Review Report

about the use of cable interception by the AIVD and the MIVD

The snapshot phase

CTIVD no. 75

Adopted on 26 January 2022

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence
and Security Services

CTIVD no. 75

REVIEW REPORT

about the use of cable interception by the AIVD and the MIVD

Contents

Review Committee
on the Intelligence
and Security Services

CTIVD no. 75

REVIEW REPORT

about the use of cable interception by the AIVD and the MIVD

Summary

This review report deals with the deployment of cable interception by the AIVD (General Intelligence and Security Service) and the MIVD (Military Intelligence and Security Service) (hereinafter referred to as 'the services') in the snapshot phase. Cable interception is also referred to as bulk interception. This means that the services intercept and collect cable communications on a large scale, with most of these data relating to individuals and/or organisations that are not and will never be the subject of the services' investigations. However, it must be possible to relate the interception to one or more investigation assignments of the services. In this review report, the CTIVD (Review Committee on the Intelligence and Security Services) answers the following investigative question:

In the period from 1 May 2018 to 31 March 2021, did the AIVD and the MIVD lawfully operationalise an access location and lawfully exercise cable interception in the snapshot phase?

During the investigation period, the services made a cable route at a communication service provider (hereinafter referred to as 'provider') suitable for interception of communications, such as internet traffic. Communication over cable routes is sent through light signals that are transported via individual fibres. Dozens of channels can be distinguished within these fibres. The physical transfer point at a communication service provider where the services receive the intercepted data (the communication) is called an access location. The data stream that is relevant to the services for the established investigation assignments is acquired at the access location. In the context of enabling cable interception, the operationalisation of the access location, and the identification of potentially relevant channels, the services have deployed special investigatory powers, such as the obligation for providers to provide information and to cooperate.

The original intention of the services was to deploy regular cable interception on all available channels on certain cable routes at the access location. This was found unlawful by the Investigatory Powers Commission (TIB), as it was not proportionate and not 'as targeted as possible'. After that, the services sought and obtained authorisation to use the power of cable interception in the form of snapshotting. Snapshotting has no independent legal basis, but concerns a limited use of cable interception powers. The difference with regular interception is that snapshotting - including the related investigation - has an exploratory purpose, while regular cable interception aims to intercept data in order to process them into intelligence products. This is also referred to as 'production'.

The approved authorisation requests include safeguards to limit the deployment of cable interception to snapshotting.

For example, the services were authorised to intercept channels for up to two hours per day, for which they had justified in advance that these channels would have high intelligence value. Moreover, the data were not to be used by intelligence teams, but only for technical investigations by persons explicitly designated for that purpose. On the basis of technical and substantive characteristics, these officers examined whether the intercepted data actually had potential intelligence value for the services' investigative assignments. In addition, the data could be retained for a maximum of one year. The CTIVD has included compliance with these safeguards in its investigation and reports on this. In addition, the CTIVD wants to use this report to contribute to debate about cable interception and the forthcoming amendment of the Act by being transparent about the practices of the services - as much as possible given the state secret nature of their work.

Conclusions of the report

The main finding and conclusion of this review report is that the heads of the AIVD and the MIVD did not sufficiently fulfil the statutory duty of care during the investigation period (I). Besides further answering the investigative questions (II), the CTIVD notes that the interpretation given to cable interception in the parliamentary debate is at odds with technical practice (III). It is also recommended that snapshotting be given an independent legal basis (IV).

I. Inadequate fulfilment of the duty of care

In this review report, the CTIVD concludes that the statutory duty of care was inadequately fulfilled during the investigation period. This is a fundamental problem underlying many of the findings in this review report. The duty of care is laid down in Section 24 of the ISS Act 2017. This duty means that the heads of the AIVD and the MIVD are responsible for applying technical, staffing and organisational measures to ensure data are processed lawfully. Among other things, the duty of care entails that the services must continually be in control of the way in which they process data and that data processing is and continues to be in line with the applicable legal regulations (compliance).

The complexity, social sensitivity and necessity of the option to deploy cable interception powers mean that a lawful processing process should be high on the priority list of the heads of service. The CTIVD finds that fulfilment of the duty of care was subordinated to operational interests during the investigation period. In particular, the lack of logging suitable for compliance *purposes* and the lack of checks on the operation of the technical systems led to this conclusion. This was one of the reasons why unlawful conduct was created or detected too late during the interception process (see below).

At the end of August 2021, the CTIVD shared the findings of its investigation with both heads of service in light of their specific responsibilities for the duty of care. The services drafted an improvement plan. In addition to the improvement plan, the intention is for cable interception for intelligence purposes to be implemented in phases, known as the production phase. The services described that the technical chain will be tested first. Only if these tests are successful will storage of the data for intelligence purposes begin.

Increased oversight

Whether the services are ready for the production phase is a question the services themselves have to answer. The CTIVD will increase its oversight and report on this further. This includes overseeing the phased implementation of cable interception.

II. Answers to the investigative questions

The investigative question is twofold. First, the question pertains to operationalising the access location. The CTIVD concludes that the services acted lawfully in key respects when creating the access location. For instance, based on the duty to provide information, the services only requested and received legally authorised information and, at the time of the technical operationalisation of the access location, there was a valid authorisation under Section 53 of the ISS Act 2017. However, the CTIVD also found unlawful conduct. These pertain to the unauthorised use of investigatory powers and to activities that took place at the provider after the expiry of authorisation periods. See chapter 5 of this review report for a full description.

The second part of the investigative question pertains to conducting cable interception in the snapshot phase. Also in response to this question, the CTIVD concludes that the services acted lawfully in some respects and acted unlawfully in other respects. One of the main conclusions regarding lawful conduct is that the way the cable interception was carried out was an interpretation of the principle of specificity. The deployment of a power in a manner that is as targeted as possible depends on several criteria. An explanation of the specificity criterion involves more than just limiting the amount of data to be collected. The criteria allow for the specificity requirement to be implemented in a manner that does justice to the nature of cable interception.

Besides meeting the specificity criterion, the services destroyed the intercepted data in a timely manner and did not share the data with foreign services. The unlawful conduct found relates to insufficient compliance with certain safeguards from the requests for authorisation, including the safeguard that the data could not be made available to intelligence teams. See chapter 6 of this review report for a full description.

Recommendations

In the review report, the CTIVD makes three recommendations that mainly concern the fulfilment of the duty of care. The main recommendations concern placing ultimate responsibility for the entire interception chain of acquisition and processing at a central and sufficiently high level so as to ensure overriding authority within both organisations. In addition, tools should be set up for internal control andeffective external oversight, including the establishment of logging for *compliance* formatting.

III. Cable interception explained

The new cable interception power was a much debated topic during the political and public debate on the ISS Act 2017. The term ‘dragnet’ was often used here, as there were (and still are) concerns that communications of persons not under investigation by the services are systematically collected on a large scale. The public and political debate during and after the drafting of the ISS Act 2017 emphasised that the cable interception power should be deployed in a manner that is as targeted as possible and that this power is linked to investigation assignments to dispel perceptions of the dragnet. Moreover, it painted the picture that it is possible for the services to pinpoint the precise channels over which relevant communications will be transported in advance of deployment. In addition, the Ministers of the Interior and Kingdom Relations and of Defence have given commitments, for example that it is virtually impossible that cable interception will be used in the coming years to investigate communications with origin and destination in the Netherlands (with the exception of cyber defence). And that irrelevant traffic, such as that from streaming services and bittorrent traffic, is filtered out. It was also promised that cable interception would be ‘as targeted as possible’.

In this review report, the CTIVD concludes that the interpretation given to cable interception is at odds with the nature of the power, the means and with implementation in technical practice. The fact that deployment is linked to an investigation assignment and that the power should be deployed in a manner that is 'as targeted as possible' does not alter the fact that cable interception is by definition a bulk power with a high degree of inherent untargeted data collection. Most of the data intercepted will always pertain to individuals and/or organisations that are not and never will be under investigation by the services. At the same time, this is also the reason why cable interception was included in the ISS Act 2017. In particular, the need for cable interception, according to the legislature, lies in recognising unprecedented threats. The very fact that it involves uncovering unprecedented cyber and other threats means that this tool is only effective if there is a certain degree of untargeted data collection. The data ultimately stored by the services are related to the services' investigation assignments. However, the criteria used to establish this relationship tend to be broad, such as geographical origin or language. In addition, the cable routes or channels through which data relevant to the investigation assignments are transported cannot be fully predicted. After all, these do not take a fixed route, but follow the cheapest and/or fastest route.

The CTIVD also concludes that the commitment on communications with origin and destination in the Netherlands is unclear and raises questions in practice, for example when it comes to feasibility and technical implementation. With regard to the commitment on the negative filtering of traffic from streaming services and bittorrent traffic, the question arises whether such traffic is actually irrelevant in advance.

The CTIVD considers it important, also in the context of an amendment to the ISS Act 2017, to draw lessons from the knowledge and experience gained with cable interception. This means that in the further public and political debate, the nature of this means and its infringement on the fundamental rights of citizens should be named by the legislature and the necessity of this means in this context should be argued, taking into account the technical reality and feasibility of implementing the required safeguards.

IV. Legal basis for snapshotting

In the review report, the CTIVD concludes that snapshotting should be provided with an independent legal basis. The current system of the ISS Act 2017 assumes that the services are sufficiently able to justify in advance that the interception is as targeted as possible. This, however, is not the case. The investigation shows that the duty to provide information as set out in Section 52 does not provide the services with sufficient information for this purpose. The CTIVD endorses the need for snapshotting and analysis of these data, as these activities contribute significantly to the interception being as targeted as possible for the production phase.

In the absence of a specific legal basis, the services were forced to deploy snapshotting based on the cable interception power. However, the legal requirements are focused on cable interception for production purposes. As a result, they are not in line with the nature and purpose of snapshotting, which is to be able to justify in advance that cable interception for production purposes is as targeted as possible.

The CTIVD therefore considers it important, also in view of foreseeability and legal certainty, that snapshotting is provided with an independent legal basis. What is important here is that the specificity requirement is applied in a way that is in line with the circumstances of the case; in this case, the nature and purpose of snapshotting.

CTIVD no. 75

REVIEW REPORT

about the use of cable interception by the AIVD and the MIVD
The snapshot phase

1. Introduction

This review report deals with investigation-related cable interception by the General Intelligence and Security Service (hereinafter referred to as 'the AIVD') and the Military Intelligence and Security Service (hereinafter referred to as 'the MIVD'). Investigation-related cable interception means that the AIVD and the MIVD (hereinafter referred to as 'the services') can intercept cable-bound communication in large quantities without this interception being aimed at a specific target, such as a person or organisation.[1]

However, it must be possible to relate the interception to one or more investigation assignments of the services. These investigation assignments arise from the Integrated Intelligence and Security Services Order (hereinafter referred to as 'the Order'). Since the entry into force of the Intelligence and Security Services Act (hereinafter referred to as 'the ISS Act 2017') on 1 May 2018, the services have been allowed to deploy the special investigatory power of cable interception. Under the previous act, the ISS Act 2002, they already had the power to intercept untargeted ether communications, such as radio traffic and satellite communications. 'Cable' generally refers to fibre-optic routes over which communications are sent, such as internet traffic from individuals and organisations. These communications consist of both technical traffic data (e.g. who is communicating with whom) and the content of communications (such as the content of an e-mail).

In this review report, the Review Committee on the Intelligence and Security Services (hereinafter referred to as 'the CTIVD') answers the question whether, in the period from 1 May 2018 to 31 March 2021, the AIVD and the MIVD lawfully operationalised an access location and lawfully exercised cable interception in the snapshot phase. In this period, the services made it possible to intercept the cable and also actually intercepted the cable. This cable interception was conducted in the form of snapshotting, which involves the short, integral cable interception of data streams. After interception, the relevance of the data stored for one or more investigation assignments of the services is assessed on the basis of technical and substantive characteristics. In the investigation period, safeguards were used to limit the infringement of the fundamental rights of citizens.

In this report, the CTIVD assesses the lawfulness of the conduct of the services in applying the legal power of cable interception in the snapshot phase. In addition, the CTIVD wants to use this report to contribute to debate about cable interception and the forthcoming amendment of the Act by being

1 A target is a person or organisation being investigated by the AIVD or the MIVD. See Appendix III to this review report for a full glossary.

transparent about the practices of the services - as much as possible given the state secret nature of their work.

Reason for the investigation

On 18 January 2021, the CTIVD announced it would investigate the services' use of cable interception powers. This investigation was largely prompted by the public debate surrounding the ISS Act 2017 and its parliamentary debate, as well as the progress reports on the implementation of this Act as issued by the CTIVD.[2]

The new cable interception power was a much-debated topic during the political and public debate on the ISS Act 2017. The term 'dragnet' was often used here, as there were (and still are) concerns that communications of persons not under investigation by the services are systematically collected on a large scale. The interception of entire residential areas was often used as an example in the debate. This could put random citizens in the services' 'dragnet'. An advisory referendum on the ISS Act 2017 was held on 21 March 2018, with more voters voting against the Act than in favour.[3]

Following the referendum, the Ministers of the Interior and Kingdom Relations and of Defence made a number of commitments. Important concerns here include the different retention period for intercepted data (three times one year instead of three years) and the commitment that 'there is virtually no prospect of cable interception being used in the coming years to investigate communications that originate and terminate in the Netherlands (with the exception of investigations for cyber defence purposes)'.[4] The Ministers also promised that, like other special investigatory powers, the deployment of the cable interception power by the services would be 'as targeted as possible'.[5,6] Members of the House of Representatives also called for accelerated oversight by the CTIVD of the services' implementation of and compliance with the Act.[7] The CTIVD was asked by the Ministers of the Interior and Kingdom Relations and of Defence to carry out enhanced oversight of the implementation of cable interception and the commitments made until the evaluation of the Act.

Since the entry into force of the ISS Act 2017, the CTIVD issued four progress reports in which it reported on the progress of the implementation of the ISS Act 2017. In these progress reports, it consistently found that cable interception was not yet operational, except for the exploratory activities carried out by the services.[8] The progress reports detected risks that also pertained to cable interception. In addition, the CTIVD issued two reports on investigation-related interception of satellite and radio communications.[9] There was no cable interception at that time. There reports describe findings that also touch on investigation-related cable interception. The political and public interest in the subject of cable interception, as well as the request for increased oversight of its use, prompted the CTIVD to investigate cable interception even at this exploratory stage. Analysing and then testing practices will provide insight into the implementation of cable interception and do justice to the concerns raised in the political and public debate.

---

2 Progress reports I to IV inclusive, available on ctivd.nl.
3 49.44% of voters voted against. 46.53% of voters voted in favour. 4.03% were blank votes.
4 Section 4 Policy Rules of the ISS Act 2017; *Parliamentary Papers II* 2017/18, 34588, no 76.
5 *Parliamentary Papers I* 2017/18, 34588, G.
6 In this report, chapter 6 reviews how these commitments have been implemented in practice.
7 See the letter from the Ministers of the Interior and Kingdom Relations and of Defence to the President of the House of Representatives dated 25 April 2018, *Parliamentary Papers II* 2017/18, 34588, no 76 (appendix) and the letter to the President of the Senate dated 6 April 2018, *Parliamentary papers I* 2017/18, 34588, G.
8 Progress Reports I and II describes that the services are operationalising cable interception. Progress Report III describes that interception powers has not yet been deployed and Report IV refers to 'exploratory activities'.
9 CTIVD review report no. 63 on the application of filters in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2018/19, 29 924, no 188 (appendix) (September 2019) and CTIVD review report no. 64 on the application of selection in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2019/20, 29 924, no 192 (appendix) (October 2019).

Structure of the report and reading guide

In this review report, the CTIVD examines and assesses the lawfulness of the services' conduct during the period from 1 May 2018 (the entry into force of the ISS Act 2017) to 31 March 2021 (hereinafter referred to as 'the investigation period'). During this period, the services operationalised a transfer point for the intercepted data, an 'access location', and deployed cable interception in the form of snapshotting. This section briefly explains the services' activities that have been investigated by the CTIVD and where the findings of these activities can be found in this report. Before discussing the findings from the investigation, Chapter 2 provides a brief explanation of cable interception.

The services started preparatory activities in 2016 so as to be ready to deploy the new cable interception powers after the entry into force of the ISS Act 2017. During this period, they gained knowledge of the Dutch cable landscape, for example. These activities are outlined in Chapter 3 to provide context to the other findings in this review report.

In Chapter 4 of this review report, the CTIVD discusses the overall view obtained through its investigation. This overall view relates to the fulfilment of the legal duty of care during the investigation period.

