

# Summary of review report

about the use of cable interception by the AIVD  
and the MIVD (in the snapshot phase)

CTIVD No. 75



Review Committee  
on the Intelligence and  
Security Services



**CTIVD No. 75**

# SUMMARY OF REVIEW REPORT

about the use of cable interception by the AIVD  
and the MIVD (in the snapshot phase)

## Summary

This review report is about the use of cable interception by the AIVD and the MIVD (hereinafter: the services) in what is known as the snapshot phase. Cable interception is also referred to as bulk interception. That means that the services intercept and collect communication from physical bearers (hereinafter: the cable) in large quantities, the vast majority of which concerns organizations or people who are not the subject of investigation by the services, nor ever will be. However, it must be possible to relate the interception to one or more of the services' investigation assignments. In this review report, the CTIVD answers to the following investigative question:

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

In the investigation period the services accessed a cable route at a communication service provider (hereinafter: provider) in order to intercept communication, such as internet traffic, at that point. Communication is relayed across cable routes by light signals that are transported through individual glass fibres. Those fibres may contain dozens of channels. The physical transfer point at a communication service provider where the services receive the intercepted data (the communication) is called the access location. The data stream that is relevant to the services for the established investigation assignment is acquired at that access location. In the context of accessing the cable for interception – known as operationalizing the access location – and identifying potentially relevant channels, the services used special investigatory powers, such as the duty to assist and provide information to which providers are subject.

The services' original intention was to set up regular cable interception on all available channels on certain cable routes on the access location. The Investigatory Powers Commission (TIB) found this to be unlawful because that was considered disproportionate and not 'as targeted as possible'. The services subsequently requested, and were granted, authorization for the power of cable interception in the form of snapshotting. Snapshotting has no separate legal basis but constitutes a limited use of the power of cable interception. The difference with regular interception is that snapshotting, including the related analysis, has an exploratory purpose, whereas regular cable interception is aimed at intercepting data to then be processed into intelligence products. The latter is also referred to as 'production'.

The approved authorization requests included safeguards to limit the use of cable interception to snapshotting. Thus the services had authorization to intercept channels no more than two hours a day, whereby they had to substantiate in advance that these channels had high intelligence value. Furthermore, that data was not allowed to be used by the intelligence teams, but only by specifically

designated persons for technical analysis. Based on technical and substantive characteristics, these officials investigated whether the intercepted data did in fact have potential intelligence value for the services' investigation assignments. Lastly, the data was not allowed to be stored for longer than one year. The CTIVD looked at compliance with those safeguards in its investigation and now reports on this issue. In addition, the CTIVD hopes its report contributes to the debate on cable interception and the upcoming amendment of current legislation by being transparent about the services' practice - in as far as possible given the state secret nature of the services' work.

### **Conclusions of the report**

The main finding and conclusion of this review report is that in the investigation period, the heads of services failed to sufficiently implement the legal duty of care (I). In addition to answering the investigative questions (II), the CTIVD establishes that the explanation given to cable interception in the parliamentary debate is at odds with the technical practice (III). A further recommendation is that snapshotting is given a separate legal basis (IV).

## **I. Insufficient implementation of duty of care**

The CTIVD concludes in this review report that the legal duty of care was insufficiently implemented in the investigation period. That constitutes a fundamental problem underlying a large part of the findings in this review report. The duty of care is laid down in Section 24 of the ISS Act 2017. That duty means that the heads of the AIVD and the MIVD are responsible for applying technical, staffing and organizational measures to ensure data is processed lawfully. The duty of care includes the continuous monitoring by both services of how they process data and to ensure that this data-processing is and continues to be in accordance with the applicable legal requirements (compliance).

Given the complexity, public sensitivities and the necessity for using cable interception, that means that a lawful processing procedure must rank high on the list of priorities of the heads of service. CTIVD notes that, in the investigation period, the implementation of the duty of care came secondary to operational interests. That conclusion was prompted in particular by the lack of suitable logging for compliance purposes and the lack of checks on the functioning of the technical systems. Consequently, unlawful conduct in the interception process occurred or was detected too late (see below).

At the end of August 2021, the CTIVD shared its findings of the investigation with both heads of service, in light of their specific responsibilities for the duty of care. Both services have since drafted an improvement plan. In addition to the improvement plan, the services intend to implement cable interception for the intelligence production process in phases. The services have specified that the technical chain will be tested first. Only when those tests have proven successful will a start be made with storing the data intended for the intelligence process.

### **Enhanced oversight**

Whether the services are ready for the production phase is a question the services will need to answer themselves. The CTIVD will oversee this closely and report on that in more detail. That oversight includes monitoring the phased implementation of cable interception.

## **II. Answers to the investigative questions**

The investigative question consists of two parts. The first examines the operationalization of the access location. The CTIVD concludes that the services acted lawfully on key components when setting up the access location. For example, the services only used the duty to provide information to request and receive legally permitted information, and a valid authorization based on Section 53 of

the ISS Act 2017 was in place at the time the access location was technically operationalized. However the CTIVD also established unlawful conduct. That refers to the use of special investigatory powers without authorization and to work carried out at the provider after the authorization terms expired. See section 5 of this review report for a full description.

