

The investigation into the use of the hacking power when collecting bulk data sets focuses on a number of areas that are new in the ISS Act 2017 and that form important safeguards for legal protection. This concerns: review by the independent TIB, the description of technical risks, the exercise of the 'clean-up obligation' and reporting on the exercise of the investigatory power. In the following section the main conclusions are presented for each component. The conclusions stated here apply to both the AIVD and the MIVD unless stated otherwise.

Assessment by the TIB

An important new safeguard in the ISS Act 2017 is the independent lawfulness assessment by the TIB of the authorization by the minister in question to exercise the hacking power. For that reason the CTIVD investigated if the collection of the bulk data sets using the hacking power in the investigation period only took place based on authorization found to be lawful by the TIB.

In three operations requested by the AIVD data had been collected after the TIB had rejected the authorization request. This is *unlawful*. This is a disregard for an important legal safeguard for the lawful use of the hacking power. The AIVD destroyed the data in question after establishing that it had been collected unlawfully.

In one operation requested by the AIVD data was collected three months after the ISS Act 2017 entered into force, based on an earlier authorization granted by the minister under the ISS Act 2002. Once the ISS Act 2017 entered into force a request for authorization was not submitted to the TIB for assessment on time. As there was reason to do so, collecting this data was *unlawful*.

Technical risks

Weighing the technical risks is important because hacking operations may have widespread societal consequences, for example for the users of an automated device or system. The services must therefore include a description of the technical risks in an authorization request to enable the TIB to take this into consideration in its assessment of the lawfulness. Moreover it is important that the services record their internal assessments of technical risks.

The description of the technical risks in the requests in the period investigated has a limited safeguard function. The CTIVD has taken note of the fact that the TIB had already entered into discussions about the implementation of the risk description with both services both during and after the investigation period.

The internal procedure that CNE follows for taking and assessing risks sufficiently safeguards a risk assessment with due observance of the recommendations. The CTIVD found no decisions on taking or not taking risks in the logs of the operations investigated.

Clean-up obligation
New to the ISS Act 2017 is a clean-up obligation for technical aids, such as a backdoor or other malicious software, after the use of the investigatory power to enter has ended. It is a best-efforts obligation, of which a report must be drawn up if the clean-up did not take place because it would disproportionately disadvantage the person involved or the service. The aim is to prevent abuse of the technical aids used by the service that could lead to large-scale damage to the owner and/or users of the automated device or system.

The services' policy outlines the clean-up obligation but does not set requirements for the report to be drafted.

In the investigated period, the clean-up obligation was carried out *lawfully* as the CTIVD did not find any operations in which technical aids had not been removed or in which the report was missing in those cases where the aids had not been removed. However, it was not always clear from the report which aids had been removed at what time and why removal had or had not been possible. That is a failing.

In a number of operations the period between the last approved authorization request for an extension of the hacking power in an ongoing operation and the first clean-up attempt was long (about a year). As the technical aids were eventually removed, the legal obligation as such was observed.

Reporting
The law stipulates that records must be made of the hacking power exercised (reporting). This includes recording the assessments made when exercising the hacking power, newly identified or substitute automated devices or systems of a target, non-target or third party and assessments regarding the technical risks. In its review report no. 53, the CTIVD recommended that the services start logging (i.e. the continuous automated and comprehensive recording of data) the hacking power exercised and the related technical actions taken.[29] The ministers at the time adopted this recommendation. Recording serves internal control purposes and enables effective external review.

The policy of the services only states that the exercise of the hacking power should be recorded but gives no further details on how this should be done in practice.

In practice, both services, specifically the joint executive CNE department, *nonetheless lawfully* carry out the recommendations in CTIVD report no. 53 and the obligation to keep records by automated logging and a manual log.

29 CTIVD review report no. 53 (published in April 2017) on the use of the hacking power by the AIVD and the MIVD, *Parliamentary Documents II* 2016/17, 29 924, no. 149 (appendix), available at www.ctivd.nl.

Answer to investigative question 2

Bulk data sets are large collections of data, the majority of which concerns organizations and/or people who are not the subject of investigation by the services, nor ever will be. This means that collecting and further processing personal data in a bulk data set constitutes a severe privacy infringement. It is therefore important that the fundamental rights of those involved who are not under investigation by the services are sufficiently protected. In the investigation, the CTIVD examines to what extent the AIVD and the MIVD have put this into practice. The conclusions in this section apply to both the AIVD and the MIVD unless stated otherwise.

Data reduction

One statutory safeguard for legal protection is a limited retention period within which the data sets from special investigatory powers, thus including bulk data sets, must be assessed for relevance. At the end of the maximum retention period of 18 months, the law requires that data not assessed for relevance is destroyed. This prevents non-relevant data from remaining available to both services for a long period of time.

