

# Review report

On the application of filters in investigation-related interception by the AIVD and the MIVD

**CTIVD no 63**

(adopted on 17 July 2019)



Review Committee  
on the Intelligence and  
Security Services

## Structure of the report

This report has the following components:

The review report

Appendix A: Elaboration of the review report

Appendix B: Assessment framework

Appendix C: Definitions

This report has a classified appendix.

Given the technical complexity of the subject matter, the CTIVD has opted to divide the report into a review report that includes the main findings and a separate appendix (A) that discusses the findings in greater detail. Appendix A should be read to obtain a deeper understanding of the subject matter. The review report and appendix A have been written to be read as separate documents and consequently some overlap cannot be avoided. The full assessment framework has been incorporated in appendix B. Appendix C contains the definitions.

**CTIVD no 63**

# REVIEW REPORT

On the application of filters in  
investigation-related interception  
by the AIVD and the MIVD

## Table of contents

<b>Summary</b>	<b>3</b>
<b>Background to the investigation</b>	<b>5</b>
<b>Investigation-related interception</b>	<b>5</b>
<b>As targeted as possible</b>	<b>6</b>
<b>Filtering</b>	<b>6</b>
<b>Policy, process descriptions and work instructions</b>	<b>7</b>
<b>Overall view: the application of filters in practice</b>	<b>8</b>
<b>Practice for the various forms of investigation-related interception</b>	<b>9</b>
<b>Random checks</b>	<b>11</b>
<b>Classified appendix</b>	<b>12</b>
<b>Conclusions</b>	<b>12</b>
<b>Recommendations</b>	<b>13</b>



## REVIEW REPORT

On the application of filters in  
investigation-related interception  
by the AIVD and the MIVD

### Summary

This report is structured based on a central question and several subsidiary questions, the answers to which are outlined in this summary. The central question reads as follows:

**How are filters applied in investigation-related interception and does that application meet the requirements set in the context of lawfulness by or pursuant to the ISS Act 2017?**

The investigatory power to conduct investigation-related interception allows the AIVD and the MIVD to collect – to a certain extent in an untargeted way inherent to the process – communication both by satellite and cable. This is in fact bulk acquisition, meaning that large amounts of data (bulk) are intercepted using investigation-related interception. It is unavoidable that in the process the services will also intercept data from people and organizations that are not, nor will be, the subject of investigation.

*Subsidiary question 1: What are the legal requirements that the filters in investigation-related interception must meet?*

The services can only comply with the requirement that the use of the power of investigation-related interception is ‘as targeted as possible’ by applying filters. This means that the services limit to a minimum any information not strictly necessary for the investigation, given the technical and operational circumstances of the case. Filters are the tool *par excellence* to ensure that interception transforms from untargeted to investigation-related. In addition to the requirement of interception being as targeted as possible, other requirements apply such as the duty of care for processing data, which is further described in Appendices A and B.

*Subsidiary question 2: Has filtering been adequately described in policy, work processes or work instructions and how are the legal requirements implemented in them?*

In the investigation period from 1 May 2018 to 1 January 2019 there were no process descriptions or work instructions relating to the most targeted filtering possible within investigation-related interception. The policy that was available lacked sufficient substance to serve as a framework for the application of filters and thus for lawfully using the investigatory power of interception. The CTIVD recommends bringing policy, process descriptions and work instructions up to date as soon as possible.

*Subsidiary question 3: How is filtering subsequently carried out in practice and is there any internal review of the functioning of the filters which enables effective oversight?*

Despite the lack of policy, filtering of intercepted satellite and radio communications is 'established practice'. The services have specific plans to also filter in the case of cable interception, which was not yet operational in the period investigated. In this period, filtering was mainly conducted based on capacity considerations and technical restrictions, as appears from the fact that when the ISS Act 2017 was introduced – resulting in far stricter privacy requirements for investigation-related interception – the practice of filtering intercepted satellite and radio communications had undergone little or no change. Therefore the requirement that interception must be 'as targeted as possible' had not had any effect.