During the investigation period, the services started operationalising an access location. The term 'access location' refers to the physical transfer point for investigation-related interception at a communication service provider. The data stream that is relevant to the services for the established investigation assignments is acquired at this access location. Communication over cable routes is usually sent through light signals that are transported via individual fibres. 'Dozens' of channels can be distinguished within these fibres. The legislature described that the services then identify the fibres and channels that can reasonably be expected to be relevant to the performance of one or more of their investigation assignments.[10] In practice, intercepting a fibre-optic route means that the services receive a copy of the light signals transported over that route. To operationalise such an access location, the services have special investigatory powers that are laid down in the ISS Act 2017.[11] The findings on operationalising the access location are discussed in Chapter 5. The term 'operationalise' refers to the set of technical and other actions required to make a particular fibre-optic route suitable for interception. This is done in cooperation with the provider that is the owner of this route.

After operationalising the access location, the services proceeded to actually intercept communications during the investigation period. To this end, too, they have special legal investigatory powers.[12] During the investigation period, the legal investigatory power of cable interception in the form of snapshotting was used to a limited extent. The findings on cable interception are discussed in Chapter 6.

The investigation revealed findings that do not directly address the question of whether the services deployed cable interception lawfully. These findings are discussed in Chapter 9. These are important given the debate on cable interception and the upcoming legislative amendment to the ISS Act 2017.

10 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 110.
11 Sections 52 and 53.
12 Sections 48 and 49(1).

Investigative question and scope

This review report answers the following investigative question:

In the period from 1 May 2018 to 31 March 2021, did the AIVD and the MIVD lawfully operationalise an access location and lawfully exercise cable interception in the snapshot phase?

To operationalise the access location, the services relied on, among other things, the duty of communication service providers to provide information and to cooperate (Sections 52 and 53). Section 48 (cable interception) was used for snapshotting. The stored data were then investigated under Section 49(1) (search aimed at interception). In addition, the general data collection and processing provisions of the ISS Act 2017 apply.[13] Of course, this report also considers previous findings from, among other things, the CTIVD's progress reports on the services' fulfilment of their duty of care when it comes to cable interception.[14] In addition to these legal provisions, the services have included additional safeguards in their authorisation requests. The Investigatory Powers Commission (*Toetsingscommissie Inzet Bevoegdheden*, hereinafter referred to as 'TIB') also imposed conditions on these authorisations. The CTIVD also included compliance with these safeguards and conditions in its investigation. This makes it a comprehensive test.

Joint implementation by two services

The implementation of cable interception takes place within the framework of investigation assignments approved by the Ministers of the Interior and Kingdom Relations and of Defence arising from the Order. Implementation is vested in a joint unit of the AIVD and MIVD, the Joint Sigint Cyber Unit (hereafter referred to as 'JSCU'). This unit is managed by both services. This means that there is a joint responsibility. Requests for authorisation to deploy investigatory powers are, however, prepared by each individual service. That is, the AIVD makes requests to the Minister of the Interior and Kingdom Relations and the MIVD makes requests to the Minister of Defence. The reason for this is that the investigation assignments for which cable interception is used may vary from one service to another.

In the investigation period, this meant that requests for authorisation of special investigatory powers, such as authorisation to perform cable interception, were addressed by the services to the relevant Ministers. After the Ministers have granted authorisation, the TIB reviews the lawfulness of the authorisation. The TIB's decision is binding. If the authorisations granted by the Ministers are found to be lawful by the TIB, cable interception can be implemented. This is implemented jointly by the JSCU. As such, the findings and lawfulness decisions apply to both the AIVD and the MIVD for the purpose of the CTIVD assessment.

Course of the investigation

At the end of August 2021, the CTIVD shared the findings of its investigation with both heads of service in light of their specific responsibilities for the duty of care. Following these consultations, the services drew up an improvement plan, which aims to strengthen service-wide internal control of data acquisition and processing. This is discussed in more detail in section 4.4.

13 See Appendix I to this review report for the full legal framework.

14 CTIVD no. 59. Progress report on the operation of the ISS Act 2017, *Parliamentary Papers II* 2018/19, 34 588, no. 80 (appendix) (Dec. 2018), CTIVD no. 62, Progress report II on the operation of the ISS Act 2017, *Parliamentary Papers II* 2018/19, 34 588, no. 83 (appendix) (June 2019), CTIVD no. 66, Progress Report III on the operation of the ISS Act 2017, *Parliamentary Papers II* 2019/20, 34 588, no. 85 (appendix) (Dec. 2019), CTIVD no. 69, Progress Report IV on the implementation of the ISS Act 2017, *Parliamentary Papers II* 2019/20, 34 588, no. 87 (appendix) (Sept. 2020), CTIVD review report no. 63 on the application of filters in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2018/19, 29 924, no. 188 (appendix) (Sept. 2019) and CTIVD review report no. 64 on the application of selection in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2019/20, 29 924, no. 192 (appendix) (Oct. 2019).

The present review report was drafted on 17 November 2021, after which the Ministers of the Interior and Kingdom Relations and of Defence were given the opportunity to respond to the findings in it. The responses of the Ministers to the findings were received on 18 January 2022 and led to several amendments and clarifications. The review report was adopted on 26 January 2022.

Appendices to the report

The review report contains several appendices. Appendix I sets out the assessment framework. Appendix II describes the investigation method adopted. Appendix III contains the glossary.

The review report has no classified appendix.

References to legislation

In this review report, the CTIVD frequently refers to legislative section numbers. Unless explicitly indicated otherwise, the CTIVD is referring to the ISS Act 2017.

Definition

In this report, the CTIVD wants to avoid any confusion between the terms 'investigation-related interception', 'bulk interception' and 'untargeted cable interception' and, therefore, uses the term 'cable interception' as much as possible in this report. So this basically means bulk cable interception. Where this report refers to investigation-related interception, this means the (technology-independent) legal system.

2. Explanation of cable interception and snapshotting

This chapter briefly explains cable interception and snapshotting, and serves as background information for interpreting the CTIVD's findings. First, it discusses the need for introducing the power in the ISS Act 2017. It then discusses European Case Law on cable interception. It then outlines the process of cable interception. Finally, it discusses snapshotting in more detail.

Rationale of cable interception

Cable interception involves bulk interception of communications, which means there is a high degree of inherent unfocused data collection. However, it must be possible to relate the interception to one or more investigation assignments of the services. The investigation assignments arise from the Order. With cable interception, the services also intercept (on a large scale) the data of persons who are not the subject of their investigation, nor ever will be. Large data collections in which the (vast) majority of data are about persons who are not the subject of investigation are called bulk data sets. Therefore, investigation-related interception is referred to as a bulk interception. This power greatly intrudes on the privacy of citizens and is thus the subject of public debate.

When the ISS Act 2017 was drafted, the need for the cable interception power was linked to the AIVD and MIVD's task of identifying threats and risks to national security in a timely manner, and at the earliest possible stage. To achieve this, the services must identify individuals, organisations and threats they did not know about before, so-called unknown threats.[15] Incidentally, this also applied to untargeted interception of satellite and radio communications under the ISS Act 2002. Another important reason for cable access is that technological changes mean that more and more communications are sent by cable. The increase in cyber threats has also prompted the legislature to allow cable interception.

Cable interception means that large quantities of cable-bound communication are intercepted without this interception being aimed at a specific target, such as a person or organisation. Should the AIVD and the MIVD only collect data on known targets or threats, chances are that they would discover new (plans for) attacks and cyber attacks too late. In addition, when identifying a new target or an imminent threat, it is important that they can use historical data to identify possible accomplices, for example. For these reasons, the services record communications, which are (only) related to their investigation assignments, but whose actual intelligence value is not yet established.

ECHR case law

The need for cable interception was also addressed in recent case law of the European Court of Human Rights (ECHR). On 25 May 2021, the Grand Chamber delivered its judgment in the cases of Big Brother Watch and Centrum för Rättvisa.[16] In this judgment, the ECHR considered the extent to which legislation enabling cable interception was compatible with the provisions of the European Convention on Human Rights (ECHR).

15 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 93.
16 EHRM 25 May 2021, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (Big Brother Watch et al. v. the United Kingdom and ECHR 25 May 2021, no. 35252/08, ECLI:CE:ECHR:2021:0525JUD003525208 (*Centrum för Rättvisa v. Sweden*).

In previous judgments, the ECHR ruled that cable interception may be necessary in a democratic society, provided it has adequate safeguards.[17] The Court confirmed this in the recent May 2021 judgments, in which it concludes that this form of interception is 'a valuable technological capacity to identify new threats in the digital domain'.[18] It argues that cyber and other threats to the national security of states have increased due to increased digitalisation and technological developments. In doing so, the ECHR pays attention to the bulk nature of cable interception, which entails that such a system must have appropriate safeguards.[19] The Court writes as follows: "In the current, increasingly digital, age the vast majority of communications take digital form and are transported across global telecommunications networks using a combination of the quickest and cheapest paths without any meaningful reference to national borders. Surveillance which is not targeted directly at individuals therefore has the capacity to have a very wide reach indeed, both inside and outside the territory of the surveilling State."[20]

In its judgments, the ECHR also addressed the intrusion on citizens' privacy as a result of cable interception. The right to protection of privacy is laid down in Article 8 of the ECHR. In determining the degree of intrusion, the ECHR describes four stages.[21] In short, according to the Court, the intrusion increases as the data are drawn further into the data processing of the intelligence and/or security services. The Court distinguishes the following stages: (1) collecting and storing communications, (2) searching the stored data using selectors or search queries, (3) examining the data selected in the previous stage and (4) using (or exploiting) the data in intelligence products. At the final stage, according to the Court, data may also be shared with services in other countries.[22] The judgments also identify eight safeguards that apply specifically to bulk interception and should be implemented in national law.[23] The need for robust safeguards, according to the Court, is greatest at the stages where specific data of individuals are examined and used, as that is where the infringement of individual citizens' rights is greatest.[24]

Cable interception process

The explanatory memorandum to the ISS Act 2017 also includes a description of (the stages of) cable interception.[25] For the reader's understanding, this description is reproduced here, in abbreviated form. It should be noted that this is a general description and the actual practices of the services are covered in Chapters 5 and 6.

Cable interception starts with the choice of the cable interception location. This choice is determined by the point in the Dutch (cable) infrastructure at which the services can intercept data necessary for their investigation assignments. The physical transfer point at a communication service provider for the intercepted data is called an access location.

17 See ECHR 29 June 2006, ECLI:CE:ECHR:2006:0629JUD005493400 (*Weber and Saravia v. Germany*), ECHR 1 July 2008, ECLI:CE:ECHR:2008:0701JUD005824300 (*Liberty et al. v. United Kingdom*), ECHR 19 June 2018, no. 35242/08, ECLI:CE:ECHR:2018:0619JUD003525208 (*Centrum för Rattvisa v. Sweden*) and ECHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2018:0913JUD005817013 (*Big Brother Watch et al. v. The United Kingdom*).
18 Par. 323 (*Big Brother Watch et al. v. the United Kingdom*) and par. 237 (*Centrum för Rattvisa v. Sweden*).
19 Par. 347 (*Big Brother Watch et al. v. the United Kingdom*) and par. 261 (*Centrum för Rattvisa v. Sweden*).
20 Par. 322 (*Big Brother Watch et al. v. the United Kingdom*) and par. 236 (*Centrum för Rattvisa v. Sweden*).
21 Par. 324-331 (*Big Brother Watch et al. v. the United Kingdom*) and par. 238-245 (*Centrum för Rattvisa v. Sweden*).
22 The ISS Act 2017 allows sharing of data with foreign intelligence and security services at an earlier stage. Sections 62, 64 and 89 allow the AIVD and the MIVD to share unevaluated data with other services. Unevaluated data are data that have not been sufficiently scrutinised by the AIVD and the MIVD, which means that there is not enough information on the nature and actual content of the data to adequately assess the necessity, propriety and accuracy of the data provision.
23 Par. 361 (*Big Brother Watch et al. v. the United Kingdom*) and par. 275 (*Centrum för Rattvisa v. Sweden*).
24 Par. 330 (*Big Brother Watch et al. v. the United Kingdom*) and par. 244 (*Centrum för Rattvisa v. Sweden*).
25 *Parliamentary Papers II* 2018/19, 29924, no. 3, p. 109 et seq.

The data stream that is relevant to the services for the established investigation assignments is acquired at this access location. At the access location, the services must then choose from the available fibres of a cable. 'Dozens' of channels can be distinguished within these fibres. The services identify the fibres and channels that are reasonably expected to be relevant to the performance of one or more of their investigation assignments. To this end, they can request information from a provider, such as a market operator or other party, where the access location could be realised. The services can also perform snapshots to determine which fibres and channels are considered relevant. This should help ensure that the services only process those data streams that are relevant to their investigations.[26]Not all data present on the intercepted fibres are stored for further processing. This is because filtering takes place shortly after the actual interception of data. Filtering is the process that determines what data are actually stored for the intelligence process. The stored data are also reduced to those that may be relevant to the services' ongoing investigations. This means that data found to be irrelevant to any of the services' ongoing investigations and data not assessed for relevance within the retention period must be destroyed immediately. The retention period for cable-interception data is one year. This retention period may be extended twice, by a maximum of one year each time.[27] The Minister, or the head of the service on the Minister's behalf, must authorise an extension of the retention period. The extension request need not be submitted to the TIB. The stored data may be used by intelligence teams for the purpose of further processing, such as analysis and selection (examining the contents of data). As already explained above, this description is tailored to regular cable interception and not snapshotting.

Similarities and differences between cable interception and interception of satellite and radio communications

The process of interception of satellite and radio communications has many similarities with that of cable interception, but there are also differences:

Whereas cable interception requires an access location, this is not required for interception of satellite and radio communications. Interception of satellite and radio communications is mainly carried out in Burum and Eibergen, respectively, where the services have their own dishes and antennas. This allows them to pick up all kinds of signals without depending on a provider. Therefore, the deployment of investigation-related interception of satellite and radio communications does not, in principle, require reliance on the legal duty of providers to cooperate.

The data streams are filtered in a broadly similar way. Both cable interception and interception of satellite and radio communications involve negative and positive filtering. Negative filtering means that after interception, traffic is not stored based on certain characteristics. Positive filtering means that traffic is actually stored based on certain characteristics.

Snapshotting

As already mentioned, the cable interception power was introduced with the ISS Act 2017. Before the introduction of this Act, under the ISS Act 2002, the services already had the power to untargeted interception of non-cablebound communications (or ether communications), e.g. radio signals and satellite communications. These forms of interception now coexist and, because of the technology-independent wording of the ISS Act 2017, both fall under the power of 'investigation-related interception' (Section 48).

26 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 110.
27 Section 48(5) of the ISS Act 2017 and Section 4 of the Policy Rules of the ISS Act 2017.

Because interception of satellite and radio communications has been possible for some time, this can be referred to as 'standard practice'.[28] This standard practice influenced how cable interception was deployed during the investigation period.

Snapshotting is an activity that already took place during interception of satellite and radio communications. The term comes from the area of signals intelligence (or Sigint). Under the ISS Act 2002, snapshotting, in practice, fell under the power to 'search'.[29] This power was included in Section 26 of the ISS Act 2002. The exercise of this power, as well as the actual interception (Section 27 of the ISS Act 2002), did not require the authorisation of the Minister concerned.[30] Therefore, the services had great freedom in deploying this power (and how it was deployed). The search power could be used in support of both targeted and untargeted interception. One of the purposes of searching in the context of untargeted interception was to determine the channels (or links in the case of satellite interception) through which potentially relevant communications are sent. Based on this investigation, the limited interception capacity could be used in the best possible way, by only intercepting channels containing as much potentially relevant traffic as possible.[31] This activity therefore contributes significantly to ensuring that the (regular) power of interception is used in the most efficient and targeted way. It is important to note that snapshotting already took place in the preliminary stage of interception of satellite and radio communications: making short integral recordings was a standard part of the search process, but was not referred to as snapshotting at that time. So no authorisation from the Ministers concerned was required for making these recordings (the searching).

Snapshotting under the ISS Act 2017

Snapshotting has no separate legal basis in the ISS Act 2017, as under the ISS Act 2002, but concerns the deployment of Section 48 (cable interception). The stored data are then investigated with the use of Section 49(1) (search aimed at interception). The term 'snapshotting' as such first appeared in the explanatory memorandum of the ISS Act 2017, where the term was used twice in total.[32] Snapshotting is described as part of the data reduction process (limiting the amount of data stored) for cable interception and not as an independent process. The relevance of the data obtained through snapshotting to one or more of the services' investigation assignments (also referred to as intelligence value) is assessed on the basis of technical and substantive characteristics of a data stream. However, there is no explicit link to a legal power. Nor is there any mention of any applicable safeguards. Therefore, snapshotting is not enshrined in the ISS Act 2017 as a separate, specific activity.

The legislature did try to enshrine the practice of searching from the ISS Act 2002 in the ISS Act 2017. For example, the search power of Section 26 of the ISS Act 2002 is (partly) included in the current Section 49(1). The explanatory memorandum explains that Section 49(1) is also referred to as 'search aimed at interception'. It is therefore most obvious to classify the activity of snapshotting under search aimed at interception. Here, it is important to note that in order to carry out a search aimed at interception, it is necessary to intercept data in the first place. In other words, authorisation for interception under Section 48 is required first.[33]This link with the deployment of the special investigatory powers in Sections 48 and 49(1) raises practical issues. These issues are addressed in chapter 9.

