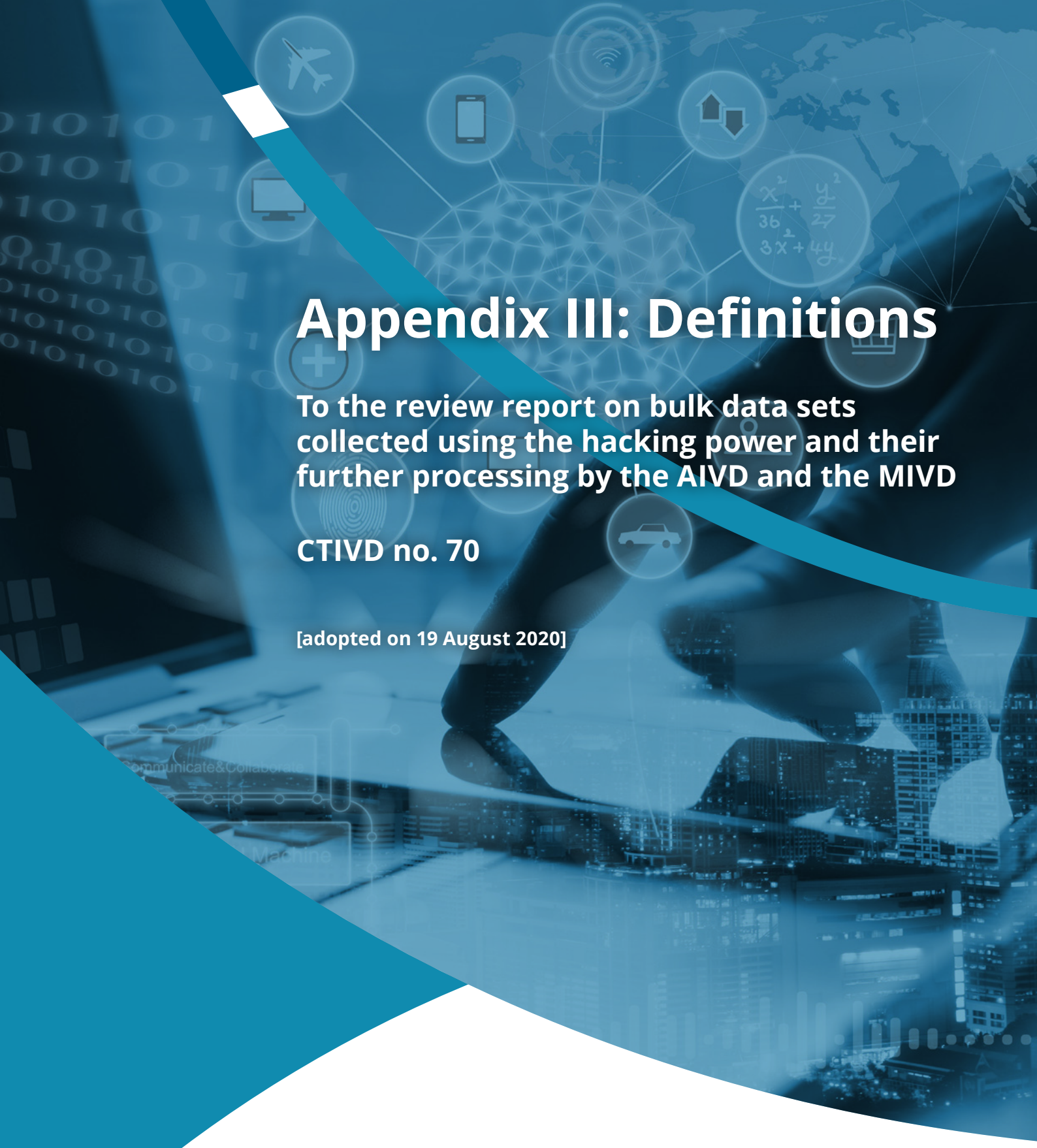

Appendix III: Definitions

To the review report on bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

CTIVD no. 70

[adopted on 19 August 2020]

CTIVD
Review Committee
on the Intelligence and
Security Services

CTIVD no 70

APPENDIX III

To the review report on bulk data sets collected using the hacking power and their further processing by the AIVD and the MIVD

Definitions

This list explains a number of terms used in the review report. In providing the descriptions, the CTIVD's aim was not completeness, but to try to give the reader as clear a picture as possible of the terms in question.