*Subsidiary question 4: Does the implementation practice meet the requirements of the ISS Act 2017?*

The investigation assessed filtering for different types of investigation-related interception. The interception of HF and UHF (local telecommunication) was found to be *lawful*, with the exception that, in the case of HF interception, data that cannot – or no longer - be connected to a current or pending investigation assignment was not destroyed immediately. This was found to be *unlawful*.

The CTIVD considers the application of filters in SHF interception (satellite communication) to be *lawful* in those cases where the contents and metadata are stored based on characteristics in a positive filter and in the case of a specific form of satellite communication. The application of filters in SHF interception relating to certain processing systems was found to be *unlawful*. Although interception of SHF is aimed at a limited number of satellites and the services only intercept links that can geographically be connected to approved investigation assignments, the services fail to always account for why filtering cannot be more targeted. Part of the processing systems used let through all content and/or metadata from recognized data or protocol types. Simply storing a wide range of data is incompatible with the requirement that interception must be 'as targeted as possible'.

Although cable interception was not yet operational in the investigation period, the plans were already known. Therefore the CTIVD was able to conduct a lawfulness assessment. In time, the services intend to apply a similar system for SHF interception as the system used for cable interception. The proposed application of filters in cable or SHF interception would, in its current form, directly lead to *unlawful conduct* because of the lack of justification for storing a wide range of metadata. The proposed application of filters on content is *lawful*, because this does meet the requirement to be as targeted as possible.

Finally, the CTIVD established that during the period investigated the services themselves did not have a full overview of the systems and operational processes used and their functioning. Internal checks that ensue from the *duty of care for data processing* did not take place on a structural basis, so that the possibility for effective review at process and data level in particular has not been sufficiently guaranteed.

The CTIVD therefore recommends bringing into effect the requirement that interception be 'as targeted as possible' and the *duty of care for data processing* in the filter process of investigation-related interception as soon as possible. That means that an internal check must be made periodically on composition, functioning and adjustment of the filters and whether or not the filters are still set to be 'as targeted as possible'.

*Answer to the central question*

Based on the findings, the answer to the central question is that filtering does take place in practice but mainly for capacity and technical reasons. The introduction of the ISS Act 2017 has caused little or no change to this practice. The requirement that the filters in investigation-related interception must be applied in 'as targeted way as possible' therefore had not had any effect on the application of the filters. This means that in the investigated period there were insufficient safeguards to ensure that the interception was indeed investigation-related and not untargeted.

## REVIEW REPORT

On the application of filters in  
investigation-related interception  
by the AIVD and the MIVD

### Background to the investigation

During the parliamentary debate and subsequent advisory referendum, the Intelligence and Security Services Act 2017 (hereinafter: ISS Act 2017) was extensively discussed. One of the most important topics in this debate was the new investigatory power for the AIVD and the MIVD to conduct investigation-related interception, known as 'OOG-interceptie' in Dutch. This investigatory power allows the services to intercept large amounts of bulk communication from either satellite and radio communications or cable. Untargeted interception of satellite and radio communications was permitted under previous legislation, the ISS Act 2002, and thus does not constitute a new investigatory power. The ISS Act 2017 did entail some tightening of the requirements to use and implement that investigatory power.

In the lead up to the advisory referendum, the CTIVD published its Final Balance on the ISS Act 2017. One major focus point already expressed in the Final Balance is the application of filters when intercepting from the cable. These filters determine which data may be stored for processing in any subsequent intelligence investigation by the AIVD and the MIVD and which may not. In other words, the filters determine whether or not the interception is actually *investigation-related*, as required by law. The CTIVD indicated it would review the filtering of data obtained by investigation-related interception.

On 4 December 2018, the CTIVD published its first progress report on the introduction of the ISS Act 2017. This report established that the practice of filtering being as targeted as possible had not been described in policy, work processes or work instructions. This led to the conclusion that the risk of *unlawful conduct* by both services was high. This in-depth investigation, which entails a full assessment of lawfulness instead of a marginal risk-assessment, assesses whether the established risks manifested themselves and if so, to what degree. The investigation covers the period from 1 May 2018 (when the ISS Act 2017 entered into force) to 1 January 2019.