---

28 Appendix A to CTIVD review report no. 63 on the application of filters in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2018/19, 29924, no. 188 (appendix) (Sept. 2019), p. 13.
29 CTIVD review report no. 28 on the deployment of Sigint by the MIVD, *Parliamentary Papers II* 2011/12, 29924, no. 74 (appendix), p. 40.
30 Under the ISS Act 2002, there was no Investigatory Powers Commission (TIB). The TIB was introduced in the ISS Act 2017..
31 CTIVD review report no. 28 on the deployment of Sigint by the MIVD, *Parliamentary Papers II* 2011/12, 29924, no. 74 (appendix), p. 19.
32 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 110.
33 An important difference from the ISS Act 2002 is that, at that time, no authorisation was required for both searches and interceptions.

Schematic representation of regular cable interception and snapshotting during the investigation period

The following is a simplified representation of the process of regular cable interception and the process of snapshotting, as carried out during the investigation period. It is important to note that the features below were applicable during the investigation period, but are not legally enshrined requirements. After all, snapshotting has no independent legal basis. These features of snapshotting are the result of the restrictions and safeguards that the services included in the requests for authorisation to deploy cable interception. Important features of regular cable interception and snapshotting are:

- Snapshotting is a form of cable interception. It involves the same kind of data, i.e. content and metadata of communications transported by cable;
- Regular cable interception is investigated both for the purpose of optimising cable interception and for processing by intelligence teams. Snapshotting takes place for the purpose of optimising cable interception;
- The duration of interception varies. Regular cable interception is requested for a maximum of one year and can take place non-stop during this year. Snapshotting is also requested for a maximum of one year; however, interception was allowed for two hours per day per channel during the investigation period;
- There is positive filtering in case of a regular deployment of cable interception. This means that only communications that meet certain characteristics are stored. Characteristics may include certain IP addresses or e-mail addresses, but also, for example, broader filters such as language;
- Negative filtering is part of regular cable interception and also had to take place during snapshotting. Negative filtering means that traffic is actually not stored based on certain characteristics;
- Data obtained by cable interception may be retained for one year. This retention period may be extended a maximum of two times by one year. On the other hand, data collected through snapshotting had to be destroyed after one year. No extension of this period was allowed during the investigation period.

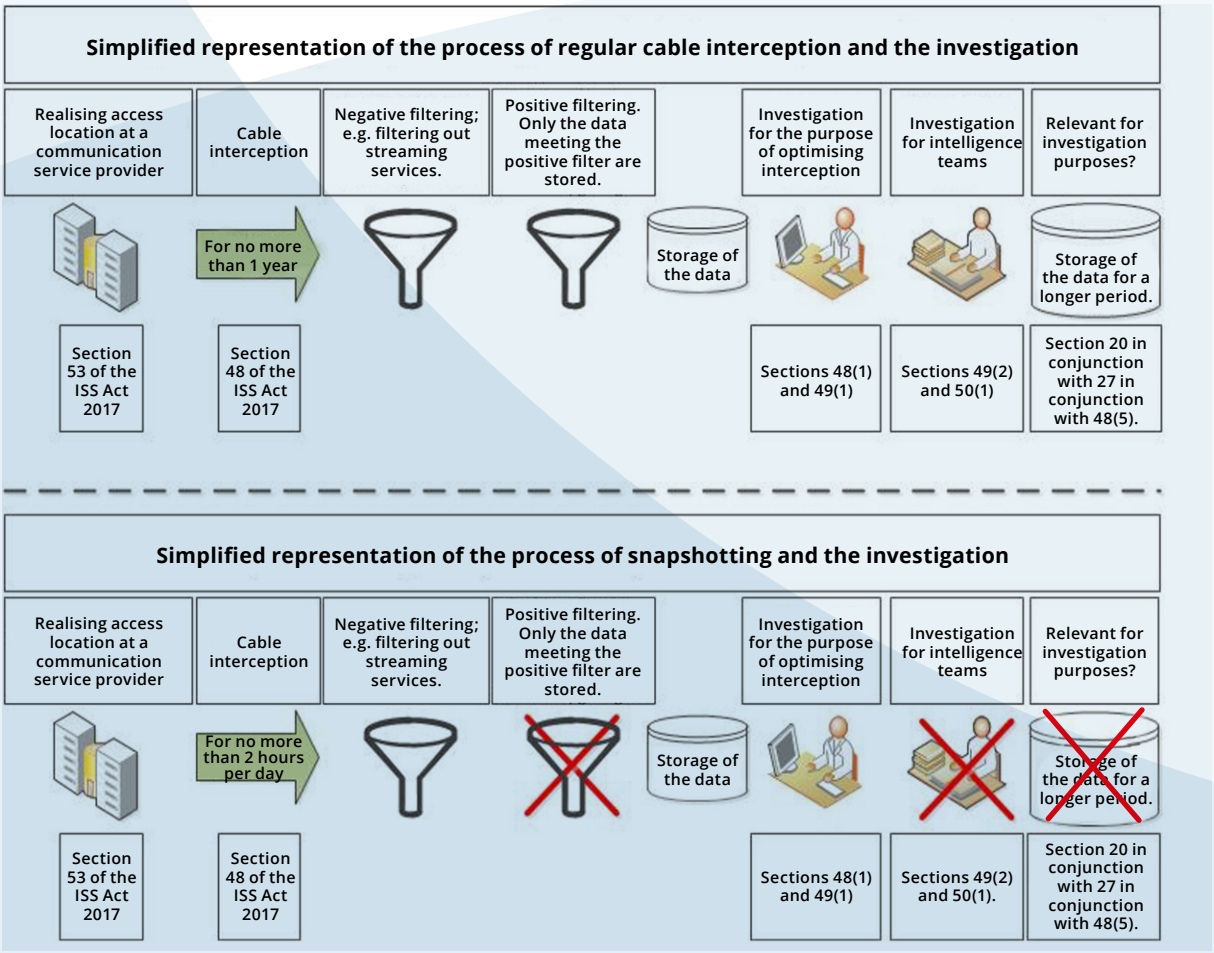

Figure 1 Simplified representation of cable interception and snapshotting in the investigation period

3. Preparatory activities for the entry into force of the ISS Act 2017

This chapter covers the activities carried out by the services before the entry into force of the ISS Act 2017 on 1 May 2018. These activities took place before the investigation period and provide context to the further findings in this review report. The CTIVD makes no lawfulness decision on these activities.

Cable landscape

In the run-up to the final entry into force of the new ISS Act, the services started mapping the Dutch cable landscape and the course of communication flows in 2016. During this phase, a team was formed within the project that was responsible for finding a potentially suitable access location. When it comes to cable interception, as already explained in Chapter 2, the services rely on organisations operating in the cable landscape, for example companies selling fibre-optic routes (and fibre-optic route capacity).

The important thing was to find locations where the services could intercept communication streams that could be related to their investigation assignments, e.g. communications from parties active in countries the AIVD and MIVD are investigating under the Order. These communication streams are handled via cable routes, which are best described when comparing them with the road network. Based on this comparison, the team mapped the locations where motorways and other roads enter and leave the Netherlands and which parties provide transport services on these routes. Ultimately, this information was used to choose an access location before the entry into force of the new ISS Act. After the entry into force of the ISS Act 2017, the services were ready to immediately start the next step: actually operationalising the access location.

Access location

The above-mentioned team was initially limited in its search to using public information, information from commercial sources and information coming from foreign partner services.[34] This information, as such, was not already available to the services, nor was it readily available elsewhere. It was therefore important to combine this information to arrive at the most complete picture of the Dutch cable landscape. Moreover, in 2017, informal discussions were held with various market operators in the Netherlands.

Based on the information gathered, the team was able to recommend a suitable first access location in autumn 2017. The decision on this was made in December 2017. The final choice was made based on several considerations, which were mainly strategic in nature. An important consideration was to find a party that was expected to easily comply with the legal duty to cooperate. Another important aspect was that this party had to handle large communication streams, as this increased the likelihood that relevant traffic could be intercepted on these cable routes for the various investigation assignments. Based on these factors, an access location was chosen at a provider that handles communication streams that can be described as a 'four-lane motorway', i.e. through which high volumes and a variety of mainly international data traffic are sent.

34 This was because there was no legal power under the ISS Act 2002 to request these data. This only became possible after the introduction of Section 52 of the ISS Act 2017.

The interception chain

During this period, the services not only searched for a suitable access location, but also made preparations for setting up the 'interception chain'. This could include setting up equipment and systems at the services needed to process communication streams intercepted at the access location into usable information for intelligence teams. It soon became clear that setting up such a chain is a technically very complicated process. Moreover, the services lacked experience in cable interception. The experience gained with interception of satellite and radio communications could not automatically be applied to cable interception.

4. Overall view: inadequate fulfilment of the duty of care

In this chapter, the CTIVD concludes that the services inadequately fulfilled their statutory duty of care during the investigation period. This finding extends across the entire investigation, forming a connecting thread in this review report. This is a fundamental problem underlying many of the other findings in this review report. This had prompted the CTIVD to discuss these findings at this point in this review report. In this chapter, the CTIVD first outlines the context of operationalising and implementing cable interception. It also details the duty of care and its fulfilment by the services. The chapter concludes with an interim conclusion and recommendations.

4.1 Context

The CTIVD notes that during the investigation period, the services mainly focused on operationalising cable interception within a short period of time. On the one hand, this deployment led to success, as the services managed to build a fully operational cable interception chain. This required great effort and commitment from staff of both services. On the other hand, the CTIVD notes that compliance with the statutory duty of care was thereby subordinated to operational interests.

In operationalising cable interception, the services have had to act as technical and legal pioneers in a complex environment. The services were technical pioneers because while they had experience with intercepting satellite and radio communications, this experience could not be applied automatically to cable interception. This meant that the services had to start from scratch when developing many systems, processes and procedures. Where this was not the case, the services made the choice to embed the technically complex process of cable interception into existing structures. In addition, operationalising an access location, building an interception chain and implementing legal and other safeguards is a technically complex process.

The services were also legal pioneers, as the legal powers to operationalise an access location and intercept communications had not previously been used for cable interception. With the introduction of the ISS Act 2017 came the introduction of the TIB, which, also without existing experience in this area, was to assess requests for authorisation in the context of cable interception. There were also legal complexities as the services had to flesh out the requirements set by the ISS Act 2017 on a lawful implementation of cable interception. This includes the requirement that cable interception, which involves a high degree of inherent untargeted data collection, should be used in a manner that is 'as targeted as possible'. In addition, the interpretation given to cable interception in the parliamentary debate on the ISS Act 2017 had to be taken into account. The TIB faced the same issues. In addition to the requirements of the ISS Act 2017 and the parliamentary debate, the services made additional commitments and safeguards in the requests for authorisation and in communications with the TIB which also needed to be implemented in practice. This created a complex set of requirements.

4.2 Duty of care

The duty of care is laid down in Section 24 of the ISS Act 2017. This duty means that the heads of the AIVD and the MIVD are responsible for applying technical, staffing and organisational measures to

ensure data are processed lawfully.[35] Promotion of the quality of data processing to ensure that data processing is lawful is a new requirement that was not included in the old ISS Act 2002. The duty of care explicitly requires more from the AIVD and the MIVD than just the introduction of the duties that the law imposes on them when collecting and analysing data and when they are actually being used by staff members of the services, among other things[36]

Among other things, the duty of care entails that the services must continually be in control of the way in which they process data and that they ensure that data processing is and continues to be in line with the applicable legal regulations (compliance). Policy, process descriptions and working instructions, in which consideration is given to the allocation of roles and responsibilities, may contribute positively to this.

The need to continually be in control also requires the services to use a number of tools that give them an insight (a central insight) into the functioning of data-processing processes and systems and, as such, puts them in a position to promptly identify risks and take appropriate measures. This is important for internal control in the services but also for the facilitation of effective external oversight by the CTIVD.

The technical and legal complexities of cable interception meant that risks of unlawful conduct were and are high. This requires that aspects of the duty of care be explicitly incorporated into the operationalisation and interception process from the outset. During the legislative process and since the entry into force of the ISS Act 2017, the CTIVD has repeatedly addressed aspects of the duty of care, including in the field of investigation-related interception in a broad sense. To this end, it initially conducted a baseline measurement and reported on the progress of the implementation of the Act in the progress reports already mentioned above. It has also addressed (the system of) investigation-related interception in two review reports.[37] In these reports, it made recommendations that were adopted by the Ministers concerned.

4.3 Fulfilment of the duty of care

When operationalising cable interception, the services opted for a project structure with several subprojects. During the investigation period, there was no central and complete overview of the entire operationalisation process. No multidisciplinary perspective was taken into account to flesh out that process, or to mitigate possible lawfulness risks and other risks. Putting aspects of the duty of care into practice, such as sufficient control mechanisms regarding lawful conduct, was not part of the initial project plan for cable interception. This review report describes several specific findings where there was either an increased risk of unlawful conduct or where this unlawful conduct actually manifested itself. Such risks and unlawful conduct could possibly have been mitigated if components of the duty of care were sufficiently embedded. Broadly speaking, the CTIVD concludes that the duty of care has not been sufficiently fulfilled in the following areas:

35 Section 24(2)(a).
36 CTIVD no. 59, Progress report on the operation of the ISS Act 2017, *Parliamentary Papers II* 2018/19, 34 588, no. 80 (appendix) (Dec. 2018), p. 7.
37 Review report no. 63 on the application of filters in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2018/19, 29 924, no 188 (appendix), review report no 64 on the application of selection in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2019/20, 29 924, no. 192 (appendix).

Automated logging

Both for carrying out adequate internal control and effective external oversight, it is important that data processing operations are recorded in such a way that there is an understanding of the path taken by data. From acquisition and storage to destruction of data, it should be transparent what happened to the data in the systems. Examples include when and why data were acquired, when and for what purpose data were accessed, whether data are relevant and when data were destroyed. This recording should be sufficiently precise to verify compliance with the data processing provisions of the ISS Act 2017. Automated logging is one way to achieve this. For many processes in the cable interception chain, the services have set up automated logging of these components, but this does not apply to all processes and components. In addition, logging is set up for the purpose of information security and not for the purpose of compliance. As such, logging is not designed to answer the question of the extent to which data have been processed lawfully. Setting up logging for the purpose of compliance should be included from the development of systems and applications. Putting such logging in place afterwards requires a lot of effort and is a complex process. Timely consideration should be given to how this should be done and how the logging can then be accessed for the purpose of internal control and external oversight. Involving internal stakeholders and the CTIVD is essential here.

Internal control

The CTIVD concludes that in practice, insufficient internal control was exercised over the cable interception process. At several points during the investigation period, legal safeguards were translated into technical implementations. Such technical implementations should be checked before they are put into production. Moreover, structural checks should be performed during the data processing process to ensure a correct operation of the technical systems. These checks have not been sufficiently structural, leading to the occurrence or late detection of unlawful conduct. These specific findings are detailed in Chapter 6.

Considerations on use of equipment

The CTIVD notes that the services use third-party equipment and systems in the interception chain. This is common in the practice of the services. Such equipment and systems (within the services' sphere of influence) are also subject to aspects of the duty of care, such as safeguarding the quality of data processing. That means the equipment and systems are reliable and the services guarantee a correct functioning. If not, there may be risks of unlawful data processing. The duty of care requires the services to weigh up these aspects and, if necessary, take risk-mitigating measures. This consideration should be the starting point for deciding whether or not to commission such equipment or systems. The CTIVD found this consideration only with regard to operational risks, but not with regard to risks related to the quality of data processing.

Recording of decisions

Decisions should be recorded in such a way that the decision moments and the considerations underlying these decisions can be traced. This applies not only to management-level decisions, but also to legal and operational decisions. The CTIVD concludes that the recording of decisions within the cable interception project was not always complete. During its investigation, the CTIVD therefore often relied on the recollections of staff members. This is not only undesirable with regard to the exercise of internal control by the services, but also complicates effective external oversight.

Policies, process descriptions and work instructions

Partly in response to previous review reports and progress reports published after the ISS Act 2017 came into force, the services developed policies for cable interception and interception of satellite and radio communications, including process descriptions and work instructions, during the investigation period. These were ready during the course of 2020. This implies that for much of the investigation period, there were no mature policies in place in this area. The CTIVD had already established this before.[38] In the context of the current investigation, the CTIVD found that the services have been gradually drafting policies and work instructions in parallel with the operationalisation of cable interception. This procedure involves risks. It should be noted that the policies ultimately developed pertain to the regular implementation of cable interception, where no separate policies were drafted for snapshotting and the associated investigations. The services initially did not anticipate the procedure during the investigation period, the mere snapshotting and the restrictions formulated in the process. After all, the first requests for authorisation were for the regular implementation of cable interception. As a result, there was little time to develop appropriate policies.