In a number of cases, the services have declared whole (or large parts of) bulk data sets relevant. As a result the data is retained without a definitive destruction term. The CTIVD considers this method to be an artifice aimed at extending the retention period of the bulk data sets in question. It is *unlawful* to declare data sets relevant that for the most part contain evidently non-relevant data, as the CTIVD noted in its third progress report.

Safeguards for further processing bulk data sets

The services use additional safeguards not explicitly laid down by law to access and use the collected bulk data sets. This is an application of the general requirement of proper and careful data processing and of the services' duty of care for the lawfulness and quality of data processing (Sections 18 and 24 of the ISS Act 2017). Although these safeguards have not been set out in overall policy for bulk data sets collected using the hacking power, it is existing practice for the services to work with an outer box/inner box procedure where it comes to bulk data sets collected using the hacking power. This procedure provides for a division of job roles and an authorization procedure (Internal Check) to access the data.

As regards the division of job roles, the CTIVD considers that this is a sufficient interpretation of the requirements of proper and careful data processing set under Section 18 of the ISS Act 2017, provided that sufficient distance, including physical distance, exists between data-analysts with outer box rights and the intelligence teams with which they are associated.

The CTIVD considers that in principle the authorization procedure used, also referred to as the Internal Check, forms a sufficient safeguard to protect data relating to organizations and/or people who are not the subject of investigation by the services, nor ever will be. The authorization procedure is therefore a sufficient implementation of the requirements of proper and careful data processing set under Section 18 of the ISS Act 2017.

Failure to follow the recommendation in report no. 55 regarding the automated return of data to the outer box after a period of time is *unlawful*.

As the Internal Checks are now recorded and the services are working on a system of periodic reports based on them, the CTIVD finds that the requirements set under Sections 18 and 24 of the ISS Act 2017 have been met.

The application of the outer box/inner box procedure to bulk data sets from two MIVD operations provides for a lower authorization level for checks than the Internal Check. This is a failing, given the observed safeguards and the specific nature of the operations in question.

In conclusion

The ISS Act 2017 does not lay down any specific regulation for processing bulk data sets, with the exception of bulk data from investigation-related interception. The investigation shows that legislation does insufficient justice to the operational interests of the services to process bulk data sets and to the protection of the fundamental rights of people who are not the subject of investigation by the services, nor ever will be. This topic deserves consideration, at the least, in the context of the evaluation of the legislation.

6. Recommendations

6.1 AIVD and MIVD

Policy and work instructions

Section 2.4: Set out in policy and/or work instructions what the procedure is of the Computer Network Exploitation (CNE) department when assessing technical risks, such as the four-eyes principle.

Section 2.5: Set out in policy and/or work instructions what the minimum requirements are for recording with respect to the clean-up obligation. Include what CNE must record in its manual log when a clean-up action was successful, such as a description of the technical aids removed and the time of removal. Furthermore, record when the hacking power is deemed to have ended and by what time a clean-up action should have taken place. The principle should be that a clean-up action is taken as soon as possible.

Section 2.6: Set out in policy and/or work instructions that keeping records on an investigatory power exercised must be done using automated and manual recording. Set out unambiguously in policy and/or work instructions which minimal automated logging the *operators* must set up and which events they should record manually in the log of an operation.

Section 3.3: Develop overall policy for bulk data sets, regardless of the investigatory power with which they were obtained. Set out unambiguously which safeguards apply, where responsibility for compliance has been assigned and how these safeguards manifest themselves in practice.

Practice

Section 2.4: Record the assessments regarding significant risks in the log of an operation, given the fact that automated logging itself is unsuitable to effectively reconstruct the risks of an operation after the fact.

Section 2.5: Draw up a report each time the authorization is rejected in operations where access is maintained because of an intended extension of the operation. The report must show why the technical aids were not cleaned up and what the corresponding risks are.

Section 3.2: Destroy the bulk data sets that were assessed as relevant in their entirety.

Section 3.3:

- Create effective distance, including physical distance, between data-analysts with outer box rights and the intelligence teams with which they are associated.
- Set up a standardized procedure for the periodic check of outer box authorizations for data-analysts.
- Based on Sections 18 and 24 of the ISS Act 2017, automated recording of search requests by data-analysts in the outer box must also serve the purpose of internal and external control.
- Lastly, the services should make the further development of reports on search requests of bulk data sets a top priority as they are a prerequisite for the lawful processing of bulk data sets.

6.2 AIVD

Practice

Section 2.3: Immediately destroy data collected without valid authorization in one operation, on the understanding that further investigation into the use of the data must remain possible.

Section 3.3: Examine how a higher authorization level for check requests can be achieved with greater distance between the requesting party and the authorizing party and set out the criterion as targeted as possible as a requirement for the substantiation of the check requests.

Oranjestraat 15, 2514 JB The Hague
P.O.Box 85556, 2508 CG The Hague

T T 070 315 58 20
E info@ctivd.nl | www.ctivd.nl