### Investigation-related interception

The investigatory power of investigation-related interception, laid down in Sections 48, 49 and 50 of the ISS Act 2017, allows the AIVD and the MIVD to intercept communication in bulk. Bulk acquisition means that a large amount of data is collected, to a certain extent in an untargeted way which is inherent to the process. In those cases, the services always also intercept data from people and organizations that are not, nor will be, the subject of investigation. That is why in the debate on the Act, the term "trawl net" was coined as a metaphor for the data collected from "innocent citizens". Nevertheless, the

investigatory power was considered necessary to be able to keep up with technological developments, such as the fact that communication has shifted to the internet and thus to the cable, while at the same time targeted methods and interception of satellite and radio communications are losing part of their value precisely because of these developments, which in turn has an impact on the (international) intelligence position of the AIVD and the MIVD.

The purpose of investigation-related interception is collecting information to enable timely discovery of unknown threats, which the services do in the context of investigation assignments based on the Integrated Intelligence and Security Services Order. One example of investigation-related interception in this respect is the storage of metadata (who calls whom and when) and the contents of telephone traffic sent by satellite, because this traffic can be related to the conflict in Syria, for example. This data can then be used to identify new targets. Another example is detecting malware in internet traffic as it passes through a fibre-optic cable.

## As targeted as possible

Although investigation-related interception is less targeted by its nature, the decision was taken following the outcome of the advisory referendum on the ISS Act 2017 that the investigatory power must be used in an 'as targeted way as possible'. This means that the services limit the acquisition of any information not strictly necessary for the investigation to a minimum, given the technical and operational circumstances of the case.

In practice the services meet the requirement of interception and storage being as targeted as possible in the following three ways: (1) the communication medium selected, (2) the data stream selected, and (3) additional positive or negative filters. Selecting the communication media to be intercepted is the first step towards the interception being as targeted as possible. The services choose to only intercept the communication on fibre-optic cables (at so-called access locations) and on satellites that are expected to contain information relevant to the investigation assignments which the services must carry out. This does not yet constitute filtering.