Improvement programme and audits

During 2019, partly in response to the aforementioned review reports and progress reports, the services launched an improvement programme called 'Investigation-related interception in Order'. This programme focused on fixing shortcomings and mitigating risks in the process of investigation-related interception following the two CTIVD reports on interception of satellite and radio communications. As part of this programme, new organisational units were created in late 2019, including the Joint Data Compliance Team (JDCT). The JDCT is a part of the JSCU, whose tasks include preventing, detecting and managing (lawfulness) risks in data processing. The JDCT conducted a service-wide inventory of lawfulness risks in the first half of 2020. This inventory included the process of cable interception. The identified risks were included in a risk register that provided insight into service-wide lawfulness risks. In addition, in 2020 the AIVD conducted two internal audits specifically aimed at identifying risks of unlawful conduct in relation to its own policies and to the control measures for investigation-related interception. Both audits, completed in March and October 2020, identified high and medium risks. During the investigation period, not all risks had yet been addressed with mitigating actions in practice. Nevertheless, the improvement programme and the audits carried out are assessed by the CTIVD as positive developments.

4.4 Improvement plan for cable interception

The findings made by the CTIVD during its investigation, as described in this chapter and in Chapters 5 and 6, prompted the CTIVD to share them with the heads of the AIVD and the MIVD in the interim in late August 2021. The CTIVD considered this important to allow the services to take the necessary measures to strengthen internal control over cable interception, even before proceeding to 'production', or regular interception. Following this, the services drew up an improvement plan, which aims to strengthen internal control of data acquisition and processing. This plan not only focuses on cable interception, but on the acquisition and processing activities of both services in a broad sense. This plan was shared with the CTIVD in early November 2021. The CTIVD notes that the improvement plan consists of three parts. The first part contains objectives to improve the chain of investigation-related interception. This objective had not been coordinated service-wide in both organisations at the time of writing this report. In addition, the objectives are conceptual in nature and can therefore be read as lines of thought.

38 CTIVD no. 69, Progress report IV on the implementation of the ISS Act 2017, *Parliamentary Papers II* 2019/20, 34 588, no. 87 (appendix) (September 2020), p. 14.

The second part consists of measures implemented in the short term. Examples include measures pertaining to testing, improvement in the area of authorisations and retention of user logs for internal control purposes. In order to actually use user logs for internal control purposes, coordination with different units within the services needs to take place first. The third part of the improvement plan concerns a description of the ambition of both services on further developing the compliance system and strengthening internal control in the long term. This part does not yet contain any concrete measures.

Further specifying and implementing the improvement plan will mitigate some of the risks identified in cable interception. The CTIVD identifies the following concerns when it comes to the improvement plan:

- Data acquisition and processing is the core activity of the services. Investigation-related interception is a special component of this, partly because of the high volume and variety of the intercepted data, including the speed of their acquisition and processing. This requires control over the entire cable interception chain to ensure lawful implementation. Fragmented responsibility means that there is no complete overview and correlations between risks and measures may be lost. Final responsibility for the entire chain of acquisition and processing should be vested centrally and at such a high level that there is overriding authority within the entire organisations of both services. On the one hand so as to ensure centralised overview, and on the other so as to ensure a timely and effective implementation of measures;
- The risk is that risk management mainly results in administration of (potential) risks and that no measures are taken in practice. When implementing the proposed measures, impacts in practice should therefore remain paramount;
- Compliance is still seen too much as a primary staff responsibility. For effective implementation, compliance should be set up as a line responsibility. It is an ongoing process, which service staff should proactively implement;
- Internal control and its tools should also enable effective external oversight.

In addition to the improvement plan, there is also the intention for a phased implementation of cable interception for intelligence purposes, the so-called production phase. The services described that the technical chain will be tested first. Only if these tests are successful will storage of the data for intelligence teams begin. However, setting up full logging for compliance purposes is a long-term measure and not ready at the time the services move to the production phase.

4.5 Interim conclusion

The CTIVD concludes that the interplay of technical complexity, a legally complex framework and the desire to realise cable interception in the short term has created an area of tension in which the duty of care has become secondary. This affected the process of operationalisation and implementation of cable interception during the investigation period. During this process, insufficient attention was paid to aspects of the duty of care, creating risks of unlawful conduct. These risks actually resulted in unlawful conduct in certain aspects during the investigation period. The CTIVD did not find any indication that the unlawful conduct identified in this review report resulted from wilful actions of individual employees. They stem in part from insufficient internal controls over the entire cable interception chain.

The core activity of the services is to process data to identify as many known and unknown threats as possible in a timely manner. For the purpose of their core business, the services have far-reaching powers that should be backed by adequate safeguards. The fact that the services are allowed to exercise these powers places great responsibility on the heads of the services. This responsibility is enshrined by law in the duty of care. One of the far-reaching powers is cable interception. The complexity, social sensitivity and necessity of the option to deploy this power mean that a lawful implementation should be high on the priority list of the heads of service.

As the CTIVD already concluded in its fourth and concluding progress report, measures such as conducting an audit can be seen as positive, but continuing attention should be paid to the translation into practice. Implementation of the duty of care took place in parallel with the implementation of cable interception, but did not sufficiently result in measures in practice. After the investigation period, the services drew up an improvement plan, which aims to strengthen service-wide internal control of data acquisition and processing. The CTIVD endorses the measures contained therein and stresses that achieving actual effects in the services' implementation practice should be the highest priority throughout the organisation. The situation in which risk management is a 'paper exercise' without effective impact in practice should be avoided. Final responsibility for the entire chain of acquisition and processing of investigation-related interception data should therefore be vested centrally and at a sufficiently high level with overriding authority within the organisations of both services. On the one hand in order to create a centralised overview, and on the other so that measures can be implemented effectively. In addition, compliance should not be a staff responsibility, but a line responsibility. It is an ongoing process, which the services should proactively implement across their organisations.

4.6 Recommendations

Given the above findings, the CTIVD recommends the services:

- To vest the final responsibility for the entire investigation-related interception chain centrally and at a sufficiently high level with overriding authority within the organisations of both services.
- To fulfil the statutory duty of care by at least:
  - setting up appropriate tools for compliance purposes, which includes putting logging in place. Both internal stakeholders and the CTIVD should be involved here. These tools should also be suitable for effective external oversight. Logging should be in place before starting the production phase of cable interception;
  - aligning the existing policy and work instructions with the practice of snapshotting and related investigation which emerged during the investigation period, where this has not already been done, and by ensuring that complete process descriptions are in place.

5. Making the cable suitable for interception at the access location

This chapter describes the activities carried out by the services, following the entry into force of the ISS Act 2017 on 1 May 2018, in the context of operationalising the access location, i.e. making the cable suitable for interception. As described in Chapter 3, by that time the services had already chosen the provider where they wanted to operationalise an access location. The introduction of the ISS Act 2017 provided the legal powers that allowed the services to require the provider to provide information about its network (duty to provide information) and to cooperate in making its network suitable for interception (duty to cooperate). This chapter answers the first part of this report's investigative question:

In the period from 1 May 2018 to 31 March 2021, did the AIVD and the MIVD lawfully operationalise an access location?

5.1 Assessment framework

The overview below lists the main requirements for the duty to provide information (Section 52) and the duty to cooperate (Section 53) as included in the ISS Act 2017. For a full description of the legal assessment framework, the CTIVD refers to Appendix I of this review report.

Specific provisions from Section 52

- The data requested fall under the Data Provision (Investigation of Communications under the ISS Act 2017) Decree (Besluit gegevensverstrekking onderzoek van communicatie Wiv 2017);
- The head of the service must have authorised use of the duty to provide information.

Specific provisions from Section 53

- The Minister must have authorised use of the duty to cooperate. The TIB will assess the lawfulness of this authorisation;
- Authorisation of the use of the duty to cooperate may be extended for a maximum of one year each time;
- The content of the authorisation request to use the duty to cooperate must meet the requirements above;
- If the cooperation is no longer necessary, the facilities installed may remain in place for a maximum of one year. If there is no longer a reason to keep the facilities in place, the provider will be relieved of its duty.

5.2 Compliance

In this section, the CTIVD discusses the findings and assessment of the use of Section 52 and Section 53 in the context of operationalising the access location. It also discusses other special investigatory powers that have been used for this purpose. The section concludes with an interim conclusion answering the question of whether the services lawfully operationalised the access location.

5.2.1 Findings regarding the duty to provide information (Section 52)

Prior to operationalising the access location, the services imposed a duty on the relevant communication service provider to provide information about its network. This information was used to map the provider's network and determine which cable routes and channels contain potentially relevant data streams. The access location was operationalised once the services had identified these data streams and obtained authorisation to impose the duty to cooperate. This means that technical facilities were put in place to receive and handle traffic streams. In addition, the services received structural information from the provider about its network and data streams. The purpose of obtaining this structural information was to ensure continued cable interception and timely awareness of any changes in traffic streams in the provider's network.

Between March 2018 and April 2021, the services received information on a structural basis from the provider where the access location was operationalised. The information mainly concerned technical and business data of the provider, which provided a picture of the services provided by the provider. Information about communication streams, such as network design, routing and signal characteristics, was provided as well.

The services initially requested this information under Section 52. The order to provide the information was valid for a period of three months. The information was used to determine the location of potentially relevant data streams. After operationalising the access location, it was necessary for the services to continue receiving information from the provider to keep them informed of changes in the provider's network. The services then included the obligation to provide information in the duty to cooperate (Section 53). The period during which the duty to cooperate was imposed did not directly correspond to the period during which the duty to provide information was imposed. Information about the network was also provided by the provider during this short interim period.

The services had expected that the authorisation under Section 53 would not be renewed in time. Section 53 is statutorily linked to Section 48 (cable interception). The duty to cooperate can therefore only be used if authorisation to deploy cable interception has already been granted. However, the extension of cable interception was uncertain. The services nevertheless wanted to be kept informed by the provider on an ongoing (and proactive) basis. For this, they again made use of Section 52 to continue receiving information on a structural basis from the provider where the access location was operationalised. This use of the duty to provide information took one year.

Assessment

In the CTIVD's assessment, the services only requested data covered by the Data Provision (Investigation of Communications under the ISS Act 2017) Decree[39]. In doing so, they did not depart from the categories of data specified by law.

With regard to the duty to provide information as contained in Section 52, the legislative history suggests that its use is only for the purpose of preparing for interception and cannot be deployed after operationalisation of the access location. It also appears to be a one-off query rather than a structural provision.[40] The CTIVD's investigation shows that the sequence suggested in the legislative history does not correspond to practice. The use of

39 Bulletin of Acts and Decrees (Stb.) 2018, 116.
40 See the assessment framework in Appendix I of this report.

Section 52 after operationalising the access location is not, in the CTIVD's view, contrary to the ISS Act 2017. The same goes for using the duty to provide information for a structural period instead of a one-off query. The law does not preclude the use of Section 52 after operationalising the access location. Nor does a fixed statutory authorisation period apply to the use of Section 52.[41] However, it is important that the justification of Section 52 is in line with practice. However, the justification of the second order under Section 52 in the investigation period did not correspond to the actual purpose of this use. The justification of the order had included purposes that could not apply at that time, given that the access location had already been chosen and had been operationalised.

The CTIVD concludes that the vast majority of the information received had a legal basis and that the files were received either under the duty to provide information (Section 52) or the duty to cooperate (Section 53). A small proportion of the files received had no legal basis.

Finally, the CTIVD considers that the interest to be protected as set out in Sections 52 and 53 is different to many other special investigatory powers of the services. Where the other investigatory powers often set standards in respect of the infringement of the fundamental rights of citizens, Sections 52 and 53 create a duty for providers. The consequences of the absence of a legal basis for a provider were limited to the provision of data that the provider was not obliged to provide at that time. The fundamental rights of citizens are not affected by this, as the data provided do not relate to citizens and/or their data.

5.2.2 Findings regarding the duty to cooperate (Section 53)

During the investigation period, Section 53 was used twice by the services against the same provider. Under the ISS Act 2017, the duty to cooperate can only be used in conjunction with the cable interception power (Section 48), as the duty refers to cooperating in the performance of interception. Cable interception was interrupted during the investigation period. The reason for this was the TIB's assessment that authorisation to extend the interception power had been granted unlawfully. Because of the aforesaid link with Section 48, this automatically meant that the authorisation for the duty to cooperate was also temporarily interrupted. After the services received another extension from the Ministers concerned and it was found to be lawful by the TIB, the services could continue cable interception and the duty to cooperate. The authorisation period for these approved extensions ended in March 2021. For about a month during the investigation period, there was no authorisation to use the duty to cooperate.

The services and the provider consulted frequently prior to and during the operationalisation of the access location. The services indicate that there is good cooperation and a good understanding. However, the services did not always communicate to the providers the applicable authorisation periods pertaining to the duty to provide information and to cooperate. The duration of the initial order to provide information (under Section 52) had not been communicated to the provider. The same applies to the authorisation for the second order, which was granted internally. Although the services handed over a 'provider letter' once at the time of the initial order, it did not contain any deadlines. A provider letter is a document informing the provider that and how it must comply with the statutory duty to cooperate or to provide information.

41 Pur suant to Section 29, an authorisation to use a special investigatory power as referred to in paragraph 3.2.5 of the ISS Act 2017 may be granted for a period of no more than three months. Section 52 is a special investigatory power from paragraph 3.2.5. However, no authorisation is granted here. Instead, the head of the service instructs a provider to provide data.

Also for the power under Section 53, a provider letter was handed over once. This letter did contain the authorisation period. However, there was no provider letter for the second authorisation granted for this power. After the expiry of the authorisation period for the extension, the services did not communicate to the provider in time that the authorisation period for cable interception and the duty to cooperate had expired.

After the expiry of the authorisation periods for Sections 48 and 53 in 2021, the communication service provider performed work in its network on the instructions of the services. This work started during the investigation period, but was largely performed outside the investigation period. According to the services, the work was necessary in order to be able to resume interception as soon as possible once the services would be granted a new authorisation to do so. If the work were to start only after obtaining a new authorisation under Sections 48 and 53, this would potentially delay interception. The work partly pertained to data streams for which authorisation had been granted in the initial authorisation request, but also partly pertained to data streams for which authorisation had not yet been granted. This work was performed by the provider on a voluntary basis, according to the services.

Assessment

Failure to comply with the duty to cooperate is punishable by law. For a provider, it should therefore be clear for which period the duty is imposed. With regard to notifying authorisation periods, the CTIVD considers that for Sections 52 and 53, the law does not provide for an explicit obligation of the services to notify the communication service provider. However, given the above, the CTIVD considers it important that the provider is notified of the (authorisation) periods when the duty to cooperate is imposed, so as to make sure that the period and duration of this duty are clear to the provider.

The investigation also shows that the provider performed work outside the authorisation period under Section 53. When asked, the services indicated that this work was performed on a voluntary basis. The CTIVD applies the principle that there should always be a legal basis for receiving information and performing work. For cooperation by a communication service provider cannot be entirely voluntary, as the law contains a duty to cooperate. The existence of a legal duty to cooperate precludes voluntary cooperation. In addition, there is no equal relationship between the provider and the services, which means that cooperation cannot be simply voluntary. Finally, it is important to note that the provider was not always informed about the period of the duty to provide information and the duty to cooperate. The question is therefore whether the provider knew that there was no longer a duty to cooperate.

With regard to the work performed, the CTIVD considers the following. In the CTIVD's view, only subsection 6 of Section 53 (duty to cooperate) can provide a basis for work to be performed outside the authorisation period under Section 53. Section 53(6) requires a provider to keep the installed facility in place in its network for one year after the expiry of the authorisation period, in case the services want to use the interception facilities again, for example in an acute emergency. In the CTIVD's assessment, this obligation of the provider to maintain the facilities may entail that it should also be possible to perform maintenance work. After all, without maintenance, this obligation has no added value. The maintenance work should allow interception to proceed at very short notice. The CTIVD notes that some of the work performed by the services was aimed at this goal, namely resuming interception as soon as a new authorisation would be granted. However, much of the work pertained to the operationalisation of a new cable route for which no authorisation had been granted yet.

Authorisation for interception yet to be granted and cooperation by the provider cannot be anticipated, as both are subject to a lawfulness assessment by the TIB. Moreover, the requests for authorisation always explicitly mentioned the cable routes. The CTIVD therefore concludes that such work does not fall within the scope of keeping an installed facility in place.

5.2.3 Other powers

Apart from the powers discussed above, the services also deployed other (special) powers of performed actions that correspond to the use of a power in the context of operationalising the access location.

For instance, the services performed actions under Section 15. Under this section, the heads of the services may make necessary provisions for the security of service staff members. This requires authorisation from the heads of the services; it cannot be mandated. During the investigation period, however, no authorisation was granted at the appropriate authorisation level. Actions have also been performed that would normally require a power under Section 40 in conjunction with Section 28(2)(a) (observation in support of proper performance of duties). No authorisation was requested and/or granted for the use of this power.