The second part of the investigative question looks at how cable interception was conducted in the snapshot phase. In answer to this question, the CTIVD similarly concluded that the services acted lawfully in parts but unlawfully in others. One of the main conclusions relating to lawful conduct was that the method of conducting cable interception is actually an interpretation of the criterion 'as targeted as possible'. Several criteria influence how targeted the use of an investigatory power is. That criterion 'as targeted as possible' entails more than simply limiting the amount of data collected. The criteria offer scope to interpret the requirement 'as targeted as possible' in a way that reflects the nature of cable interception.

The services complied with the criterion 'as targeted as possible' and in addition they destroyed the intercepted data promptly and did not share the data with foreign services. The established unlawful conduct concerns the lack of compliance with certain safeguards in the requests for authorization, including the safeguard that the data should not be made available to intelligence teams. See section 6 of this review report for a full description.

### **Recommendations**

The CTIVD makes three recommendations in its review report that mainly relate to the interpretation of the duty of care. The key recommendations are to place ultimate accountability for the entire interception chain from acquisition and processing at a central level sufficiently high up so that there is an overriding authority within both organizations. In addition instruments should be set up for internal control and effective external oversight, which includes setting up logging for compliance purposes.

## **III. Explanation of cable interception**

The new investigatory power of cable interception was a much-discussed topic during the political and social debate on the ISS Act 2017. The term 'dragnet' was frequently used in that context because there was and still is a fear that communication is collected routinely and in bulk about people who are not the subject of investigation by the services. During and after the introduction of the ISS Act 2017, the social and political debate focused on how cable interception as a means could be as targeted as possible and on the fact that this investigatory power is linked to investigation assignments, in the attempt to dispel the impression of a dragnet. The services were presented as being able to identify in advance the exact channels through which the relevant information is transported. In addition, the minister of the Interior and Kingdom Relations and the minister of Defence made several pledges, one of which was that there is virtually no prospect of cable interception being used in the coming years for investigation into communication that originates and terminates within the Netherlands (except for cyber defence purposes). Another was that traffic which is known in advance not to be relevant, such as streaming service and bit-torrent traffic, would be filtered out. A further pledge was that cable interception would be conducted 'as targeted as possible'.

The CTIVD concludes in this review report that the explanation given to cable interception is at odds with the nature of the investigatory power, the means and the implementation in the technical practice. The fact that the use is linked to an investigation assignment and that the investigatory power should be used in as targeted way possible, does not alter the fact that cable interception is by definition a bulk power which to a large extent constitutes collecting data in an inherently untargeted way. The majority of the data that is intercepted will always involve people and/or organizations that are not

under investigation by the services, nor ever will be. At the same time, this is exactly the reason why cable interception was included in the ISS Act 2017. In the legislator's view, the necessity for cable interception lies mainly in recognizing unknown threats. Precisely the fact that the cyber threats that need to be exposed are unknown, means that this method can only be effective if the collection of data is, to a certain extent, untargeted. The data ultimately stored by the services is linked to the services' investigation assignments. The criteria by which that link is established however, are generally broad, such as geographical origin or language. Furthermore it is impossible to fully predict through which cable routes or channels the data relevant to the investigation assignments will be transported, as the data does not take a fixed route but follows the cheapest or fastest one.

The CTIVD also concludes that the pledge about communication that originates and terminates within the Netherlands is unclear and raises questions in practice, for example where it concerns feasibility and technical implementation. The pledge about negative filtering of traffic from streaming services and bit-torrent traffic raises the question whether such traffic is truly not relevant by default.


Partly in the context of an amendment to the ISS Act 2017, the CTIVD considers it important to profit from the lessons learned and the experience gained with cable interception. That means that in the ongoing social and political debate, the nature of this means and the infringement on the fundamental rights of the general public must be specified by the legislator and the need for this means must be substantiated in that context. That implies taking into account the technical reality and feasibility of implementing the required safeguards.

#### **IV. Legal grounds for snapshotting**

The CTIVD concludes in its review report that snapshotting must be given a separate legal basis. The current system under the ISS Act 2017 assumes that the services are able to substantiate to a sufficient degree in advance how targeted the interception will be. However that proves not to be the case. The investigation shows that the duty to inform under Section 52 yields too little information for the services to do so. The CTIVD endorses the need for snapshotting and the analysis of that data, because these activities contribute significantly to the interception being targeted for the production phase.

The lack of specific legal grounds compelled the services to use snapshotting based on the investigatory power of cable interception. However the legal requirements are aimed at cable interception for the production, making them unsuitable to the nature and purpose of snapshotting, i.e. being able to substantiate in advance that the cable interception for production will be targeted.

The CTIVD therefore considers it important, partly in light of the foreseeability and legal certainty, that snapshotting is given a separate legal basis. It is important that the requirement 'as targeted as possible' is applied in a way appropriate to the circumstances of the case; in this case, the nature and purpose of snapshotting.



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

**T** 070 315 58 20

**E** [info@ctivd.nl](mailto:info@ctivd.nl) | [www.ctivd.nl](http://www.ctivd.nl)