## Filtering

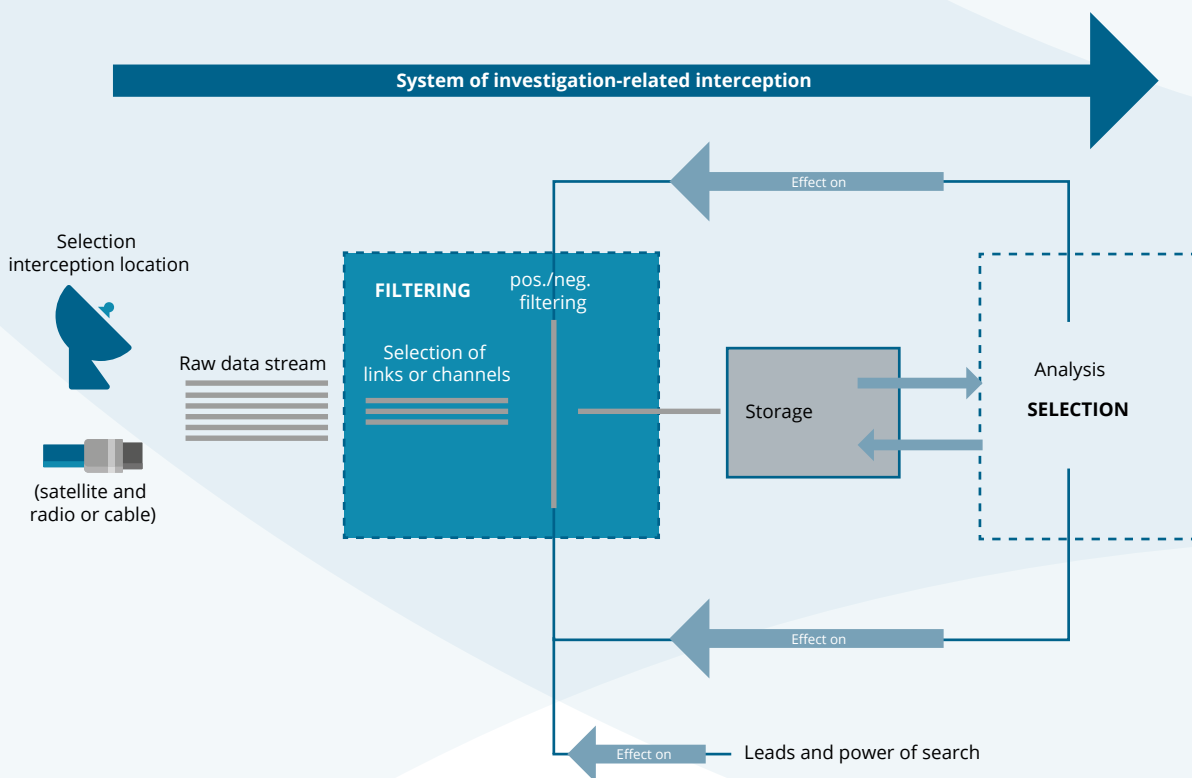
Once the choice for the communication media to be intercepted has been made, filtering starts. Filtering is part of the interception power in Section 48 of the ISS Act 2017. Filtering is a process that determines which data from data streams (metadata and communication content) that make use of the communication media selected by the services will ultimately be stored, short-term or long-term, for the AIVD and/or MIVD's ongoing investigations and which will not. This is done by (2) selecting the data stream and (3) additional positive or negative filters.

An important fact to consider when selecting the data stream is that a fibre-optic cable consists of multiple fibres, which in turn can be divided into dozens of other channels. The data streams via satellite and radio communications are spread over a range of frequencies or frequency bands. In satellite interception these are referred to as links. The services select only those data streams (and therefore channels, frequencies and links) which are reasonably expected to be relevant to ongoing investigations by the services. The services base these expectations on knowledge they already have or have obtained from external parties. They may also take short integral recordings (snapshots) of the data streams to analyse the traffic for potential relevance. This process is called search aimed at interception, for which Section 49(1) of the ISS Act 2017 provides a legal basis. This exploratory investigatory power ultimately contributes to the use of the interception power being as targeted as possible.



Even after selecting the data streams that are to be intercepted, these will always still contain data that is a priori not relevant to the ongoing investigations by the AIVD and the MIVD. Therefore it is not necessary to store all intercepted data from data streams for long periods of time. For this reason shortly after interception, a further positive and negative filtering is conducted in the processing systems. A negative filter indicates which data must not be passed through to be stored. An example is excluding YouTube or Netflix traffic.

A positive filter indicates which data must be passed through to the services' storage because of its potential relevance to their ongoing investigations. The positive filter may for example include technical characteristics, such as telephone numbers or email addresses, of which the services have indications that they are being used by a target (such as leads in the context of search aimed at selection as referred to in Section 49(2) of the ISS Act 2017). In any case, the positive filter contains the so-called selection criteria. These are technical characteristics for which there is authorization to learn the content of the communication (*selection* as referred to in Section 50(1)(a) of the ISS Act 2017). Before the power of selection itself can be used, authorization must be given by the Minister and that authorization must then be assessed as *lawful* by the TIB. A positive filter could therefore include a telephone number that is being used by a target, for whom the AIVD or the MIVD have been authorized to select their communication.



## Policy, process descriptions and work instructions

In the period investigated there were no process descriptions or work instructions that related to investigation-related interception, including the application of filters in as targeted a way as possible. The policy that was available lacked sufficient substance to serve as a framework for the *lawful* use the investigatory power of interception.