Assessment

The other powers were used without authorisation at the appropriate authorisation level. In the CTIVD's assessment, one of the reasons for the services' actions was that, for these specific elements, insufficient coordination was sought with legal staff and the service units normally involved in the implementation or preparation of these powers. The CTIVD also believes that there was no central and complete overview of the entire operationalisation process.

5.3 Interim conclusion

This chapter described the findings that address the first part of the investigative question, namely whether the services lawfully operationalised an access location during the investigation period. The CTIVD's investigation shows that operationalising the access location meant that the services had to act as pioneers. The duty to provide information and the duty to cooperate were used for the first time, and the services had to find out how to ensure that information could be received on a structural basis both before and after operationalising the access location. The services also ran into the situation where there was temporarily no authorisation for cable interception and, as a result, the duty to cooperate could not be used. However, work had to be performed in order to be able to resume interception as soon as possible once the services would be granted a new authorisation to do so. If the work were to start only after obtaining a new authorisation under Sections 48 and 53, this would potentially delay interception.

With regard to the first part of the investigative question, which pertains to the lawfulness of operationalising an access location, the CTIVD concludes that:

- The services received information on a structural basis from the provider in the context of realising the access location. In doing so, they did not depart from the categories of data permitted by law. The vast majority of the information received during the investigation period also had a legal basis, either under the duty to provide information (Section 52) or the duty to cooperate (Section 53). Frequent consultations were held with the provider prior to (and during) the operationalisation of the access location. At the time of the technical operationalisation of the access location, there was a valid authorisation under Section 53. The services acted lawfully in these respects.

- After the expiry of the authorisations for cable interception (Section 48) and the duty to cooperate (Section 53), the services instructed the communication service provider to operationalise new cable routes, while no new authorisation to intercept these routes had been obtained yet. Such work cannot be performed on a voluntary basis, nor is it covered by keeping the installed facility in place (Section 53(6)). Moreover, the services received information from the provider for short periods without a legal basis. Finally, apart from the use of the duty to provide information and to cooperate, the services used other (special) powers for the purpose of operationalising the access location. No valid authorisation had been granted for these powers. The services acted unlawfully in these respects.

5.4 Recommendations

Given the above findings, the CTIVD recommends:

- Laying down the authorisation periods, methods of use and the scope of the duty to provide information and to cooperate in policies and work instructions. This should at least show how and when these duties are communicated to the relevant provider and what the content of the provider letters should be. They should also specify that such work cannot be performed by the provider on a voluntary basis. The services should ensure proper records of the provider letters and compliance with the relevant policies and work instructions.

6. Implementation of cable interception: snapshotting

This chapter deals with the implementation of the cable interception power by the services. It first discusses the assessment framework. This consists of both the legal requirements and the safeguards included in the requests for authorisation that the services addressed to the Ministers and the TIB. It is these promised safeguards that led to a limited use of cable interception, known as snapshotting. However, the power used is still the cable interception power, despite the fact that this power was used in the form of snapshotting. It then briefly describes how the snapshot phase was established during the investigation period. It then discusses the services' compliance with the safeguards included in the requests and tests them against the frameworks of the ISS Act 2017. At the end of this chapter, the CTIVD answers the second part of the investigative question of this review report:

In the period from 1 May 2018 to 31 March 2021, did the AIVD and the MIVD lawfully exercise cable interception in the snapshot phase?

The CTIVD has not investigated the substantiation of the requests for authorisation, as their lawfulness has already been assessed by the TIB. This means that the CTIVD has not re-assessed the requirements of necessity, proportionality and subsidiarity. However, the same does not apply to the specificity requirement. The CTIVD has included this in its assessment because the Ministers of the Interior and Kingdom Relations and of Defence explicitly asked it to report on this.[42]

6.1 Assessment framework

Snapshotting has no separate legal basis in the ISS Act 2017, as under the ISS Act 2002, but concerns the deployment of Section 48. The stored data are then investigated under Section 49(1). Under Section 48, the AIVD and the MIVD are authorised to carry out "investigation-related interception, reception and recording of any form of telecommunication or data transfer". The section does not specify that it must be a particular form of interception, such as cable interception or interception of satellite and radio communications. This is due to the fact that the ISS Act 2017 was written in technology-neutral terms. In practice, this means that the services are authorised to store communications or data obtained through satellites or internet cables, for example. This form of interception is not exclusively aimed at specific targets (for a more detailed explanation, see Chapter 2).

Pursuant to Section 48 (interception), the services may also conduct technical analyses to optimise use of the interception power. To this end, they are also allowed to consult content, provided they only do so to check the proper performance of receipt. In this context, 'content' refers to the content of communication (such as the text of an e-mail) in contrast to traffic data, i.e. metadata (who is communicating with whom. For example, the sender and receiver of an e-mail). A search aimed at interception is laid down in Section 49(1). This power is closely related to the power of interception from Section 48. In practice, these two powers are therefore applied for together. A search aimed at interception allows the services to investigate data intercepted with Section 48 for the purpose of:

42 Letter to the President of the Senate dated 6 April 2018, Parliamentary papers I 2017/18, 34588, G.

- determining the characteristics and nature of the telecommunication;
- determining the identity of the person or organisation associated with the telecommunication.

In short, this investigatory power enables the services to determine whether they are actually intercepting the data envisaged.

In the overview below, the CTIVD briefly discusses the main requirements set out in the ISS Act 2017 for the deployment of cable interception. The overview also contains the restrictions and safeguards that the services included in the requests for authorisation to deploy cable interception. Together, they form the framework used by the CTIVD in its lawfulness assessment. For a full description of the legal assessment framework, the CTIVD refers to Appendix I of this review report.

Specific provisions from Sections 48, 49(1) and explanatory notes thereto

- Authorisation for the deployment of cable interception and search aimed at interception is granted for up to one year by the Minister concerned, after which its lawfulness is assessed by the TIB (see section 6.3.1);
- Data may only be processed for the purposes set out in Sections 48 and 49(1). Records may be kept of the results of the investigation based on Section 49(1) (see section 6.3.2);
- A division of roles and tasks exists when intercepted data are processed, and the relevant employees should be designated (see section 6.3.2);
- The power of interception is deployed in a manner that is 'as targeted as possible' (see section 6.3.3);
- The power of cable interception will not be used to investigate communication that originates and terminates in the Netherlands, except where an investigation relates to cyber defence (see section 6.3.4);[43]
- Data acquired through cable interception may be retained for up to one year. This period may be extended by one year a maximum of two times. The extension must be authorised by the head of the service (see section 6.3.5).

Additional safeguards and restrictions

- The safeguards below are additional to the legal framework from the ISS Act 2017. These safeguards were either included by the services in the relevant requests for authorisation or were included in an explanation provided by the services in response to questions from the TIB. These specific safeguards were therefore applicable during the investigation period.
- The services only intercept channels for which the authorisation granted has been assessed as lawful by the TIB (see section 6.3.1);
- Interception is limited to a recording of up to two hours per day per channel (see section 6.3.1);
- The services 'generate' metadata based on characteristics of the raw intercepted communications. At least half of these generated metadata should be destroyed within three months (see section 6.3.5);
- The intercepted data are stored for a maximum of one year, unless they are deemed relevant in the interim. Data declared to be relevant are not made available to intelligence teams (see section 6.3.5));[44]

43 This is a reproduction of the commitment as given by the Ministers of the Interior and Kingdom Relations and of Defence in the covering letter to the Policy Rules of the ISS Act 2017, *Parliamentary Papers II* 2017/18, 34588, no 76, p. 3.

44 This safeguard stems from the statutory retention period. The goal of intercepting the data should be achieved after one year. Therefore, an extension of the retention period is not to be expected.

- Only on rare occasions will data be declared relevant by officials designated for this purpose. This will be done at most at the raw package level and only to the extent that it is unavoidable in support of a report that deals with assessing the potential intelligence value of a data stream (see section 6.3.5);
- The intercepted data are not made available to intelligence teams for further processing (see section 6.3.6);[45]
- Traffic from streaming services (such as Netflix and Spotify) and bittorrent traffic does not pass through thanks to the use of negative filters (see section 6.3.7);[46]
- The data obtained through snapshotting are not shared with foreign services (see section 6.3.8);
- Only certain analysis techniques (defined to the TIB) are applied to the intercepted data (see section 6.3.9).

6.2 Creation of the 'snapshot phase'

It was not the services' original intention to deploy cable interception in the limited form of snapshotting. They initially, in the autumn of 2018, submitted a total of seven requests for the deployment of the interception power and the associated search power aimed at interception.[47] These requests were approved by the Ministers concerned and assumed a 'regular' deployment of the cable interception power. That is, using the special investigatory powers of selection and automated data analysis, the intercepted data would be made available to intelligence teams.[48] The requests pertained to intercepting all available channels on certain cable routes at the access location. Here, it was foreseen that the services could determine the intelligence value of these channels at their discretion to assess which channels would be put 'into production'. Putting a particular channel into production means that the intercepted data are processed throughout the interception chain; that is, the data are filtered and then stored for analysis in the intelligence process. This is similar to the procedure used for interception of satellite and radio communications.[49] These authorisations were assessed by the TIB at the end of 2018. The TIB concluded that the authorisations granted by the Ministers of the Interior and Kingdom Relations and of Defence were unlawful. The TIB's decision is binding. That is, the special investigatory power approved by the Minister could not be deployed. According to the TIB, the way in which the services wanted to deploy cable interception did not meet the requirement that the deployment should be 'as targeted as possible'. Moreover, the TIB ruled that the proposed deployment was not proportionate. For the services, this meant going back to the drawing board to change their approach in the light of the TIB's assessment.

45 This safeguard also stems from the fact that authorisation was sought only for Sections 48 and 49(1). The data may only be investigated for the purposes mentioned in these sections. Investigations for the purpose of the intelligence process require authorisation under Sections 49(2) and 50. This safeguard does mean that data from cable interception should not be included with already ongoing authorisations under Section 49(2) and Section 50 for, for example, interception of satellite and radio communications.

46 This is also a representation of the text as included in the appendix to the letter to Parliament 'Wiv 2017 and regeerakkoord' of 15 December 2017 from the Minister of the Interior and Kingdom Relations and Defence, *Parliamentary Papers II* 2017/18, 34588, no. 69, p. 3. This provides information about the implementation of the authority to intercept cables.

47 Four AIVD requests and three MIVD requests. These requests were largely similar except for the investigative questions and areas of investigation.

48 Such deployment is provided for in the legal system of investigation-related interception (Sections 48 to 50).

49 See Chapter 2 of this report for a more detailed explanation of interception of satellite and radio communications.

This led to the services submitting new requests in early 2019. This involved two AIVD requests and one MIVD request. These three requests were approved by the Ministers concerned. These new requests were significantly different from the requests submitted in 2018. The main change was the form of interception: instead of the 'regular' form of interception, it concerned only the limited use of cable interception; snapshotting. As explained in Chapter 2, the purpose of this form of short-term interception is to investigate intercepted channels for potential intelligence value. Therefore, there is no positive filtering at this stage. The main restriction during the investigation period was that the intercepted data would not be made available to intelligence teams under any circumstances. In other words, no interception for 'production' purposes. The consideration for this restriction was that this would allow the services to first assess the communications handled through the targeted cable routes. Based on that assessment, they could submit a more targeted request for interception on behalf of the intelligence teams at a later date.

Another change was the choice to intercept certain channels on the cable routes only. To this end and in response to queries from the TIB, the services had divided the available channels into three categories, depending on the expected intelligence value (with category 1 for those channels with expected high intelligence value). In the first quarter of 2019, the TIB ruled that the authorisations had been lawfully granted, but only made this decision for channels classified in category 1. These requests for authorisation were therefore very different from the deployment initially requested by the services (in 2018). In essence, the difference could not have been bigger: from broad deployment to a very limited form of cable interception. After the operationalisation of the access location and the technical creation of the interception chain, the services started intercepting data in the form of snapshotting in late 2019.

In early 2020, the services then submitted three requests (again two from the AIVD and one from the MIVD) for extension of the powers requested in 2019. These requests were authorised by the Ministers concerned. The TIB assessed these granted authorisations as unlawful. The TIB reached this conclusion because, among other things, these requests lacked a safeguard, which was included in the 2019 requests. This involved no longer negatively filtering traffic from streaming services and bittorrent traffic. This approach was considered by the TIB to be contrary to the interpretation of the cable interception power as contained in the legislative history of the ISS Act 2017. In addition, it was deemed in violation of the specificity requirement. Following this, the services submitted new authorisations approved by the Ministers concerned in which these deliberate changes had been reversed. These requests were assessed as lawful by the TIB in March 2020. The term of these requests was again the statutory period of one year and ended in March 2021.

6.3 Compliance

In this section, the CTIVD outlines the procedures used by the services for implementing the cable interception power through snapshotting.

6.3.1 Authorisation to intercept on specific channels for a limited duration

During the investigation period, cable interception for snapshot purposes was authorised twice for the statutory term of one year. Therefore, the interception should only have taken place within these periods.

The CTIVD concludes that both services requested separate authorisations. This resulted in the situation that the first authorisation period (from 2019 to 2020) for both services did not run parallel, with a difference of several days. Moreover, the services were only allowed to intercept channels for which authorisation had been granted.

Findings

The CTIVD's technical investigation revealed that only channels that were classified as Category 1 were intercepted. For the vast majority of the interception period, the services also complied with the commitment that channels could be intercepted for a maximum of two hours per day per channel. For a limited number of days, the services carried out tests in the interception chain where data were intercepted for longer than two hours per day per channel. Most of these data were stored in the services' systems and were available for snapshot investigations. In addition, the CTIVD concludes that during the first authorisation period, the authorisation period for the MIVD was a few days longer than that of the AIVD. Interception took place during these days. However, because of the lack of conclusive logging and sufficient recording, it is no longer possible for the services to trace which channels were intercepted and whether account was taken of the fact that the AIVD's request for authorisation had ended at that point. For the second authorisation period, the services terminated the interception in time.

Assessment

The CTIVD concludes that the services acted in accordance with the authorisations as far as the intercepted channels are concerned. This is also true for most of the interception period for the commitment that channels could be intercepted for a maximum of two hours per day per channel. The tests that took place and involved intercepting data for more than two hours were necessary, partly in view of the obligations arising from the duty of care. What is essential here, however, is that excess intercepted data are destroyed immediately after the test and that these data are not further stored and used for (technical) investigations. However, the data were not destroyed immediately after the test, so these data were stored and used in the investigation. Finally, the CTIVD concludes that for the short period during which data were intercepted without authorisation for the AIVD and authorisation had been granted for MIVD investigation assignments only, it is impossible for the services and for the CTIVD to trace which channels were intercepted. So it cannot be ruled out that channels were intercepted that can be related to investigation assignments and to the AIVD's request for authorisation, for which there was therefore no ongoing authorisation. With regard to the second period during which cable interception for snapshot purposes took place, the services complied with the statutory authorisation periods.

6.3.2 Division of roles and tasks

In this section, the CTIVD examines how the services implemented the requirement of division of roles and tasks. This means that only certain employees are authorised to know the content of certain data and are assigned specific tasks that do not apply to others. To gain access to interception data, the relevant employee must first hold a position designated in the services' designation decision to perform tasks under Section 48 or Section 49(1). Second, the employee must also actually have a duty and perform work under Section 48 or Section 49(1). After all, employees that hold a certain position may perform different tasks.

Findings

Within the services, a team of designated officials was responsible for the analysis of the intercepted data. The investigation carried out by this team focused mainly on assessing the potential intelligence value of the intercepted data, meaning that this team investigated the nature of the data traffic on the various channels and the data types they contained. They were looking for data types that intelligence teams had indicated they needed in their investigations. They also tried to identify which channels contained the greatest amount of these data types and whether they could be related to the areas of attention and investigation assignments. Occasionally, they combined data to show that intelligence teams could do the same later in the 'production phase'. This was not done in order to obtain intelligence, but to investigate and demonstrate the possibilities of cable interception.

Other tasks of this team included carrying out technical analyses in the context of optimising the interception chain and verifying that the intercepted data were properly processed by the systems set up for this purpose. In addition, this team provided proposals for developing parsers. Parsers are software rules that allow intercepted data to be stored and further processed in the services' systems. Finally, the team was tasked with developing investigation methods for cable interception so that it could eventually be applied by intelligence teams.

Besides this team, other functions also obtained authorisation for the interception data. There are authorisation groups within the services that have access to all data sources, which means that these function groups also have access to the snapshot data. Not all staff members in this function group were given tasks in the cable interception process.

Assessment

In practice, the services designated persons authorised to investigate snapshot data under Sections 48(1) and 49(1), or a combination thereof. This means that these individuals could be authorised to access these data.

The authorisation of and the manner in which the investigation was conducted by the relevant team are within the framework of the ISS Act 2017. For the purpose of conducting this investigation, the staff members of this team were designated as officials who were allowed to perform work in the context of Section 48 as well as Section 49(1). In the CTIVD's view, this mixing is also in line with the ISS Act 2017, insofar as the starting point remains that these officials are appointed to the exclusion of others to be allowed to examine the content of communications and that access to these data is necessary for the performance of their function and/or task.