Authorization request	The document in which the request to use the hacking power is substantiated and which is submitted to the relevant minister for authorization.
Automated device or system	A device or group of interconnected or related devices, of which one or more automatically processes computer data using a program. Examples include computer systems, computer networks and smartphones.
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.
Bulk hack	The collection of a bulk data set using the hacking power.
Clean-up obligation	The legal best-efforts obligation to remove technical aids used in the exercise of the hacking power (specifically hacking into an automated device or system) (Section 45(7) of the ISS Act 2017).
CNE	Computer Network Exploitation. This term refers, in the context of the current investigation, to a department of the Joint Sigint Cyber Unit (JSCU), which is specialized in hacking automated devices or systems.
Division of job roles and tasks	Restricting access to data based on the job role or tasks of service staff members. This means that depending on the tasks assigned to a staff member's job role, that service staff member may gain access to certain data that is not accessible to others.
Due care	General requirement for data processing. Safeguarding the accuracy in terms of content and the correct reproduction of the data that is processed (Section 18(2) of the ISS Act 2017).

Failing	A point for improvement in the future. The established defect is not of such importance or severity that it has resulted in a decision of unlawful conduct (yet).
Fundamental rights	Basic rights set out in for example international treaties and defined in case law, such as the European Convention on Human Rights (ECHR). Examples of these rights include the right to respect for one's personal and family life (privacy), freedom of speech and the right to liberty and security.
Hacking power	This is a special investigatory power to explore and enter an automated device or system (Section 45 of the ISS Act 2017).
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.
Investigation-related interception	A special investigatory power to intercept any form of telecommunication or data transfer. It has been included in the ISS Act 2017 as a three-staged system: (1) interception by the Joint Sigint Cyber Unit (Section 48 of the ISS Act 2017), (2) the optimization of the interception and selection process (Section 49 of the ISS Act 2017) and (3) the analysis of the communication and metadata content (Section 50 of the ISS Act 2017).
ISS Act 2002	Intelligence and Security Services Act 2002. This Act expired with the introduction of the ISS Act 2017 on 1 May 2018.
ISS Act 2017	Intelligence and Security Services Act 2017. This Act entered into force on 1 May 2018.
JSCU	Joint Sigint Cyber Unit. The JSCU is the joint unit of the AIVD and the MIVD that processes data in the areas of signals intelligence (sigint) and cyber.
Log	A journal in which service staff manually record actions, assessments and events.
Logging	The systematic automated registration of data on the use and functioning of a computer program.
Necessity	General requirement for data processing. The act of processing must serve a certain objective and must contribute to the realization of that objective (Section 18(1) of the ISS Act 2017).
Non-target	Non-targets are not the subject of investigation by the services but have some sort of personal or business relationship with a target.
Operator	This term refers, in the context of the current investigation, to a specialized staff member from the Computer Network Exploitation department who is tasked with using the hacking power.
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.

Propriety	General requirement for data processing (Section 18(2) of the ISS Act 2017). One aspect of this is a weighting between the objective of the data processing and the negative impact on the persons or organizations whose data will be processed.
Record keeping	The legal obligation to keep a record of the use of an investigatory power, also referred to as reporting (Section 31 of the ISS Act 2017). This may be carried out in a number of ways.
Record obligation	The obligation for the AIVD and the MIVD to keep a transparent record of which data and data files are exchanged in the context of cooperative partnerships.
Relevance	Data is relevant if it has significance for the investigation for which it has been obtained or for any other ongoing investigation. When data is assessed for relevance, a substantive deliberation must be made "whether the data contributes in a positive sense to the investigation or whether that data could provide a negative response to certain questions, disprove hypotheses or otherwise be of crucial importance" (Section 27 of the ISS Act 2017).
Reporting	See under 'Record keeping'.
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.
Target	A person or organization that is being investigated by the AIVD or MIVD.
Technical characteristic	A feature that can be traced back to various elements of telecommunication, for example a telephone number or an email address. Technical characteristics can be used as a selection criterion.
TIB	The Investigatory Powers Commission, a body that assesses in advance whether the use of a number of special investigatory powers by the AIVD and the MIVD is lawful. The TIB's decision is binding.
Unlawful	An assessment of the AIVD or MIVD's conduct. An 'unlawful' assessment always means that the conduct conflicts with legislation and regulations. Legislation and regulations in this case refers to the ISS Act 2017, case law and the recommendations from previous review reports adopted by ministers. The assessment takes into account the nature of the interests infringed and the extent of the infringement.

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

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