Based on the first progress report published on 4 December 2018, the Joint Sigint Cyber Unit (hereinafter: 'JSCU'), a joint unit of the AIVD and the MIVD, has been busy updating the policy and bringing it into line with the ISS Act 2017. A draft of the new policy was shared with the CTIVD in March 2019 and was supplemented at the beginning of May 2019.

This new policy has almost the same principles as the assessment framework adopted by the CTIVD in this investigation. The process descriptions that reflect the interception process are practically identical to the findings in this investigation. The services have told us that they will elaborate this further in the work instructions to be drawn up, which contain specific directions for employees involved in investigation-related interception. When this report was drafted, these work instructions were not yet available. The CTIVD recommends bringing the policy that is lacking for filtering, and in particular the work instructions, up to date as soon as possible. It is of the essence to provide employees with specific instructions on how to apply filters in practice.

## Overall view: the application of filters in practice

The overall view is that filtering of interception of satellite and radio communications is 'established practice'. The services also have specific plans to filter in the case of cable interception, which was not yet operational in the investigated period. Applying filters contributes significantly to preventing an infringement of the right to privacy (or any other fundamental right) or to limiting that infringement to an acceptable level.

In the investigated period, filtering was mainly conducted based on capacity considerations and technical restrictions, as appears from the fact that when the ISS Act 2017 was introduced - resulting in far stricter privacy requirements for bulk interception - the practice of filtering when intercepting satellite and radio communications had caused little or no change to policy or the practice of filtering. The new legislation has not led to any substantial changes to the composition of filters or to an amendment of the procedure for compiling or adjusting filters. Therefore the requirement that interception must be 'as targeted as possible' in the filtering process had not been implemented during the investigated period. That means that in the investigated period there were insufficient safeguards to ensure that the interception was indeed investigation-related and not untargeted.

In addition, the service units who conduct the investigation-related interception generally receive no qualitative feedback from the intelligence process, for example about the functioning and result of the filtering. It is important that feedback is provided on the intelligence value of intercepted communication media and data streams, so that the filters can be adjusted accordingly if necessary. In short, feedback is essential to be able to filter in as targeted a way as possible. This could also increase the operational value of interception, in addition to improving the lawfulness. The CTIVD recommends arranging for qualitative feedback relating to investigation-related interception.

In interviews conducted in the course of its investigation, the CTIVD established that JSCU staff tasked with actual interception - sometimes in senior posts and crucial positions in the interception and filter process - were not always fully informed of the new legal framework applicable to their work. The CTIVD therefore recommends taking organizational and staffing measures to ensure that staff are better informed of the legal framework and content of internal policy.

The investigation also shows that during the investigated period the services themselves did not have full overview of the systems and operational processes used or the procedures followed. However, in the course of the investigation their overview increased. Internal checks that ensue from the *duty of care for data processing* did not take place on a structural basis, so that it has not been sufficiently guaranteed that effective review can take place at process and data level in particular.

The CTIVD therefore recommends bringing into effect the requirement of interception that is 'as targeted as possible' and the *duty of care for data processing* in the filter process of investigation-related interception as soon as possible. That means that an internal check must be made periodically on composition, functioning and adjustment of the filters and whether or not the filters are still set to be 'as targeted as possible'. For that purpose the roles and responsibilities must be laid down clearly. The services have already taken the first steps in that direction.

## Practice for the various forms of investigation-related interception

It is not easy to provide an overall view of the practice of filtering because the practical implementation can differ per interception type. These differences can be found in the level of filtering but also in the position the filter takes within the processing procedure. The findings below apply to both services unless indicated that the finding applies only to either the AIVD or the MIVD.

### High Frequency (HF)

HF communication consists of radio transmitters and receivers sending messages via satellite. Users of HF may be governments, diplomatic institutions and military organizations, but also weather and radio stations. As a result, the HF bands generally contain little civilian communication. That reduces the interference with the right to privacy (among other things) compared with other forms of interception aimed at more publicly accessible communication methods.