With regard to the services' staff members with broad access to all data sources, the CTIVD is of the opinion that these staff members should not have been authorised. Not all staff members within this function group had a role in this process.

6.3.3 Specificity

During the investigation period, the specificity requirement was initially laid down in a policy rule.[50] Halfway through 2021, this requirement became part of the ISS Act 2017 through a legislative amendment.

50 *Parliamentary Papers II* 2017/18, 34588, no. 76.

From the entry into force of the ISS Act 2017, the CTIVD followed the TIB's interpretation of the specificity criterion, namely: "the extent to which the acquisition involves minimising data not strictly necessary for the investigation, given the technical and operational circumstances of the case.[51] The explanatory memorandum to the aforementioned act amending the ISS Act 2017 was published in July 2019, also adhering to this definition and containing a further explanation of the different weighting factors of the specificity criterion[52]. The memorandum lists the following factors that may affect the specificity of the use of a power:

- The intelligence context, e.g. the nature of the threat being investigated;
- The stage of an investigation;
- The possibility of falsification;
- The time element, e.g. whether there is an acute threat;
- Limitations in technology;
- Financial aspects.

In addition, the memorandum argues 'that the added value of applying the specificity criterion depends on the type of power deployed'. In the CTIVD's opinion, an explanation of the specificity criterion therefore involves more than just limiting the amount of data to be collected. The addition of the word 'possible' leaves room for an interpretation of specificity that does justice to the nature of the relevant power. For example, the interpretation of specificity in cable interception is never the same as the interpretation of specificity when installing a telephone tap at a target.

The CTIVD already addressed the interpretation of specificity in this form of interception in its review report on the application of filters in investigation-related interception (of satellite and radio communications).[53] The interpretation of specificity is expressed in different phases of the interception process: (1) the choice of the communication bearer, (2) the choice of data stream and (3) the filtering of the intercepted data. This general principle also applies to cable interception. It is important to note that the specificity of cable interception cannot be assessed only for each stage of the interception process. Specificity should therefore be considered over the entire process of cable interception, including the stages of storage and processing of the intercepted data. What is important in assessing the specificity of the use of cable interception during the investigation period is that it involved snapshotting and that the services included the safeguard that the data were not to be used for the intelligence process.

Findings

For the interpretation of the specificity of cable interception, it is important to state first and foremost that it is (virtually) impossible to deploy this power in a manner that is just as targeted as other powers, such as a tap or a hack. It is inherent in the nature of the power that large amounts of data are intercepted that, while relating to an investigation assignment (and therefore being 'investigation-related'), most of these data still relate to individuals and/or organisations that are not the subject of investigation by the services.[54] The untargeted nature of cable interception lies not only in the nature of the cable interception power, but also relates to the intelligence context in which it is deployed.

51 TIB Annual Report 2018-2019, available at tib-ivd.nl.
52 *Parliamentary Papers II* 2018/19, 35242, no. 3
53 Appendix A to CTIVD review report no. 63 on the application of filters in investigation-related interception by the AIVD and the MIVD, *Parliamentary Papers II* 2018/19, 29924, no. 188 (appendix) (Sept. 2019), p. 7.
54 See also Chapter 9 in this report.

During the investigation period, cable interception was deployed for investigation assignments focused on foreign countries and thus on intercepting communication that originates and/or terminates in those foreign countries.[55,56] Moreover, the Ministers of the Interior and Kingdom Relations and of Defence pledged that 'there was virtually no prospect of cable interception being used in the coming years to investigate communications that originate and terminate in the Netherlands'.[57] This pledge was also part of the services' requests for authorisation. The services chose to create an access location at a provider through which high volumes and a variety of mainly international data traffic are sent (the aforementioned 'four-lane motorway').

Based on the information obtained, the services then prepared the aforementioned classification of categories of channels to be intercepted (see section 6.2). This classification was included in the authorisation requests submitted in 2019 and covered three categories:

- Category 1 included channels with expected high intelligence value for the investigation assignments;
- Category 2 included channels of unknown intelligence value for the investigation assignments; and
- Category 3 included channels with an expected low or absent intelligence value for the investigation assignments.

The channels classified in the three categories covered part of the total number of channels on the cable routes. The services requested authorisation to intercept channels in categories 1 and 2. Ultimately, only the authorisation to intercept data on channels in category 1 was assessed as lawful by the TIB. This ruled out intercepting data on channels in category 2 (and category 3). According to the TIB, these channels could not be related to the investigation assignments beforehand. The services performed snapshotting on the category 1 channels.

There was no positive filtering during the snapshotting. This made the deployment of cable interception wider in an initial (exploratory) phase. As a result, a lot of data were intercepted that may not be related to the services' investigation assignments. During the investigation period, the services applied the safeguard that data were destroyed after one year. Moreover, the data were to be (technically) examined only by designated officials and were not to be used in the intelligence process.

Assessment

In view of the above, the CTIVD concludes that, during the investigation period, the deployment of the cable interception power through snapshotting was an interpretation of a deployment that was 'as targeted as possible'.

The access location chosen lends itself to interception for the purpose of a wide range of the services' investigation assignments. The same applies to the cable routes chosen at the access location. In practice, the services requested and obtained authorisation to intercept data on cable routes that were expected to handle traffic to and from the two areas of attention from the investigation assignments. Given the intelligence context, it is therefore, in the CTIVD's opinion, understandable that the services chose to create an access location at a provider through which high volumes and a variety of mainly international data traffic are sent (the aforementioned 'four-lane motorway'). Financial aspects are another element in fulfilling the specificity criterion, especially when operationalising an access location, as this involves high costs.

55 An exception to this pledge has been made for the investigation of cyber defence.
56 ECHR 25 May 2021, nos. 58170/13, 62322/14 and 24960/15, ECLI:CE:ECHR:2021:0525JUD005817013 (Big Brother Watch et al. v. the United Kingdom).
57 *Parliamentary Papers II* 2017/18, 34588, no. 76.

According to the legislature, the services may be required to spend the financial resources available in an efficient manner.[58] This makes the initial operationalisation of a single access location handling a wide variety of communications highly arguable, compared to the alternative of an access location that lends itself to a (more) limited number of investigation assignments.

An important additional criterion for assessing the specificity of cable interception during the investigation period is the phase of the investigation. When it comes to choosing the data streams to be intercepted, it was explained in the parliamentary discussion of the bill that this choice can be made at channel level. For this reason, the services distinguished between the channels and categorised them. The TIB assessed that the services had substantiated only for category 1 channels that they could be related to the investigation assignments. Up to a certain extent, the services could gain knowledge of the cable landscape from the preliminary investigation carried out by them, including the information they had obtained from the provider based on the duty to provide information under Section 52. However, this knowledge was limited and included the name of a party handling traffic on a specific channel. The services had no concrete knowledge of the communications actually transported over the cable routes chosen. The analysis that the services eventually carried out with respect to the intercepted data shows that the prior knowledge does not always match the communication actually handled on a given channel. It cannot therefore be ruled out that category 2 channels also had potential intelligence value for the investigation assignments, as these channels were on routes that could be related to the investigation assignments. In addition, during the investigation period, the services had set up sufficient safeguards to protect the data (the contents of which were not necessary for the investigation), such as excluding data for processing by intelligence teams and a limited retention period.

The CTIVD therefore considers that the services complied with the requirement to deploy cable interception in the most targeted way possible. However, the question to be asked is whether, given how the internet works, channel-based substantiation is the most effective way to fulfil the specificity requirement. This question is elaborated on in Chapter 9.

6.3.4 Communication that originates and terminates in the Netherlands

Following commitments by the Ministers of the Interior and Kingdom Relations and of Defence, the applications for authorisation included the safeguard that 'there was virtually no prospect of cable interception being used in the coming years to investigate communications that originate and terminate in the Netherlands (with the exception of cyber defence)'. This commitment was made in response to the outcome of the advisory referendum on the ISS Act 2017.[59] As the CTIVD describes in Appendix I of this review report, the precise scope and meaning of the commitment by the Ministers is not unambiguous. This will be discussed in greater detail in Chapter 9.

Findings

The CTIVD's investigation shows that during the investigation period, the services did not use cable interception for investigation assignments (other than cyber defence) targeting the Netherlands. However, this does not mean that no communication that originates and terminates in the Netherlands was intercepted at all. For this cannot be avoided, given the routing of cable communications. Cable communications are transported via the cheapest and/or fastest route. This does not rule out the fact that communications that originate and terminate in the Netherlands are also transported via international cable routes.

58 *Parliamentary Papers II* 2018/19, 35242, no. 3.
59 *Parliamentary Papers II* 2017/18, 34588, no 76, p. 3.

In addition, these communications were allowed to be intercepted for cyber defence purposes, which is an additional reason why the commitment cannot pertain to interception as such. The services' expectation was that domestic traffic would make up a very limited proportion of the intercepted data, given the fact that they intercept cable routes through which almost exclusively international data traffic is sent.

Apart from mentioning it in the authorisation requests, the services did not give any further substance to the commitment. This means, for example, that they did not apply negative filters to filter out communications originating and terminating in the Netherlands. As a result, to the extent these communications were present on the relevant channels, they were intercepted and stored.

The services subjected these data to technical investigations. As explained in more detail in section 6.3.2, the services' investigation during the investigation period was limited to analysing the potential intelligence value of the intercepted data. Within that investigation, they tried to do counts to determine the volume of communications originating and terminating in the Netherlands as intercepted by them. They also investigated how the Ministers' commitment could be implemented in a technical sense. This investigation was to provide insights into how the services should handle domestic communications once they are authorised to proceed to 'production'.[60]

Assessment

The exact scope of the Ministers' commitment is not unambiguous. The CTIVD concludes that the focus of this commitment is to exclude intercepted data originating and terminating in the Netherlands from *investigation* and not from *interception*. This also follows from the fact that it is allowed to intercept domestic traffic for cyber defence purposes. During the investigation period, interception was limited to snapshotting, with the services applying the safeguard that intercepted data would not be used by intelligence teams for investigation purposes. The investigation in which intercepted data were used was limited to a technical investigation and focused on determining potential intelligence value and identifying possible future filters. Nevertheless, in the 'production phase', when data can be used by intelligence teams, the services should apply adequate safeguards. For the commitment is part of the legal framework for cable interception.

6.3.5 Data reduction and relevance

In this section, the CTIVD examines compliance with three safeguards regarding data processing after interception. Firstly, compliance with the obligation to destroy half of the metadata generated within three months and, secondly, compliance with the maximum retention period of one year for intercepted data (except for data declared relevant). Finally, it examines how the services dealt with declaring data relevant and whether they did so only in highly exceptional cases.

Findings regarding data reduction

The services reduce data using automated processes that implement data destruction. Samples from the CTIVD's IT Unit confirmed the correct functioning of these processes.

60 'Production' means that they no longer just take snapshots, but actually analyse and exploit the intercepted data from an intelligence point of view.

Assessment

The services fulfilled the obligation to destroy half of the metadata generated within three months. They also retained the snapshot data for a maximum of one year and destroyed it in a timely manner.

Findings regarding relevance

'Declaring data relevant' is an act that is performed on data obtained with the use of investigatory powers.[61] Data may be relevant to the investigation in the context in which they were obtained, or in the context of any other investigation by the relevant service. Once data are determined to be relevant in this way, they can be retained and further processed, including for other investigations.[62] The data are labelled 'relevant' in the systems. This does not mean that the data can then be accessed and used by all service staff. Staff members should also have specific authorisations for the data in order to access them.

Service staff assigned to investigate the intercepted data during the investigation period indicated that they did not declare any (raw) data relevant. The relevant staff members kept notes of the results of their investigations under Section 49(3). Declaring the underlying data relevant and thereby retaining them was not deemed necessary. However, samples of data were kept for knowledge sharing on an internal environment that could only be accessed by these staff members.

The services made the choice to treat the intercepted (snapshot) data according to the usual processing system, which they also use, for example, for data from hacks and taps and based on other powers. This processing system of the services automatically labels all incoming data. The label indicates, for example, the power based on which the data were obtained, but also whether data have been assessed as relevant. Another part of the processing system is that data are automatically (implicitly) declared relevant based on certain (technical) characteristics. Declaring data implicitly relevant means that the stored data are automatically compared with certain characteristics. If stored data match these characteristics, the data are labelled as relevant.[63] This process is also applied to snapshot data. As a result, data were labelled as relevant in the systems. However, due to the technical set-up of the systems, this labelling did not affect the retention period of the intercepted data. The services had made technical arrangements to ensure a hard retention period of one year for the intercepted data. After this year, the data were automatically destroyed. Nor has there been any change in the authorisations to this data, which means that the labelling did not result in the interception data being accessed by the intelligence process. In short, therefore, this merely involves a technical label that, as far as the CTIVD has been able to establish, did not affect the data themselves.

Assessment

In the CTIVD's view, the services acted in line with the commitment made. Data were not (explicitly) assessed as relevant by service staff. Although the data were labelled as relevant, this labelling had no consequences for the process of automatically declaring the data relevant. The data were not kept for more than a year, nor did the data become widely available. Nor has there been any change in the authorisations to these data.

61 As laid down in Section 27 and Section 48(5).
62 *Parliamentary papers II* 2016/17, 34588, no. 3, p. 42.
63 A more detailed explanation of the process of automatically (implicitly) declaring data relevant can be found in Progress Report III on the operation of the ISS Act 2017, *Parliamentary Papers II* 2019/20, 34 588, no. 85 (appendix) (Dec. 2019), p. 11.

Therefore, the choice to process the snapshot data through the usual system in this case did not affect further data processing. However, this procedure does entail an increased risk of unlawful conduct and therefore requires enhanced internal control.

6.3.6 Shielding data from intelligence teams

The safeguard that the data intercepted during the snapshot phase were not made available to intelligence teams is key. After all, snapshotting involves the collection of large amounts of obviously irrelevant data, related to individuals and/or organisations the services do not focus on. This safeguard therefore prevents a situation in which the intercepted data are further processed and can be processed, for example, in an intelligence team's analysis. This is consistent with the purpose for which the interception may be used, namely to investigate the potential intelligence value of the intercepted data. The CTIVD notes that service staff were very aware of this safeguard and that the services made efforts to technically embed it in their systems.

Findings

The CTIVD conducted a technical investigation into the automated logging of search requests made by service employees on the intercepted data.[64] The services generate this logging with information security in mind, not compliance. As such, logging is not designed to answer the question of the extent to which data have been processed lawfully. However, the CTIVD was still able to use the logging for its investigation. This investigation focused, among other things, on whether snapshot data were properly shielded from intelligence teams. This investigation found that a very limited portion of the intercepted data was accessible to intelligence teams during the investigation period. This was not a conscious decision by the services, but was caused by a technical error. The services found out about this too late due to a lack of adequate internal controls. A more detailed explanation of this technical error is given below.

As described earlier, the services made the choice to handle the intercepted (snapshot) data according to the usual processing system. This processing system of the services automatically labels all incoming data. Due to an error in the code of the labelling system, the snapshot data had not been labelled as such. As a result, if data in the snapshot data matched certain characteristics, they became available to all intelligence teams. The fact that the data were available did not mean that the data were actually accessed by the teams. However, the CTIVD's technical investigation revealed that search requests on the snapshot data had been made by staff members not originally authorised to do so, such as staff members of intelligence teams.

The CTIVD discussed these findings with the services. This revealed that the services had previously known about the release of the data to intelligence teams, but failed to report it to the CTIVD. The reason for this was that after the services had found the error, they investigated the consequences of this incident. In doing so, they examined whether the data had been accessed by intelligence teams and concluded at the time that the data had been accessed only by persons designated to do so. The incident was therefore qualified as a 'low impact' incident at the time and was not reported to the CTIVD.[65]

64 For a description of the technical investigation, see Appendix II of this report.
65 The services failed to proactively report the error in the code during the CTIVD's investigation.

Following questions from the CTIVD, the services conducted a follow-up investigation into the identified search requests on the released data. This showed that the services had drawn an incorrect conclusion in their original investigation into the incident. This conclusion was based on a dashboard that had been fed with incomplete data, unlike the data the CTIVD had requested from the services for the purpose of its technical investigation. The investigation also found that the automated process that was supposed to detect such incidents did not work because it was not configured to check for snapshot data.

Following this finding, the services conducted another investigation, this time mainly into the extent to which snapshot data had been used by teams in intelligence products. The CTIVD concludes that it is not possible for the services to fully trace whether and in what way the data were visible to staff members in the intelligence process. Following the services' investigation and the CTIVD's investigation, technical changes have been implemented to prevent data from being accessed by the intelligence teams in the future.

