Appendix I: Investigation plan and methodology

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]

Review Committee on the Intelligence and Security Services

CTIVD no. 70

APPENDIX I

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

Investigation plan and methodology

Investigation plan

In this appendix, the CTIVD explains the plan and methodology of the investigation into the collection of bulk data sets using the hacking power and their further processing by the AIVD and the MIVD.

The investigation covers the period from 1 May 2018, the date on which the ISS Act 2017 entered into force, to 1 November 2019.

With its investigation, the CTIVD answers the following investigative questions:

- *In the period investigated, did the AIVD and the MIVD lawfully use the hacking power when collecting bulk data sets ('bulk hacks')?*
- *In the period investigated, did the AIVD and the MIVD lawfully process the bulk data sets obtained by the hacking power?*

The first investigative question focuses on a number of elements in the use of the hacking power which are new in the ISS Act 2017. We distinguish the following subsidiary questions:

- *Did the collection of the bulk data sets using the hacking power in the investigation period take place based on authorization found to be lawful by the TIB?*
- *Have the technical risks that could occur when using the hacking power been described in the authorization requests in line with the real-life situation?*
- *Did the services comply with the clean-up obligation?*
- *Did the services keep records of the use of the hacking power?*

The second investigative question can be specified based on the following subsidiary questions:

- *How do the AIVD and the MIVD deal with the legal requirements relating to the relevance assessment under Section 27 of the ISS Act 2017?*
- *To what extent do the AIVD and the MIVD fulfil the procedural safeguards for the further processing of bulk data sets collected by a hack?*

Scope of the investigation

The investigative questions referred to above relate to different phases, i.e. collecting bulk data sets using the hacking power (Section 45 of the ISS Act 2017) on the one hand, and the further processing of that data by the AIVD and the MIVD on the other. The investigation focuses on the services' policy, work instructions and practice (i.e. the bulk hack operations conducted in the period investigated and the further processing of the data collected in that way). There are eleven operations approved by the TIB in the investigated period, in addition to four rejected operations. One operation was approved in the course of the investigation period and later, on extension, rejected in that same investigation period. The CTIVD identified these operations based on its own investigation and the information provided by both services. Although this investigation focuses on hacking operations that yielded a bulk data set, it does not mean that all hacking operations conducted or all available bulk data sets were included in the investigation.

Collection of data

As regards the investigative questions about the lawfulness of the use of the hacking power (collection phase) in practice, the CTIVD opted to divide the investigation into the new elements of Section 45 of the ISS Act 2017, more specifically:

- The authorization by the minister and the preceding lawfulness assessment by the TIB (subsection 3 in conjunction with Section 32). The assessment by the TIB is an important safeguard in the ISS Act 2017 for lawful use. The TIB assesses the necessity, proportionality, subsidiarity of the use of the hacking power and whether that use is as targeted as possible.
- Describing technical risks in the request for authorization including the use of unknown vulnerabilities (subsection 4). That also involves the internal assessment and recording of the risks.
- Compliance with the clean-up obligation when an operation has ended (subsection 7).

Furthermore, the investigation focuses, as regards the acquisition phase, on how the recommendation in report no 53 was followed up, i.e. keeping records on the exercise of the hacking power (now Section 31 of the ISS Act 2017), including automated logging.[1] The lawfulness assessment by the TIB as such is not part of this investigation.

Further processing

As regards the further processing of bulk data sets from the hacking power, the emphasis is on the procedural safeguards that apply to the accessibility of this data to the intelligence process. The legal starting point is the requirement to assess the data for relevance and the applicable retention period for doing so (pursuant to Section 27 of the ISS Act 2017). The CTIVD also looks at how the safeguards used by the services were executed. This includes looking at how the recommendations adopted by the ministers from report no. 55 were followed up. The current investigation did not examine how the data from the bulk data sets is used in the intelligence process. Nor did the CTIVD examine to what extent the bulk data sets actually are meaningful to the services' conducted investigations, or whether the infringement of fundamental rights outweighs the services' interests. This question is factored into the assessment and substantiation of the requirements of necessity and proportionality in the authorization requests and any extension requests which require a substantiation of the value of the data for the investigation.

1 CTIVD review report no. 53 (published in April 2017) on the use of the hacking power by the AIVD and the MIVD, *Parliamentary Documents II* 2016/17, 29 924, no. 149 (appendix), available at www.ctivd.nl.

Investigation method

The CTIVD drafted a legal assessment framework to be able to review the policy or work instructions and the practice of collecting bulk data sets using the hacking power and the safeguards on further processing. The framework has its foundations in the ISS Act 2017 as well as the Policy Rules, the parliamentary history, relevant case law, previous review reports and the recommendations adopted by the Minister of the Interior and Kingdom Relations and the Minister of Defence. Both services' internal policy was also taken into account when the framework was drafted. The assessment framework is included in Appendix II to the review report.

The CTIVD conducted a file investigation in which policy documents and work instructions were assessed. The CTIVD also examined which safeguards apply to accessing the bulk data for purposes of the intelligence process. The legal starting point is the requirement to assess the data for relevance and the applicable retention period for doing so (pursuant to Section 27 of the ISS Act 2017). In addition, the services use various safeguards.

Furthermore, all requests for authorization or extension for bulk hack operations in the investigation period were examined.

As part of the investigation, interviews were held with legal experts, policy officers and operational staff of both services. These interviews were held to obtain a more detailed picture of the services' conduct and work process and to validate the investigation results. Technical experts were also interviewed to aid the investigation of collecting, unlocking and further processing data.

In addition, the CTIVD itself also conducted a technical investigation into the services' systems. The cyber security expert of the CTIVD forms part of the investigation group for that reason. The CTIVD conducted a comprehensive technical examination of all bulk hack operations in the investigation period and assessed them on the points of lawful collection of bulk data sets, the description of technical risks, the recording of the clean-up obligation conducted (if applicable) and the presence of automated logging of the hacking power. In addition, in a number of operations which were taken as a sample, an in-depth investigation was carried out by way of a technical check. This probe looked in more detail at the quality and scope of the logging and the technical risks of the operations. The outcome on these points is a representative picture of the practice of bulk hacks carried out in the investigation period.

Duration

On 11 September 2019, the CTIVD announced it would conduct a lawfulness investigation into the application of the hacking power exercised by the AIVD and the MIVD when collecting bulk data sets.[2] The investigation concluded on 10 June 2020 when the draft review report was drawn up. The Minister of the Interior and Kingdom Relations and the Minister of Defence were given the opportunity to respond to the findings given in the review report. The responses of the Minister of the Interior and Kingdom Relations and the Minister of Defence were received on 14 August 2020. The review report was adopted on 19 August 2020.

2 See www.ctivd.nl.

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