The interception of HF bands is mainly carried out in Eibergen. The technical nature of HF traffic, in particular the constantly changing frequencies used, renders it almost impossible to exclude any connections beforehand. The services do, however, take active measures to exclude traffic from broadcasters and amateur broadcasters. So although there is hardly any negative filtering at the level of data streams, i.e. frequencies, this is acceptable given the technical restrictions of the systems used, where it comes to filtering and given the nature of the communication traffic.

However, in the systems used for interception, positive filtering does take place on the basis of characteristics known to the services, such as the used frequency, transmission equipment and location. The nature of HF traffic means that it does not contain any metadata of its own. The contents of the communication recognized on the basis of these characteristics are stored. This type of filtering makes the most significant contribution to reducing the intercepted communication to just the information which is (potentially) relevant to the services' investigation assignments. The application of filters in HF interception was found to be *lawful*.

In the short-term, however, a solution must be found for the immediate destruction of data that is recognized but that cannot, or no longer, be related to a current investigation assignment or ongoing investigation. Although the services currently store this information in an enclosed area and do not use it for their investigations, the fact that this evidently non-relevant data is not immediately destroyed is *unlawful*.

### Super High Frequency (SHF or satellite traffic)

The services are capable, with the help of the ground station in Burum among others, of intercepting SHF signals that are transmitted via satellites. The various links on a satellite are used to deal with a variety of communication forms, such as telephone and messaging traffic. These links can also contain internet traffic. In principle, the communication that is intercepted has either its origin or its destination abroad.

It holds true for the overwhelming majority of satellites that only those links are included that are technically suitable for interception. This is the first form of technical filtering, which as a rule excludes a considerable number of links. In addition, the services only intercept those links that contain geographical characteristics which can be related to approved investigation assignments. These two filter rounds, both technical and on characteristics, reduce the intercepted communication to a limited part of the total traffic via a satellite.

The intercepted communication is subsequently transferred into a stream of digital information. This contains the communication data from all links included in the interception. To access the information from this stream which the services store for their intelligence process, the stream is first duplicated several times. These duplicated streams are then fed as input into various systems.

These distinct processing systems are able to recognize data from the stream, i.e. data in a known classification, such as the type of communication, protocol or communication service, and translate it into output that is understandable for the AIVD and the MIVD in the form of content, metadata or a combination of both. That makes it possible to 'fish out' certain forms of speech or text messages from the stream. Data not recognized by any of the systems are irretrievably lost and are, in a legal sense, destroyed.

Part of the processing systems used, however, let through all content and/or metadata from recognized data or protocol types. This data allowed through is ultimately stored to be used in the ongoing investigations by the AIVD and the MIVD. The services do not justify in all cases why the filtering cannot be carried out in a more targeted way. Simply storing a wide range of data is incompatible with the requirement that interception must be 'as targeted as possible'. The application of filters in SHF interception was therefore found to be *unlawful*, where it concerns these processing systems. The CTIVD considers the application of filters in SHF interception to be *lawful* in those cases where the contents and metadata are stored based on characteristics in a positive filter and in the case of a specific form of satellite communication.

### **Local interception of telecommunication (Ultra High Frequency)**

The services have systems that allow interception of telecommunication in the UHF spectrum in a relatively restricted (geographic) area .. This method is mainly used in the context of support for Dutch missions abroad. The intercepted communication generally has its origin or destination abroad.

The main contribution to the requirement of being as targeted as possible lies in the restricted area where this means of interception can be used. In addition, this form of local interception allows negative filtering on the basis of characteristics such as directions (location) and frequencies. In addition, positive filtering is applied to spoken content using technical characteristics determined in advance. The other communication is not filtered. The result is that all other intercepted (written) content and metadata - excluding spoken communication - also becomes available for both services. Given the purpose for which it is used and its geographical delineation among other factors, this form of interception meets the requirement of interception that is as targeted as possible. The CTIVD assesses the application of filters in local interception of telecommunication as *lawful*.