Assessment

Because snapshot data were available to intelligence staff members and were also accessed by those staff members, the services violated a safeguard included in the authorisation requests that were assessed as lawful. The fact that the data were accessed by staff members of intelligence teams did not lead to further exploitation (use in intelligence products) of these data, according to the investigation conducted by the services. However, this cannot be completely ruled out by the services and the CTIVD.

6.3.7 Negative filtering of streaming and bittorrent traffic

Part of the cable interception authorisation requests included a requirement that the services do not store streaming and bittorrent traffic (i.e. that they use negative filtering). At some point during the investigation, the services informed the CTIVD of an incident regarding the application of these negative filters during the investigation period. This incident can be divided into two separate events with different causes.

Findings

The first event resulted from the use of certain equipment that served (among other things) to apply negative filters. This equipment did not function properly, which meant that the use of negative filters also did not function properly for several months during the investigation period. The services then investigated the matter. This investigation showed that traffic with characteristics included in the negative filter and pertaining to streaming services and bittorrent traffic, still passed through and was stored.

The second event occurred after the non-functioning equipment was replaced by the services with new equipment. This new equipment had to be set up by the services themselves. These settings were configured by a technical staff member. This configuring was based on an incorrect assumption regarding the ISS Act 2017 and the safeguards included in the authorisation requests. The assumption was that, in the context of snapshotting, no negative filtering needed to be applied to intercepted traffic as a whole. However, this assumption was inconsistent with the requirement included in the authorisation requests to apply negative filers. As a result, no negative filters were applied to the intercepted data for several months.

Assessment

By failing to apply negative filters to traffic from streaming services and bittorrent traffic, the services violated a safeguard contained in the authorisation requests that were assessed as lawful. In the CTIVD's view, however, the infringement on fundamental rights of citizens was limited as the data were subject to a limited retention period and had been shielded from intelligence teams. The latter does not apply to the data that were accessible to intelligence teams (see section 6.3.6). The CTIVD did not investigate the extent to which these data related to traffic from streaming services or bittorrent traffic.

As described in Chapter 4, the (technical) settings of the equipment were not sufficiently considered from a multidisciplinary perspective. In addition, there were no internal controls. The proper functioning and settings were not checked before the equipment was put into production. After the equipment was put into production, the correct functioning of the equipment was not periodically checked. The CTIVD considers it important to note that the technical staff member who configured the filters cannot be held responsible for this, but it was due to there being no control system capable of detecting this kind of human errors.

6.3.8 Sharing data with partner services

The services did not share snapshot data with foreign services during the investigation period. The requirement that the data obtained from snapshotting are not shared with foreign services is therefore met.

6.3.9 Analysis techniques

The services were only allowed to apply certain analysis techniques (defined to the TIB) to the intercepted data. They did not apply any analytical techniques other than those described. This means that the requirement that only certain analysis techniques (defined to the TIB) are applied to the intercepted data has been met.

6.4 Interim conclusion

This chapter describes the findings that address the second part of the investigative question. Regarding the question of whether the services lawfully implemented cable interception for snapshot purposes during the investigation period, the CTIVD concludes that:

- The services intercepted channels that had been authorised and adhered to the agreed duration of no more than two hours per day per channel for the vast majority of the interception period. Moreover, with regard to the second period during which interception for snapshot purposes took place, they complied with the statutory authorisation periods (section 6.3.1). With regard to the specificity requirement, the CTIVD finds that, during the investigation period, the deployment of the cable interception power through snapshotting was an interpretation of a deployment that was 'as targeted as possible'. The explanation of the act has identified several factors that may affect the specificity of the use of a power. In the CTIVD's opinion, an explanation of the specificity criterion involves more than just limiting the amount of data to be collected. The addition of the word 'possible' leaves room for an interpretation of specificity that does justice to the nature of the relevant power (section 6.3.3).

The services also acted in accordance with the commitment that traffic originating and terminating in the Netherlands would not be investigated, except for cyber defence (section 6.3.4). Finally, they acted lawfully with regard to data reduction and explicit relevance (section 6.3.5), not sharing data with foreign services (section 6.3.8) and applying analysis techniques (section 6.3.9). This is therefore lawful.

- The services have not sufficiently implemented the required division of roles and tasks under Sections 48 and 49 (section 6.3.2). Moreover, data were made available to intelligence teams and data have actually been accessed by service staff in intelligence teams (section 6.3.6). In addition, no negative filtering was applied (in a sufficiently conclusive manner) (section 6.3.7) and the data collected during the testing of the systems where communications were intercepted for more than two hours per day per channel should have been destroyed. Finally, for the AIVD, for a short period of time, it cannot be ruled out that communications were intercepted without authorisation (section 6.3.1). The services acted unlawfully in these respects.

As also described in Chapter 2, intercepting and storing communications infringes on citizens' fundamental rights. According to the ECHR, this infringement increases as the data are drawn further into the processing process of the intelligence and/or security services. As explained in Chapter 2, the ECHR defines four stages of cable interception. Stage 1 involves collecting and storing the communications, stage 2 involves searching the data using selectors and search queries, state 3 involves examining the data selected and stage 4 involves using the data in intelligence products.

During the investigation period, communications were intercepted (collected) and stored by the services (phase 1). The data were also searched and examined (stages 2 and 3), but this was done almost exclusively from a technical perspective with the aim of assessing the potential intelligence value of the intercepted data.[66] The data were not used in intelligence products (stage 4).[67] The services complied with the retention periods and data were destroyed after one year. Finally, only channels for which authorisation was granted were intercepted and no data were shared with foreign intelligence and security services. These findings lead to the conclusion that fundamental rights of citizens were infringed upon, but that this infringement was limited.

6.5 Recommendations

The findings identified in this chapter stem from the fact that the services inadequately fulfilled their duty of care, as described in Chapter 4. The recommendations in Chapter 4 regarding the duty of care therefore apply in full. In addition, the CTIVD recommends:

- to set up the authorisation process in such a way that the focus is on assessing whether the task of the relevant staff member makes it necessary to access investigation-related interception data.

66 Stages 2 and 3 as described in case law refer to searching and examining the data from an intelligence perspective. The selectors that are subsequently used can then be related to specific organisations and individuals, for example.

67 It should be noted here that data may perhaps have been accessed by staff in the intelligence process given the findings in section 6.3.7. However, according to the investigation conducted by the services, these data were not used in intelligence products. This cannot be completely ruled out by the services and the CTIVD.

7. Conclusions

In this report, the CTIVD investigated whether, in the period from 1 May 2018 to 31 March 2021, the AIVD and the MIVD lawfully operationalised an access location and lawfully exercised cable interception in the snapshot phase. This chapter discusses the conclusions on this investigative question. First, a brief description is given of how cable interception was deployed during the investigation period. It then describes the context in which the services have operationalised cable interception. This context also serves as a background for the conclusions of this investigation, which are discussed successively. It concludes with a description of the services' improvement plans.

Cable interception in the investigation period

During the investigation period, the services operationalised one access location at a communication service provider. The duty to provide information (Section 52) was used in order to operationalise the access location. The services used this power to collect information from the provider about its infrastructure. The services also used the duty to cooperate (Section 53). This duty requires the provider to cooperate in making its infrastructure (the cables) suitable for interception. In addition, the services used specific special investigatory powers to operationalise the access location.

During the investigation period, the services used the cable interception power (Section 48) and the power of search aimed at interception (Section 49(1)). The deployment of cable interception must be authorised by the Ministers. The TIB then assesses the lawfulness of this authorisation. The first requests for authorisation pertained to intercepting all available channels on certain cable routes at the access location. Here, it was foreseen that the services could determine the intelligence value of these channels at their discretion to assess which channels would be put 'into production'. This was found to be unlawful by the TIB. During the process of requesting authorisation and the TIB's final lawfulness assessment, various restrictions and safeguards were added to the requests for authorisation that limited the final implementation of cable interception. During the investigation period, cable interception was deployed in a limited form, namely 'snapshotting'. Through snapshotting, the services intercepted the cable for a limited duration for (technical) investigation purposes, aimed to determine the potential intelligence value of the intercepted channels. Unlike with regular cable interception, the use of the intercepted data for intelligence investigations was ruled out here. In addition, the services were limited to intercepting certain channels on the cable routes that they could access at the access location. As a result of the lawfulness decision made by the TIB, the services could only intercept channels that they expected in advance to have high intelligence value. In response to queries from the TIB, the services had divided the available channels into three categories, depending on the expected intelligence value (with category 1 for those channels with expected high intelligence value). In the first quarter of 2019, the TIB ruled that the authorisations had been lawfully granted, but only made this decision for channels classified in category 1. By making the requests for authorisation, the services had also intended to intercept channels of unknown intelligence value for the purpose of snapshotting. The TIB did not grant authorisation to do so. A limited retention period was one of the other important safeguards included in the requests for authorisation that were assessed as lawful. The services were allowed to keep the data obtained through snapshotting for a maximum of one year.

Complexity

In operationalising cable interception, the services have had to act as technical and legal pioneers in a complex environment. The services were technical pioneers because while they had experience with intercepting satellite and radio communications, this experience could not be applied automatically to cable interception. This meant that the services had to start from scratch when developing many systems, processes and procedures. In addition, operationalising an access location, building an interception chain and implementing legal and other safeguards is a technically complex process. The services were also legal pioneers, as the legal powers to operationalise an access location and intercept communications had not previously been used for cable interception. The services, but also the TIB, had to flesh out the requirements set by the ISS Act 2017 on a lawful implementation of cable interception. This includes the requirement that cable interception, a power that involves a high degree of inherent untargeted data collection, should be used in a manner that is 'as targeted as possible'. In addition, the interpretation given to cable interception in the parliamentary debate on the ISS Act 2017 had to be taken into account. The CTIVD concludes that the interplay of technical complexity, a legally complex framework and the desire to realise cable interception in the short term has created an area of tension in which the duty of care has become secondary. In practice, this area of tension has affected the operationalisation of the access location and the implementation of cable interception.

Investigative question

This review report answers the following investigative question:

In the period from 1 May 2018 to 31 March 2021, did the AIVD and the MIVD lawfully operationalise an access location and lawfully exercise cable interception in the snapshot phase?

The CTIVD has not investigated the substantiation of the requests for authorisation, as their lawfulness has already been assessed by the TIB. This means that the CTIVD has not re-assessed the requirements of necessity, proportionality and subsidiarity. However, the same does not apply to the specificity requirement. The CTIVD has included this in its assessment because the Ministers of the Interior and Kingdom Relations and of Defence explicitly asked it to report on this.[68]

Duty of care

In this review report, the CTIVD concludes that the services inadequately fulfilled their statutory duty of care during the investigation period. This is a fundamental problem underlying many of the findings in this review report. While this was not caused by the complexity outlined above, it does serve as a context for the findings regarding the duty of care.

The duty of care is laid down in Section 24 of the ISS Act 2017. This duty means that the heads of the AIVD and the MIVD are responsible for applying technical, staffing and organisational measures to ensure data are processed lawfully. Among other things, the duty of care entails that both services must continually be in control of the way in which they process data and ensure that data processing is and continues to be in line with the applicable legal regulations (compliance). The duty of care explicitly requires more from the heads of the AIVD and the MIVD than just the introduction of the duties that the law imposes on them when collecting and analysing data and when they are actually being used by staff members of the services, among other things.[69]

68 Letter to the President of the Senate dated 6 April 2018, *Parliamentary papers I* 2017/18, 34588, G.
69 CTIVD no. 59, Progress report on the operation of the ISS Act 2017, *Parliamentary Papers II* 2018/19, 34 588, no. 80 (appendix) (Dec. 2018), p. 7.

Cable interception is a far-reaching power. Moreover, in actual practice there is such technical and legal complexities that risks of unlawful conduct were and are high. This requires that aspects of the duty of care be explicitly incorporated into the operationalisation and interception process from the outset. The CTIVD concludes, however, that the heads of the services inadequately fulfilled their statutory duty of care during the investigation period. In practice, insufficient internal control was exercised over the cable interception process. At several points during the investigation period, legal safeguards were translated into technical implementations. Such technical implementations should be checked before they are put into production. Moreover, structural checks should be performed during the data processing process to ensure a correct operation of the technical systems. These checks were insufficient, leading to the occurrence or late detection of unlawful conduct.

However, this does not mean that the services did not pay any attention to fulfilling the duty of care. In the context of the duty of care, the services conducted a broad inventory of lawfulness risks at an advanced stage of the investigation period. This included cable interception. This inventory resulted in a risk register. In addition, in 2020 the AIVD conducted two internal audits specifically aimed at identifying risks of unlawful conduct in relation to its own policies and to the control measures for investigation-related interception. Both audits, completed in March and October 2020, identified high and medium risks. As the CTIVD already concluded in its fourth and concluding progress report, measures such as conducting an audit can be seen as positive, but continuing attention should be paid to the translation into practice.

Answer to the investigative question

With regard to the first part of the investigative question, which pertains to the lawfulness of operationalising an access location, the CTIVD concludes that:

- The services received information on a structural basis from the provider in the context of realising the access location. In the CTIVD's assessment, the services only requested data covered by the Data Provision (Investigation of Communications under the ISS Act 2017) Decree. In doing so, they did not depart from the categories of data specified therein. The vast majority of the information received during the investigation period also had a legal basis, either under the duty to provide information (Section 52) or the duty to cooperate (Section 53). Frequent consultations were held with the provider prior to (and during) the operationalisation of the access location (section 5.2.1). At the time of the technical operationalisation of the access location, there was a valid authorisation under Section 53 (section 5.2.2). The services acted lawfully in these respects.

- After the expiry of the authorisations for cable interception (Section 48) and for the use of the duty to cooperate (Section 53), the services instructed the communication service provider to operationalise new cable routes, while no new authorisation to intercept these routes had been obtained yet. Such work cannot be performed on a voluntary basis, nor is it covered by keeping the installed facility in place as described in Section 53(6) (section 5.2.2). Moreover, the services received information from the provider for short periods without a legal basis (section 5.2.1). Finally, apart from the use of the duty to provide information and to cooperate, the services used other special powers for the purpose of operationalising the access location. No valid authorisation had been granted for these powers (section 5.2.2). The services acted unlawfully in these respects.

With regard to the second part of the investigative question whether the services lawfully implemented cable interception for the purpose of snapshotting during the investigation period, the CTIVD concludes that:

- The services intercepted channels that had been authorised and adhered to the agreed duration of no more than two hours per day per channel for the vast majority of the interception period. Moreover, with regard to the second period during which interception for snapshot purposes took place, they complied with the statutory authorisation periods (section 6.3.1). With regard to the specificity requirement, the CTIVD finds that, during the investigation period, deployment of the cable interception power through snapshotting was an interpretation of a deployment that was 'as targeted as possible'. The explanation of the act has identified several factors that may affect the specificity of the use of a power. In the CTIVD's opinion, an explanation of the specificity criterion involves more than just limiting the amount of data to be collected. The addition of the word 'possible' leaves room for an interpretation of specificity that does justice to the nature of the relevant power (section 6.3.3). The services also acted in accordance with the commitment that traffic originating and terminating in the Netherlands would not be investigated, except for cyber defence (section 6.3.4). Finally, they acted lawfully with regard to data reduction and explicit relevance (section 6.3.5), not sharing data with foreign services (section 6.3.8) and applying analysis techniques (section 6.3.9). This is therefore lawful.

- The services have not sufficiently implemented the required division of roles and tasks under Sections 48 and 49 (section 6.3.2). Moreover, data were made available to intelligence teams and data have actually been accessed by service staff in intelligence teams (section 6.3.6). In addition, no negative filtering was applied (in a sufficiently conclusive manner) (section 6.3.7) and the data collected during the testing of the systems where communications were intercepted for more than two hours per day per channel should have been destroyed. Finally, for the AIVD, for a short period of time, it cannot be ruled out that communications were intercepted without authorisation (section 6.3.1). The services acted unlawfully in these respects.

Degree of infringement of citizens' fundamental rights

As also described in Chapter 2, intercepting and storing communications infringes on citizens' fundamental rights. According to the ECHR, this infringement increases as the data are drawn further into the processing process of the intelligence and/or security services. The ECHR defines four stages of cable interception. Stage 1 involves collecting and storing the communications, stage 2 involves searching the data using selectors and search queries, state 3 involves examining the data selected and stage 4 involves using the data in intelligence products.

During the investigation period, communications were intercepted (collected) and stored by the services (phase 1). The data were also searched and examined (stages 2 and 3), but this was done almost exclusively from a technical perspective with the aim of assessing the potential intelligence value of the intercepted data.[70] The data were not used in intelligence products (stage 4).[71] The services complied with the retention periods and data were destroyed after one year.

70 Stages 2 and 3 as described in case law refer to searching and examining the data from an intelligence perspective. The selectors that are subsequently used can then be related to specific organisations and individuals, for example.

71 It should be noted here that data may perhaps have been accessed by staff in the intelligence process given the findings in section 6.3.7. However, according to the investigation conducted by the services, these data were not used in intelligence products. This cannot be completely ruled out by the services and the CTIVD.

