Appendix III: Definitions

to the 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

APPENDIX III: DEFINITIONS

to the review report about the use of cable interception by the AIVD and the MIVD

This glossary explains several terms used in the review report. The CTIVD has not aimed for completeness in the descriptions provided but rather has tried to give readers an understanding of the relevant terms that is as concrete as possible.

Access location	The physical transfer point at a communication service provider where it receives the intercepted data. The data stream that is relevant to the services for the established investigation assignments is acquired at this access location.
As targeted as possible	This involves keeping to a minimum the acquisition and processing of data not strictly necessary for the investigation, given the technical and operational circumstances of the case.
Bulk (data set)	Bulk data sets are large collections of data, the vast majority of which concern organizations or people who are not the subject of investigation by the services, nor ever will be.
Cable interception	The use of investigation-related interception on the cable.
Cyber	An umbrella term for various activities in respect of computer networks and data streams.
Cyber Defence	Protection against digital threats like cyber attacks and malware.
Data processing	Collecting, recording, arranging, storing, updating, altering, retrieving, consulting or using data, disseminating data by means of forwarding, distributing data or any other form of making available of data, and the assembling, interrelating, protecting, deleting or destroying of data (Section 1, preamble and (f), of the ISS Act 2017).
Data stream	Data that move from one system to another via a connection.
Division of tasks and roles	This is a form of compartmentation in which a position and/or role and/or is decisive for access to data. It determines whether an employee will have authorisation to examine certain data to others do not have access, based on the tasks that have been conferred on the position of the employee in question.

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 is processed lawfully.
Ether	In the present investigation, this term refers to non-cablebound communication like satellite and radio signals.
Filter	The filtering process is decisive for the difference between the data streams available (communication) on the communication media chosen by the services and the data from these streams that are ultimately stored for the intelligence process. As such, filters are the ultimate tool to use when seeking to progress from untargeted to investigation-related interception. A distinction can be made between positive and negative filters.
Foreign intelligence or security service	An intelligence or security service from another State.
Integrated Intelligence and Security Services Order	The Integrated Intelligence and Security Services Order is an order from the Council for Intelligence and Security Services, a sub-council of the Council of Ministers. The investigations of the AIVD and the MIVD are guided by this order, which is adopted once every four years. The investigation priorities are determined by the responsible Ministers from the ministries that use AIVD and MIVD information most. The Integrated Intelligence and Security Services Order is drawn up in consultation between the Ministries and the AIVD and the MIVD. The specifics of the investigation themes and prioritisation are set out in the appendix to the Integrated Intelligence and Security Services Order, which is a state secret.
Intelligence service	A service that conducts investigations into other countries for the purpose of identifying real and potential threats to the service's own national security.
IP (internet protocol)	The protocol that facilitates communication between computer networks.
ISS Act 2017	Intelligence and Security Services Act 2017 (Wet op de inlichtingen- en veiligheidsdiensten 2017).
Investigation-related	If it is not possible to specify the person, organisation or technical characteristic to whom or which the use of an investigatory power or data processing pertains, but this is carried out in a manner that is 'as target as possible' for the purpose of a current investigation assignment ensuing from the Integrated Intelligence and Security Services Order.
Investigation-related interception	Investigation-related interception is an investigatory power set out in Section 48 of the ISS Act 2017. This investigatory power has been formulated in a technology-independent manner and may allude to cable interception and the interception of satellite and radio communications, amongst other things.

JSCU	Joint Sigint Cyber Unit, a combined technical unit of AIVD and MIVD that focuses on the processing of sigint and cyber data.
Metadata	Data about communication. For example, telephone-call metadata include the telephone numbers in question, the start and end times of the call and the data from the mobile phone towers concerned.
Negative filter	The negative filter determines what will not be stored. If no criteria have been included in the filter, all data will be stored. The filter ensures that irrelevant data that are known/recognised in advance are not stored. This is done on the basis of characteristics.
Personal data	Data relating to an identifiable or identified individual natural person (e.g. a name or a photograph) (Section 1, preamble and (e), of the ISS Act 2017)
Positive filter	The positive filter determines what will be stored. The data to be stored are determined on the basis of characteristics. These characteristics include the selection criteria associated with Section 50 of the ISS Act 2017. For example, telephone numbers or e-mail addresses. If a characteristic matches with the intercepted data, the communication in question will be stored.
Provider	The communication service provider. The natural or legal person that, in the course of a profession or business, offers the users of its service the possibility to communicate aided by an automated device or system, or that processes or stores data for the purpose of such a service or the users of such a service.
Search	The exploration of communication as referred to in Section 49 of the ISS Act 2017. Search geared towards interception, regulated in Section 49(1), pertains to the determination of the characteristics and nature of telecommunication and the identity of the person or organisation associated with the communication. Search geared towards selection, regulated in Section 49(2), pertains to the identification and verification of selection criteria and to the identification of persons or organisations.
Security service	A service that conducts investigations into persons and organizations that potentially represent a threat to the continued existence of the democratic constitutional state, or to security or other vital interests of the State, or to the security and readiness of the armed forces
Sigint	Sigint stands for 'signals intelligence': information that is gathered by intercepting (electronic) signals.
Snapshots	Short integral recordings (interception) of the data streams available.
Special investigatory power	An investigatory power of the service which regulates the use of a specific method that infringes privacy and also lays down the circumstances and conditions under which the power may be exercised. Special investigatory powers are generally exercised in secret. The special investigatory powers are laid down in Sections 40 to 58 of the ISS Act 2017 (for example interception and observation). Some special investigatory powers are assessed by the Investigatory Powers Commission (TIB) on the lawfulness of the authorization granted by the minister

Specificity requirement	The requirement that special investigatory powers must be used in a manner that is 'as targeted as possible'.
Target	A person or organization that is being investigated by the AIVD or MIVD.
Technical characteristic	A characteristic that can be traced back to various elements of communication or telecommunication; for example a telephone number or an e-mail address.
Untargeted	If it is not possible to specify in advance the person, organisation or technical characteristics to whom or which the use of an investigator power or a data acquisition pertains.

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