### **Plans for cable interception and future SHF interception**

In the period investigated, the power of investigation-related interception of the cable had not yet been put into practice. However, it is possible to provide a first assessment, because part of the plans to do so and the processing system to be used are already known. In the future, this system will replace the majority of the processing systems currently used for SHF interception.

The system only allows content and corresponding metadata to pass through for storage if these comply with the characteristics included in the positive filter. The system thus complies, where it concerns filtering on content, with the requirement that interception must be 'as targeted as possible' and is therefore *lawful*.

The system also allows all metadata of data types and protocols recognized by the system to pass through. Of all metadata not recognized by the system a very small data set is still passed through to be stored. During the period investigated, no clear definitions of the terms metadata and content had been given in policy. When this report was drafted, these definitions were in place. The CTIVD agrees with the definitions, except the fact that - contrary to what is stated in policy - communication that is publicly available or not aimed at a defined group, such as a message on Twitter, should indeed qualify as content.

Moreover, it is important that these definitions are reflected in the technical configuration of the processing system to be used for cable interception, otherwise it cannot be ruled out that information that should be seen as content is allowed through and stored as metadata. The same goes for the promise by the ministers that there is virtually no prospect of investigation-related interception being used in the coming years on traffic with origin and destination in the Netherlands (domestic traffic) except in the context of cyber defence. In this case also it is important to translate this requirement into policy, process descriptions and work instructions and to implement the ensuing technical measures into the relevant systems.

Allowing all (recognized) metadata through to be stored, temporarily or not, is not in line with interception being 'as targeted as possible'. Before cable interception becomes operational, the services must be able to justify for which types of data and protocols it is necessary to store a wide range of metadata and why no further restrictions can be applied in order to meet the requirement of interception being as targeted as possible. This must be recorded to allow for internal checks and external review of the deliberations made. When this report was drafted, this explanation was not yet available. The CTIVD asserts that the proposed application of filters in cable or SHF interception would, in its current form, directly lead to *unlawful conduct*.

## Random checks

To validate the findings, the CTIVD's ICT Unit conducted a random technical check. This random check consisted of collecting aggregated information about data obtained from investigation-related interception. For each interception means (HF, SHF and UHF) the Unit examined the features of the intercepted data stored in the databases, which therefore had been allowed through the filters. These features could for example be the type of data stored, the geographical regions the communication is from and in how many cases the content of that communication was also stored.

This information was subsequently compared with the findings from the investigated period. The outcome of the random check largely corresponded with what was to be expected on the basis of the findings. In a couple of cases the results of the random check raised new questions, which were investigated further. The final results of the random check confirm the findings, conclusions and recommendations as recorded in this report. The results of the random check and a more detailed description of the filters used have been included in a classified appendix to this report.

# Classified appendix

In light of protecting national security, a number of further details relating to the investigation have been described in a classified appendix. This classified appendix consists of seven pages and does not report any *unlawful conduct* that has not been included in the public review report.

## Conclusions

### General conclusions

1. Filtering is established practice and is mainly conducted based on capacity reasons and technical restrictions.
2. The introduction of the ISS Act 2017 has led to little or no change in policy or practice of filtering in the interception of satellite and radio communications, so that the requirement that interception must be 'as targeted as possible' in the filtering process had not been implemented.
3. JSCU staff tasked with actual interception are not always fully informed of the new legal framework applicable to their work.
4. There was no policy or other written documentation in which the implementation of the filtering process for interception of satellite and radio communications or cable interception was recorded to a sufficient degree of detail so that it could provide direction for the filtering process. There was, however, general policy and the services have shared their new policy with the CTIVD after the investigated period.
5. During the investigated period, the services themselves lacked a comprehensive overview of the systems and operational processes used and the procedures followed. However, in the course of the investigation their overview increased. Internal checks that ensue from the *duty of care for data processing* did not take place on a structural basis.
6. The service units that conduct the investigation-related interception generally receive no qualitative feedback from the intelligence process.

### Conclusions per interception means

7. The application of filters in HF interception was found to be *lawful*, except for the lack of destruction of data that is recognized but that cannot, or no longer, be related to a current investigation assignment or ongoing investigation. The latter is *unlawful*.
8. The application of filters in SHF interception relating to certain processing systems was found to be *unlawful*. Although SHF interception is aimed at a limited number of satellites and the services only intercept links that can geographically be connected to approved investigation assignments, the services fail to always account for why filtering cannot be more targeted. Part of the processing systems used let through all content and/or metadata from recognized data or protocol types. Simply storing a wide range of data is incompatible with the requirement that interception must be 'as targeted as possible'. The CTIVD considers the application of filters in SHF interception to be *lawful* in those cases where the content and metadata are stored based on characteristics in a positive filter and in the case of a specific form of satellite communication.

9. The application of filters in local interception of telecommunication (UHF) is *lawful*. The main contribution to the requirement of being as targeted as possible lies in the restricted area where this means of interception can be used. The result of technical and geographical restrictions is that the potential infringement by the use of this means is relatively low. In addition, negative filtering can take place and there is positive filtering for spoken content. Given the purpose for which it is used, among other factors, this form of interception meets the requirement of interception that is as targeted as possible.
10. The proposed application of filters in cable or SHF interception would, in its current form, directly lead to *unlawful conduct*. There is no justification for the storage of a wide range of metadata. Likewise, the services lack an adequate overview of the whole of systems and processes, and how these function, and the policy for content and metadata in regard to filters still needs to be technologically embedded. The services have already taken the first steps in that direction. The proposed filtering of content is *lawful*.

## Recommendations

This report looked at how the services apply filters in investigation-related interception and whether this application meets the requirements set in the context of lawfulness by or pursuant to the ISS Act 2017. The results of the findings in these chapters lead to the following recommendations.

### General Recommendations


1. In addition to specific policy and process descriptions, draw up work instructions as soon as possible relating to filtering in investigation-related interception to achieve a comprehensive policy and provide specific guidance for the filter process in practice. It is important, in particular where it concerns filtering, that all the requirements of appendix A.3 are included in those work instructions. This makes it necessary to focus on the fundamental issues arising from these requirements, such as the technical distinction between content and metadata and the treatment of domestic traffic (on the cable).
2. Describe what the *duty of care for data processing* entails for the filtering process within investigation-related interception. This means that the services should at least periodically check the composition, functioning and adjustment of the filters, the corresponding systems and processes, and whether or not the filters are still set to be 'as targeted as possible'. Lay down the roles and responsibilities for that purpose in a clear way.
3. Organize qualitative feedback relating to investigation-related interception between those parties involved in the acquisition and filtering of data and staff in the intelligence process, so that the filters can be adjusted on that basis. That will not only benefit the requirement of being as targeted as possible, and consequently the lawfulness of the filtering and interception process, but it can also contribute to the operational value of interception. Although this recommendation applies to all investigation-related interception, it applies particularly to HF and SHF.
4. Ensure that the JSCU staff involved in investigation-related interception have sufficient knowledge about new policy and the current framework of the ISS Act 2017, emphasizing the legal provisions pertaining to investigation-related interception which are directly applicable to their work. This does not mean that they need to acquire an in-depth knowledge of law, but they must be able to place their work within the legal framework and know where to seek a legal advisory opinion when in doubt about the lawfulness of their actions.

### **Recommendations per interception means**

5. HF interception: Immediately destroy any data that cannot be related to current investigation assignments or ongoing investigations and that are evidently non-relevant.
6. SHF interception: Adjust the filters so that interception is 'as targeted as possible'. Substantiate and record internally for those cases where a wide range of content or metadata is stored why filtering in SHF interception cannot be more targeted. This must be recorded to allow for internal checks and external review of the deliberations made.
7. Plans for SHF and cable interception: Substantiate and record per data and protocol type why the storage of a wide range of metadata is necessary in light of 'as targeted interception as possible' before cable interception becomes operational. This must be recorded to allow for internal checks and external review of the deliberations made.







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