Finally, only channels for which authorisation was granted were intercepted and no data were shared with foreign intelligence and security services. These findings lead to the conclusion that fundamental rights of citizens were infringed upon, but that this infringement was limited.

Improvement plan

The implementation of the duty of care took place in parallel with the implementation of cable interception, but did not sufficiently result in measures in practice. At the end of August 2021, the CTIVD shared the findings of its investigation with both heads of service in light of their specific responsibilities for the statutory duty of care. Following these consultations, the services drew up an improvement plan, which aims to strengthen service-wide internal control of data acquisition and processing. The CTIVD endorses the measures contained therein and stresses that achieving actual effects in the services' implementation practice should be the highest priority throughout the organisation. Final responsibility for the entire chain of acquisition and processing of investigation-related interception data should therefore be vested at a level with sufficient overriding authority within the organisations of both services. On the one hand so as to ensure centralised overview, and on the other so as to ensure a timely and effective implementation of measures. In addition, compliance should not be a primary staff responsibility, but a line responsibility. It is an ongoing process, which the services should proactively implement across their organisations. Finally, internal control and supporting tools should also enable effective external oversight.

In addition to the improvement plan, the intention is for cable interception for intelligence purposes, known as the production phase, to be implemented in phases. The services described that the technical chain will be tested first. Only if these tests are successful will storage of the data for intelligence teams begin.

Increased oversight

Whether the services are ready for the 'production phase' is a question the services themselves have to answer. The CTIVD will increase its oversight and report on this further. This includes reviewing the phased implementation of cable interception, as described in the services' improvement plan.

8. Recommendations

In this report, the CTIVD has made several recommendations that relate to the operationalisation phase of the access location and those relating to the implementation of cable interception. The recommendations are listed below. The CTIVD recommends the AIVD and the MIVD:

1. To vest the final responsibility for the entire investigation-related interception chain centrally and at a sufficiently high level with overriding authority within the organisations of both services (Chapter 4).

2. To fulfil the statutory duty of care by at least:
   - setting up appropriate tools for compliance purposes, which includes putting logging in place. Both internal stakeholders and the CTIVD should be involved here. These tools should also be suitable for effective external oversight. Logging should be in place before starting the production phase of cable interception (Chapter 4);
   - aligning the existing policy and work instructions with the practice of snapshotting which emerged during the investigation period, where this has not already been done, and by ensuring that complete process descriptions are in place (Chapter 4);
   - to set up the authorisation process in such a way that the focus is on assessing whether the task of the relevant staff member makes it necessary to access investigation-related interception data (Chapter 6).

3. Laying down the authorisation periods, methods of use and the scope of the duty to provide information and to cooperate in policies and work instructions. This should at least show how and when these duties are communicated to the relevant provider and what the content of the provider letters should be. They should also specify that such work cannot be performed by the provider on a voluntary basis. The services should ensure proper records of the provider letters and compliance with the relevant policies and work instructions (Chapter 5).

9. Reflection for the purpose of amending the ISS Act 2017

With this review report, the CTIVD aims not only to conduct a lawfulness assessment, but also to contribute to the debate on investigation-related interception (and cable interception in particular) and the upcoming legislative amendment. During its investigation, the CTIVD observed that the Act, the interpretation of the Act and its implementation in practice were not entirely consistent on a number of points. This has consequences for the implementation of cable interception. This chapter lists the bottlenecks and gives a conclusion.

What does specificity mean in cable interception?

Cable interception is the power that mainly dominated public and political debate during the drafting of the ISS Act 2017. The terms 'dragnet' and 'data trawling act' were used frequently in this regard, and concerns were raised that this power would lead to the interception of entire neighbourhoods or Dutch cities. It was indicated by the (then) Minister of the Interior and Kingdom Relations in 2017 that data were indeed collected and analysed systematically and on a certain (large) scale through cable interception. This was, after all, the nature of cable interception.[72]

However, in a later debate, the Minister clarified that cable interception was not a dragnet power and emphasised the specificity of this means. The Ministry of the Interior and Kingdom Relations argued, among other things, that 'cable interception is always done for a specified purpose': 'Investigation-related interception allows for the interception of specific data streams that fit within the services' investigation assignments where proportionate to the threat and where the deployment of lighter means is not possible'.[73] In addition, examples were given of the expected volume reduction in cable interception. For example, the following example was cited: 'a cable contains 24 fibres with a total of 480 channels. Of those 480 channels, 3 channels are relevant to one or more investigation assignments and these are divided between 2 fibres. Only from these 3 relevant channels (out of the 480 channels in that particular cable) will the data be intercepted. It is expected that 95% to 98% of the data actually intercepted is expected to be deleted and destroyed immediately upon initial filtering. This is followed by a further volume reduction in stages 2 and 3. The proportion of the data transmitted through the cable that ends up being retrieved is many times less than one per mille'.[74]

However, the question is whether linking channels to investigation assignments is actually possible in all cases and is an effective fulfilment of the 'as targeted as possible' criterion. After all, data that are transported do not take a fixed route, but follow the cheapest and/or fastest route. As a result, the routes or channels through which data relevant to the investigation assignments are transported can therefore not be fully predicted. Also, the above example assumes that it is possible for the services to know where in the cable the data of, for example, targets are located. In addition, cable interception is included in the ISS Act 2017 for the purpose of recognising 'unprecedented threats'. Particularly for unprecedented threats, it is difficult to predict where in the cable the relevant data are located. The CTIVD believes that specificity in cable interception should mainly be sought in the application of filters, and less in the choice of channels. By setting positive and negative filters, it is possible to prevent all data from eventually being stored, except for data that could be related to an investigation assignment. Filters are therefore the ultimate tool to use when seeking to progress from untargeted interception to investigation-related interception.

72 *Parliamentary Papers II* 2016/17, 34588, no. 52, p. 4.
73 *Parliamentary Papers II* 2016/17, 34588, no. 18, p. 106.
74 *Parliamentary Papers II* 2016/17, 34588, no. 3, pages 110 and 111.

The fact that deployment of cable interception is linked to an investigation assignment, the power should be deployed in a manner that is 'as targeted as possible' and the final amount of data stored is limited compared to the total volume of intercepted data does not alter the fact that cable interception is by definition a bulk power with a high degree of inherent untargeted data collection. Most of the data intercepted and stored will always pertain to individuals and/or organisations that are not and never will be under investigation by the services. At the same time, this is also the reason why cable interception was included in the ISS Act 2017. In particular, the need for cable interception, according to the legislature, lies in recognising unprecedented threats. The very fact that it involves uncovering unprecedented threats means that this tool is only effective if there is a certain degree of untargeted data collection. The data ultimately stored by the services, whose relevance may then be assessed for up to three years, are related to investigation assignments. However, the criteria used to establish this relationship tend to be broad, such as geographical origin or language.

Absence of an adequate legal basis for snapshotting

Based on Section 52 (the duty to provide information), under the current system of the ISS Act 2017, the services should be able to gather sufficient knowledge about data streams to express a reasonable expectation that they are relevant in the context of their investigation assignments, and to indicate where the interception should take place in that case. This should take place at channel level, given the legislative history. In practice, however, it appears that the services are unable to properly justify this. It was considered by the TIB on the basis of the first request for authorisation that the services, with the knowledge they had gathered under Section 52, did not have sufficient understanding of the nature of traffic and data handled through the targeted fibre-optic routes. In addition, the services' analysis of the intercepted data shows that assumptions made on the basis of a provider's information are not always correct (anymore). The conclusion is that information pertaining to the 'outside' of a cable route is not always related to the nature of the data that are actually transported on the 'inside' of the cable. In other words, prior interception (snapshotting) is necessary in order to ensure the specificity of interception. However, the current ISS Act 2017 does not provide for this specific form of prior interception.

In practice, this prior interception was attempted through snapshotting. During the investigation period, the powers of cable interception (Section 48) and search aimed at interception (Section 49(1)) were used for this purpose with the aim of justifying specificity for production requests. Without a separate legal basis for snapshotting, this creates a problem: The legal requirements applicable to interception are fully applied to snapshotting, including the requirement that it be 'as targeted as possible'.

In doing so, however, the purpose of snapshotting is ignored. The aim of this activity is to carry out the subsequent stage of investigation-related interception in a manner that is 'as targeted as possible' and that infringes on citizens' fundamental rights as less as possible. Therefore, to achieve this purpose, a broad use of snapshotting is required. For if the deployment is too limited, insufficient knowledge is gained in order to actually deploy the final interception in a manner that is 'as targeted as possible'. The CTIVD therefore considers it important that the specificity requirement can be applied in a way that is in line with the circumstances of the case; in this case, snapshotting and the purpose of snapshotting. This should include a safeguard that the data collected should not be used by intelligence teams and should be destroyed after one year. This form of snapshotting may, in view of the amendment to the ISS Act 2017, be provided with an independent legal basis. This would also benefit the foreseeability of this activity.

The ISS Act 2017 Evaluation Committee also concludes that under Section 52 (duty to provide information) and public sources, the services were unable to gather sufficient information in order to justify the specificity of cable interception.[75] The Evaluation Committee's report recommends the creation of a new legal power that would allow the services to carry out short measurements. The sole purpose of a measurement is to optimise the operationalisation of an access location and/or the actual interception. The CTIVD takes the view that it should be clear that this is not merely a technical measurement, but actually a short-term cable interception. In addition, account should be taken of the fact that such a power must be deployable at two different points in the process. Firstly, it should be possible to deploy this power at different communication service providers to investigate the cable routes in order to be able to choose a provider. Secondly, it should be possible to intercept data on a broad basis in the next stage, namely the interception stage. Once the provider has been selected and the access location has been operationalised, the service must be able to intercept data on a broad basis in order to determine the location of the relevant data streams at the provider. This deployment should also be possible during the interception process, as data flows are not static. After all, if the power is not explained in sufficiently concrete terms, this creates the risk of new implementation bottlenecks arising.

The lack of a specific legal basis for snapshotting also affects the next stage of cable interception and of investigation-related interception more broadly. To renew the authorisation, according to the ISS Act 2017, the request for renewal of the authorisation should include the results obtained for the relevant investigation. This is complicated by the safeguard that the intercepted data cannot be used in the intelligence process. Therefore, no investigation was conducted into specific individuals, and the results therefore only focus on the next step: deploying (actual) interception in a manner that is as targeted as possible. This is in contrast to concrete results when collected data are used for the intelligence process. If snapshotting is provided with a specific legal basis, the application for interception will not be an application for extension, but an application for a different power with its own lawfulness assessment. The knowledge gained from the deployment of the snapshotting power can then be used to justify the interception power.

Commitments by the Ministers

As already mentioned in this review report, the Ministers of the Interior and Kingdom Relations and of Defence made several commitments in the context of the drafting of the ISS Act 2017 that relate to cable interception. These commitments have had an effect in cable interception practice and were also part of the assessment framework of both the TIB and the CTIVD. However, it is questionable whether it was the intention of the Ministers that these commitments would eventually become part of the legal framework and whether sufficient consideration was given to the enforceability of these commitments. Therefore, the legislature should pay attention to this and given an opinion in the context of the legislative amendment.

The commitment that there is virtually no prospect of cable interception being used in the coming years to investigate communications that originate and terminate in the Netherlands is not unequivocal. This commitment gives rise to the question whether the Ministers meant that these data will not be intercepted at all or that the data may be intercepted but will not be used for intelligence investigations. The interests to be protected in relation to this commitment are not clear either. Given the context in which the commitments were made, the Ministers may have sought to avoid the impression in the public debate that entire Dutch neighbourhoods were being intercepted. However, this is where the legal world is incompatible with the technical world.

75 *Parliamentary Papers II* 2020/21, 34 588, no. 88 (appendix 965058, p. 88 et seq.).

For instance, the question is whether the commitment literally refers to communications originating and terminating in the Netherlands or whether it extends further, e.g. to protect communications of all Dutch citizens. Another question to be asked is how to deal with Dutch citizens abroad or non-Dutch citizens in the Netherlands. Secondly, the ambiguity stems from how the commitment should be technically implemented. For example, whether a negative filter with Dutch IP addresses or based on Dutch language should be applied, and to what extent such filters are (or can be) 'watertight' at all. This also gives rise to the question as to what extent special personal data (such as ethnic origin) are processed. From interviews conducted by the CTIVD, it understands that in assessing the services, it is almost technically impossible to meet the Ministers' commitment.

In addition to these commitments in the policy rules, the Ministers have stated several times that the deployment of negative filters means that data that are irrelevant beforehand will not be stored. According to the Minister, some clear examples are Netflix and YouTube. But also the content of many web browsing activities, Facebook traffic, etc. has no intelligence value, according to the Minister. [76] Again, this shows that practice causes friction between the legal and political world. For the question is whether this traffic is in fact irrelevant beforehand. In the context of finding unprecedented targets, such data may very well be relevant.

Duty to cooperate in practice

In the ISS Act 2017, the duty to cooperate under Section 53 is linked to the power of interception (Section 48). This means that the duty to cooperate can only be used if authorisation has been obtained for the interception power. The legislator opted for a duty for the provider to cooperate with the interception because it was necessary to prevent the services from depending on voluntary cooperation given the importance of national security. If a provider refuses to cooperate, such refusal is liable to punishment.

As the extension of the cable interception was rejected, it was not possible to extend the authorisation for the duty to cooperate in time. During the period when there was no authorisation for interception, however, the services had to be able to carry out activities at the provider (see section 5.2), to ensure that interception could be started immediately upon approval of the authorisations. This situation raised several legal questions, namely whether the activities could be carried out on a voluntary basis. The relationship between the provider and the services was good and the provider was cooperative. There is also the question of which activities of the provider may fall under the duty to cooperate. The current law and interpretation of the law has safeguards if a provider does not cooperate. However, the legislature should also account for the possibility of a provider being proactive and (overly) cooperative in its cooperation with the services. Such cooperation speeds up the operational process, but has risks regarding fundamental rights of citizens. Lastly, there is the question of which activities fall under keeping an installed facility in place. In section 5.2, the CTIVD assessed practices during the investigation period. However, the duty to cooperate has been underexposed in the interpretation of the law and parliamentary debate. It would, therefore, benefit foreseeability if the legislature were to comment on this in any legislative amendments.

In addition, practice has shown that justifying and obtaining authorisation for cable interception is a long process. Operationalising an access location and technically realising the interception chain also took a long time. Combined, this means that a long period of time elapses from the time authorisation for interception is granted before actual interception can begin.

76 *Parliamentary Papers II* 2016/17, 34588, no. 18, p. 71.

The CTIVD sees the need to avoid delays given the importance of national security. For this reason, it calls attention to the link between the duty to cooperate (Section 53) and the power of interception (Section 48) in the context of the legislative amendment.

Conclusion

The legislature emphasised that the power of cable interception was necessary to protect national security. More than three years have now passed since the implementation of the ISS Act 2017 and the creation of cable interception powers. This period can be broken down into (I) collecting information under Section 52 and submitting the initial requests for authorisation (about five months), (II) obtaining authorisation after a rejection of the initial requests (about seven months), (III) then creating the interception chain (about eight months) and (IV) interception for the purpose of snapshotting with the aim of justifying specificity in the production requests (about 15 months). The authorisations for snapshotting had already expired for several months at the time of the adoption of this review report, and the interception has since ceased.

In this report, the CTIVD concludes that during the investigation period, the implementation of cable interception was strongly influenced by the interpretation given to this power when the ISS Act 2017 was drafted. Partly due to the public and political debate, the emphasis was placed on specificity, whereas it is a means that involves a high degree of inherent untargeted data collection. This explanation has affected the creation and interpretation of the legal frameworks for implementing cable interception. This interplay resulted in a complex set of requirements within which authorisation for cable interception had to be requested and granted, but also within which the interception had to be executed.

This also raises the question of the extent to which the interception carried out contributed to the original goal: being able to justify the specificity of production requests. As already described, interception was limited to certain channels. This is only part of the cable route on which the services can intercept data. Therefore, there is no complete picture. What is more, the cable landscape is dynamic: communication streams can change. The production request was not approved at the time of writing this report. It is therefore possible that the intercepted data may no longer provide an up-to-date picture of the communications landscape. In addition, it was not allowed to use the data for the intelligence process. As a result, the interception did not make a contribution to the services' tasks and thus to protecting national security. Interviews conducted by the CTIVD show that during the investigation period, the cable interception did contribute to the set-up of systems, the operationalisation of the interception chain and the acquisition of knowledge and expertise of cable interception. However, this was not the original main purpose of cable interception.

The CTIVD considers it important, also in the context of the amendment to the ISS Act 2017, to draw lessons from the knowledge and experience gained with cable interception. This means that in the further public and political debate, the untargeted nature of this means and its infringement on the fundamental rights of citizens should be named by the legislature and the necessity of this means in this context should be argued, taking into account the technical reality and feasibility of implementing the required safeguards. This is in the interest of the political and public debate on this power. This is also important for the effective deployment of this means in practice, and for the review of this means by both oversight bodies.

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

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl