Review Report

On the use of the investigatory power to hack by the AIVD and the MIVD in 2015

CTIVD no. 53

8 March 2017

Review Committee
on the Intelligence and
Security Services

Review Committee
on the Intelligence and
Security Services

CTIVD no. 53

REVIEW REPORT

On the use of the investigatory power to hack by the AIVD and the MIVD in 2015

Table of contents

Review Committee
on the Intelligence and
Security Services

CTIVD no. 53

SUMMARY

of the Review Report
on the use of the investigatory power to hack
by the AIVD and the MIVD in 2015

The AIVD and the MIVD have the legal (investigatory) power to "hack", that is, to break into computer systems. In this Review Report, the CTIVD finds that the AIVD and the MIVD in general use this power in a well-considered manner. Hacking is found to be an effective power: in most cases, it produced results that were in the interest of national security and could not have been obtained in any other way.

In the vast majority of the dozens of hacking operations reviewed that were conducted in 2015, the AIVD and the MIVD acted in accordance with the law. Overall, the services are aware of the seriousness of the interference with the rights and interests of the parties involved associated with the use of the hacking power. This first and foremost concerns the right to protection of privacy, but also the importance of safeguarding the integrity of IT systems.

However, shortcomings have been identified with respect to certain procedures. The most important of these is the structural failure by the services to destroy data at times they are obliged to do so. In addition, both services still fail to observe (non-statutory) retention periods for unevaluated data copied and stored during a hack, despite having promised the House of Representatives that they would do so. They also fail to destroy data that is found to be not relevant and data that has been unjustly processed. These omissions by the services are unlawful.

Shortcomings have also been identified concerning unknown vulnerabilities, the so-called "zero days". Both the procedure to be followed and the relevant assessments to be made when deciding whether to report such vulnerabilities have not been detailed and laid down by the AIVD. In addition, the assessments made are not centrally recorded, rendering both internal control and external review of these assessments difficult. This procedure is negligent.

The procedure for seeking authorisation to extend the use of the hacking power, too, is lacking. The way the administrative processes are organised means that the AIVD does not report the most recent state of affairs in the substantiation provided for the request to extend authorisation. This is negligent. The MIVD does not seek the Minister's authorisation for the extension. This means that it is possible for the course or the nature of the operation to change, over time, and to deviate from what the Minister had originally authorised. In one case, this was found to have been unlawful.

This Report also provides attention to several instances of unlawful conduct that were of an incidental nature. In a number of cases, the target and/or the computer systems to be hacked were described in overly general terms. In addition, the services acted outside of the scope of the authorisation granted to them in a limited number of cases. In one case, the MIVD provided unevaluated data to a foreign service without having received the required Ministerial authorisation.

Review Committee
on the Intelligence and
Security Services

CTIVD no. 53

REVIEW REPORT

On the use of the investigatory power to hack
by the AIVD and the MIVD in 2015

1 Introduction

The hacking power

The General Intelligence and Security Service (hereinafter: the "AIVD") and the Military Intelligence and Security Service (hereinafter: the "MIVD") are authorised to break into computer systems. This investigatory power is set out in Article 24 of the Intelligence and Security Services Act 2002 (ISS Act 2002). In the common parlance of both services and in the political arena, this power is referred to as the "hacking power". The CTIVD uses this term accordingly. Examples of hacking include breaking into a smartphone, an e-mail account, a laptop or a server. Investigatory powers such as hacking are generally used against so-called "targets" or "objects of investigation": persons or organisations subjected to an investigation by the services in the exercise of their security or intelligence task. In this Report, the CTIVD will use the term "target".

Background to the investigation

The hacking power has been addressed in previous CTIVD Reports, albeit within the context of a larger field of investigation, most significantly in Review Report no. 38 on the processing of telecommunications data by the AIVD and the MIVD and Review Report no. 39 on the investigative activities of the AIVD on social media. The findings in these Reports, as well as the ongoing technological and social developments resulting in personal information being increasingly more often digitally available, were cause for this more in-depth investigation.[1]

Scope of the investigation

On 17 March 2016, the CTIVD announced that it would perform an in-depth investigation into the AIVD and the MIVD's use of their hacking power.[2] The investigation focuses on both *physical hacks*, involving one of the services having (temporary) possession of the computer system, and *remote hacks*, involving the breaking into a system not directly physically available, for instance over the Internet. **The investigation focusses on the question whether the AIVD and the MIVD have, over the period under investigation (1 January 2015 through 17 March 2016), exercised their hacking power lawfully and with due care.**

[1] CTIVD Review Report no. 38 on the processing of telecommunications data by the AIVD and the MIVD, *Parliamentary Documents II* 2013/14, 29 924, no. 105 (appendix) and CTIVD Review Report no. 39 on the investigative activities of the AIVD on social media, *Parliamentary Documents II* 2013/2014, 29 924, no. 114 (appendix). Hereinafter referred to as: CTIVD Review Reports nos. 38 and 39.

[2] Cover letter, available for consultation on www.ctivd.nl

Methodology

Appendix I to this report provides an account of the methodology used in this investigation. Summarily put, an investigation took place of those hacking operations by the services started in the 2015 calendar year where the target systems had been successfully broken into prior to the start of this review investigation (17 March 2016). As the MIVD makes relatively little use of the hacking power, all successful MIVD operations conducted during the investigation period have been reviewed. A selection was made of all successful operations conducted by the AIVD, such on the basis of the specific facts and circumstances characterising those operations. This includes operations where the hacking power was used against certain specific (groups of) persons, such as persons entitled to professional privilege, non-targets and third parties, or operations where data was reproduced (copied and stored) in an untargeted manner (comprehensively). Those operations that, according to the AIVD, were particularly effective also made the selection.[3] This group was complemented by operations selected on the basis of the type of hack used (the modus operandi employed) and of the AIVD's areas of attention.

Assessment of practice and procedure

The legal assessment framework is detailed in Appendix II to this Report. Wherever applicable, this framework ties in with the currently pending ISS Act 20.. Bill, which is set to become the new Intelligence and Security Services Act. This Report will refer to the relevant rules of law for each Chapter or topic. Each practice was assessed on its lawfulness and adherence to the principle of due care on the basis of this framework. Where conduct was found to be *negligent*, this means that, while the reasons provided for the use of the hacking power were lacking, the CTIVD found, on the basis of its own further investigation, that the use of the hacking power met the requirements of necessity, proportionality and subsidiarity. A procedure is negligent if it contains legal shortcomings but the associated risks have not, or only hardly, manifested themselves. Conduct was found to be *unlawful* if it violated applicable legislation or if the reasons provided for the use of the hacking power were lacking to such a degree that this could not be remedied. In this connection, account is taken of the seriousness of the infringement and the nature of the interests of the parties involved that have been infringed upon.

The public Review Report and the secret Appendix

Wherever possible, a systemic approachwas chosen in this Report. This means that the CTIVD first considered policy, procedures and (standard) practices and next reviewed the individual operations selected. This systemic approach was effected most thoroughly in Chapter 2 (Overall view and effectiveness), Chapter 5 (Authorisation) and Chapter 7 (Copying, assessing and destroying data). In addition, and in accordance with the standard CTIVD procedure, all instances of unlawful and negligent conduct have been included in the public Review Report. For reasons of protecting national security, the specifics of a number of operations are detailed in the secret appendix. This secret appendix is of limited size (three pages' long).

Timeline of the investigation

The investigation concluded with the drafting of this Report, which was completed on 23 December 2016. The Ministers of the Interior and Kingdom Relations (hereinafter: "BZK") and Defence were given the opportunity to respond to the findings of this Review Report. The Minister of BZK's response came in on 24 February 2017 and the Minister of Defence's on 22 February 2017. These responses gave reason to conduct further consultations with the MIVD and to implement a couple of amendments. The Review Report was adopted on 8 March 2017.

[3] The basis of the selection is further detailed in Chapter 2 and Appendix I.

Structure of the Report

The Report is sequentially organised. This means that, following the section on the overall view (Chapter 2) and a short overview of the working process (Chapter 3), this Report reflects the sequence of this working process when addressing the various aspects of the use of the hacking power. Chapter 4 details the run-up to the use: the preliminary investigation and the drafting of the substantiation of the request for authorisation, both in general terms and with respect to certain special situations like the use of the hacking power against organisations, persons entitled to professional privilege, non-targets or third parties, or in case of later additions. Chapter 5 concerns the authorisation, Chapter 6 the performance of the hack and Chapter 7 further data processing. Chapter 8 discusses the provision of unevaluated data obtained through hacks. Finally, Chapters 9 and 10 provide the conclusions and recommendations of this Report.

2 Overall view and effectiveness

Overall view

The CTIVD finds that the AIVD and the MIVD as a rule act in a well-considered manner and in accordance with the law when exercising their hacking power. This is due, first, to the fact that the services are aware of the serious interference with the fundamental rights and interests of the parties involved that may result from exercising the hacking power. Such fundamental rights first and foremost concern the right to protection of privacy. The degree of interference with the private life of the parties involved is comparable to that associated with a search or interception of telecommunication. The protection of the integrity of IT systems, too, is a relevant interest in relation to the hacking power, as secure and reliable IT systems have become essential to the proper functioning of society. This integrity is primarily impacted by the act of breaking into the system itself, but also by inserting or sustaining vulnerabilities therein.

In addition, hacking is in practice very laborious and requires a great deal of expertise, while it does not always prove possible to gain access. These factors have resulted in the requirement that assessments be made prior to the actual use of the hacking power. This has led to a procedure that promotes the lawful use and exercise of the hacking power.

Effectiveness

One of the questions the CTIVD attempted to answer with this investigation is whether, and if so, to what degree, the hacking power is effective in terms of protecting the national security. This specifically concerns effectiveness within the meaning of the lawfulness review. If, in the general experience, a certain power is found to produce few relevant results, this may, in – similar – cases effect the question whether the infringement of the fundamental rights of the parties involved is in balance with the objective to be achieved by using it (proportionality).

No clear and unequivocal definition of effectiveness exists. We therefore asked the (various) teams of the services to provide their own definitions. What all responses had in common was that the hacking power was found to be effective, because it allows for obtaining large quantities of valuable information with a high degree of reliability, without giving rise to direct risk to natural persons (officers, informers). Once a computer system has been broken into, the specific information sought after can be selected and copied more precisely, thereby limiting the infringement of privacy.

The CTIVD’s investigation confirms this reasoning. One or more elements of this definition of effectiveness were identified in the majority of the operations reviewed. Certain operations were also found to be especially effective in the context of protecting national security. In those cases, the specific options available to the services by using the hacking power were decisive in producing the results. That is, these results could not have been obtained through the use of any other power. One example is the situation where two users communicate with each other using encrypted messages. Such communication which is encrypted during transition can generally not be rendered legible upon interception. The use of the hacking power provides a solution in such situations.

Unlawful conduct and negligent conduct

The finding that the hacking power was, as a rule, exercised effectively and lawfully over the investigation period does not, however, mean that no instances of unlawful conduct or negligent conduct were identified during the investigation. The – limited number of – structural shortcomings identified are generally caused by procedures used throughout the services that are found to be lacking. The incidental cases identified of unlawful conduct and negligent conduct have more diverse causes. Most such cases are the result of time pressure after gaining access or the lack of familiarity with the legal preconditions specifically applicable to the use of the hacking power.

3 The hacking power and the working process

The hacking power

"Hacking" concerns the breaking into a computer system. "Breaking into" means that the computer system is entered against the will of, and without authorisation from, the party that has title to it. A "computer system" is a device meant for the electronic storage, processing and transfer of data. The same definition as used in criminal law is applied here.[4] Devices not meeting these three cumulative conditions are not deemed to be computer systems by the legislature. This means that devices that only transfer or store data, such as simple telephones and USB sticks, respectively, are not deemed to be computer systems. Desktop computers and laptops are deemed to be computer systems, as are tablets and modern smartphones. The legislative history of the ISS Act 20.. provides that, in practice, hacking shall especially relate to the breaking into – stand-alone – computers and networks of computers, including servers.

The AIVD and the MIVD may only use their hacking power if, and to the extent, such is in the interest of national security required for the proper performance of their security or intelligence tasks. The intelligence task concerns conducting investigations into other countries and the potential and armed forces of foreign powers in the interest of the Dutch foreign and security policy or of the international legal order, or for the purpose of the proper composition and effective use of the armed forces. Such investigations are conducted by the AIVD, unless it concerns militarily relevant topics, in which case they are generally conducted by the MIVD. The security task concerns the recognition of threats to the continued existence of the democratic legal order or to the security or other compelling interests of the State (AIVD), or to the security and readiness of the armed forces (MIVD).

The working process

So as to represent the various topics addressed in this report, as well as the relations existing between them, a short summary of the working process followed by the services when using their hacking power is provided in the below. This description is based on the policy adopted by the services and the practical application identified during the investigation.

Both services have formal Mandate Regulations in force that determine the level of authorisation, for instance. The AIVD has also drawn up a number of policy documents for the operational teams, covering, *inter alia*, the level of authorisation and the joint exercise of different investigatory powers, as well as working instructions. During the investigation period, the MIVD had not adopted any policies or working instructions covering hacking for the operational teams.

Hacking operations are performed by the Joint Sigint Cyber Unit (hereinafter: the "JSCU"). The JSCU is a joint operations unit of the AIVD and the MIVD that is active in the field of Sigint and Cyber. As the JSCU, too, works in accordance with certain standard procedures, we are able to outline the following picture of the various stages of the working process.

[4] Refer to Section 80e of the Dutch Criminal Code. In the Computer Crime Act III, this definition is amended to conform with the (wider) definition as used in the Convention on Cybercrime. This definition is reproduced in the ISS Act 20... See also Appendix II, p. 6 and the CTIVD's View on the ISS Act 20.. Bill, Appendix II (November 2016), p. 10, available for consultation on www.ctivid.nl

The preliminary investigation (see also Chapter 4)

In almost all cases, the responsible operational teams of both the AIVD and the MIVD decide themselves whether to make use of the hacking power. The operational teams next consult with the JSCU on the technical feasibility of a hack. If a hack is found to be feasible, the JSCU next performs a so-called preliminary investigation.

The request for authorisation (see also Chapter 4)

If the decision is made to exercise the hacking power, the team drafts an extensive substantiation of its request for authorisation. The JSCU is involved with the drafting of those sections related to the technical side of the operation. As a rule, the request for authorisation is drafted by the processer (AIVD) or analyst (MIVD) of the operational team concerned.

Authorisation (see also Chapter 5)

AIVD

The request must be approved by the heads of the team and of the unit. If the hack concerned is a physical one, with the service – temporarily – having possession of the computer system, the operation can next be performed. Authorisation for a physical hack is granted for a single use of the power only. If the hack concerned is a remote one, i.e., if it takes place on a computer system outside the direct physical reach of the service, such as via the Internet, authorisation by the Director-General (the head) of the AIVD is required. Once the Director-General has approved the use of the power, the Legal Affairs department as a rule draws up a summary of the request. This summary is bundled with those of other requests once every three months and submitted to the Minister of BZK for authorisation. If there is urgency involved, the request is submitted to the Minister in its entirety or orally. Final authorisation for a remote hack is provided by the Minister. Authorisation for any extensions of remote hacking operations conducted by the AIVD, too, is granted by the Minister.

MIVD

The MIVD does not, in the authorisation procedure, differentiate between physical and remote hacks. All requests for authorisation drawn up are, upon having received approval from the team head, the head of bureau, the department head, the Legal Affairs Staff Department and the Director, submitted to the Legal Affairs Directorate and the Secretary-General of the Ministry of Defence for assessment, before being submitted in writing to the Minister of Defence. If the request for the use of the hacking power concerns places not being used by the Ministry of Defence, the authorisation of the Minister of BZK is required, as well. The Director of the MIVD is authorised to extend both physical and remote hacking operations.

Additions (see also Chapter 4)

So-called “additions” are other computer systems belonging to the same person or organisation that complement or substitute the computer systems referred to in the initial request for authorisation. The addition must meet the relevant criteria stated in the authorisation for the physical or remote hack. This means that new computer systems can be covered by the authorisation, without the Minister being requested to grant additional authorisation. Adding new systems is possible in the context of the so-called “broad” authorisation (for instance, because it cannot be determined in advance which computer systems are relevant to the investigation) or of requests related to as yet unknown members of an organisation and their computerised systems.

Within the AIVD, addition is approved internally, by the unit head. In case of an extension of the hacking operation, the Minister of BZK is informed about the computer systems added to the initial request.

Within the MIVD, the analyst concerned decides whether a computer system can be added under the initial charge. In practice, the analyst often consults with the head of the bureau and the Legal Affairs Staff Department before deciding on an addition. Additions are, next, also attached to the requests for extension submitted to the Director for approval.

The performance and the processing of data (see also Chapters 6 through 8)

Once authorisation at the right level is obtained, the JSCU can perform the hack. In general, the choices made and technical actions performed in the context of the hack are logged mainly by hand. When operational choices about the performance of the hack are made that relate to the substance of the operation and are important to the team, consultations with the team are held. Data obtained by way of the operation is made available to the team by the use of applications. The teams assess whether the information is relevant to their investigation. This data may, with due observance of the applicable legal rules, also be submitted to foreign services.

4 Drafting the request for authorisation

4.1 Preliminary investigation

Assessment framework (section 4.1, p. 9, of Appendix II):

- When performing the preliminary investigation for the purpose of breaking into a computer system, no knowledge may be acquired of the content of the data.

Findings

If the operational team is of the opinion that a hack is required, it consults with the JSCU on the technical feasibility of performing it. As a rule, the JSCU next performs a preliminary investigation. When performing this preliminary investigation, the JSCU provides an estimate of the required capacity and the technical feasibility (the odds of success). In this connection it also considers and assesses the possible risks, such as doing damage to IT systems and the threat of the hack being identified.

In principle, the computer system is not broken into during the preliminary investigation; instead, it is only assessed from the "outside" (the publicly accessible side). In some cases, a test is carried out with certain log-in details, to discover if they grant access to a computer system. While this so-called "validation of credentials" does formally constitute breaking into the computer system, the data stored on it is not accessed: the operational team only verifies if the credentials are correct. This practice is found to be both lawful and in accordance with the principles of due care. No situations have been identified where knowledge was obtained of the content of data during the preliminary investigation.

4.2 Requests for authorisation for the use of the hacking power in general

If the operation, in view of the results of the preliminary investigation and the importance to national security, has sufficient priority to be executed, the operational team drafts a request for authorisation. The request for authorisation provides the substantiation for the use of the hacking power. The provision of proper substantiation is important because it lays down, in a way that enables assessment, the considerations the services must by law make before exercising an investigatory power. It must state the necessity of the use of the power and answer the questions whether the infringement of the fundamental rights and interests of the parties involved are in balance with the objectives to be realised by the use (proportionality) and whether means or procedures of a less infringing nature could also be applied (subsidiarity), respectively.

The substantiation serves both an internal and an external interest. Internally, it serves as an important safeguard: providing this substantiation ensures that attention is paid to whether the use of the investigatory power is, in fact, necessary, proportional and in line with the requirement of subsidiarity. It also forces the author to consider the purpose of the investigatory power and the ways its use infringes on rights and interests. It is important in this connection that the party executing the hacking power (carrying out the hack) is often not the party conducting the operational investigation. So as to provide the party executing the power with sufficient steering and limitations, the substantiation must clearly state the concrete objective to be obtained by using the power and the scope of the authorisation to be granted.

The external function of the substantiation concerns the provision of information to all parties less familiar with the investigation in question, such as the Minister. The substantiation explains the facts and circumstances that have resulted in the request for authorisation. It allows both the hierarchically and politically responsible parties to assess whether the request can be granted as meeting the applicable legal preconditions. The party granting the authorisation may also attach further conditions – for example, with respect to the duration the powers can be used for or the degree to which it may infringe on rights and interests – before taking the responsibility for the use of the hacking power. In addition, the substantiation allows for the CTIVD to perform (external) oversight on the use of the powers.

Assessment framework (section 4.2, p. 10, of Appendix II):

- The request for authorisation must substantiate the persons or organisations and the computer systems the hacking power is to be used against and, as specifically as possible, state the objective to be realised by the use, as well as the information to be obtained by the use of the hacking power.

Findings

During the investigation period the AIVD availed of a simple working instruction on the drafting of a request for authorisation. In addition, the accompanying template used by the processers served as a guideline for incorporating the required elements in the request for authorisation. The MIVD did not use such working instructions. The requests submitted were based on requests that had previously been granted. As a rule, the necessity of the operation to be executed was explained extensively, attention also being paid to the proportionality and subsidiarity. In the opinion of the CTIVD, the MIVD's requests would benefit from being more succinct and better structured. It believes the formats – only developed after the end of the investigation period – to be a solid instrument to realise this.

The reviewed requests for authorisation, both of the AIVD and of the MIVD, were generally found to be sufficiently substantiated as concerns the necessity, proportionality and subsidiarity of the use of the powers. Both services in their (internal) requests for authorisation generally also state the computer systems and the persons or organisations the powers will be used against. A characteristic of the hacking power is that it is often impossible to state in advance which data will be discovered in the computer systems. In consequence, some of the initial requests for authorisation provide only an abstract overview of the information the services aimed to obtain. This overview was elaborated upon in the requests for an extension, by stating the developments and results of the operation.

4.3 The request for authorisation to use the hacking power against unknown persons or organisations

In some cases, the requests for authorisation fail to state the person or organisation the hacking power is used against. This may occur when the computer system to be hacked is known, yet the persons or organisations using it is not.

Assessment framework (section 4.2, p. 10, of Appendix II):

- If it is not possible to directly state the persons or organisations the hacking power will be used against, the service, once it has obtained the details of the users' identities, must immediately supplement the substantiation for the request for authorisation and notify the party granting the authorisation.

Findings
Both the AIVD and the MIVD in a number of cases started up operations to break into a computer system without its users being known to them. The services did sometimes have a suspicion, though. One example concerns an IP address used for a cyber attack known to the MIVD. In another case, the AIVD broke into an Internet account used for spreading Jihadist propaganda.

Despite the Ministers having previously committed[5] to separately informing the party granting the authorisation (the Minister or the Director) the moment the identity of the user becomes known, this did generally not occur. Further investigation has shown, however, that this identity was in each case considered in the assessment if that information was relevant for the decisions to be made in the further course of the operation. Nor have operations been identified that should have been halted once the identity became known but were not. The failure to provide immediate notification therefore did not result in situations where the operations were not, or no longer, necessary, proportional or in line with the requirement of subsidiarity. The procedure of the AIVD and the MIVD is therefore deemed to be negligent in this connection. The services are advised to bring their procedures in line with the commitment undertaken by the Ministers.

4.4 The request for authorisation to use the hacking power against unknown computer systems

It was found that both the AIVD and the MIVD submitted so-called "broad" requests for authorisation in which the persons and organisations were minutely specified, but the computer systems to be targeted were described in less detail.

> Assessment framework (section 4.2, p. 11, of Appendix II):
>
> - If it is not possible to have the request for authorisation directly relate to one or more specific computer systems, the service will supplement the request for authorisation by way of an addition once these become known, providing a substantiation.

Findings
Operations for which a broad authorisation has been granted can roughly be divided into two categories. The first concerns requests for authorisation for a physical hack and the one-off copying of the data present on those computer systems. The second concerns remote hacks that were aimed at identifying new computer systems linked to the same target, or which were likely to result in the discovery of such.

Physical hacks
For each of the requests for a physical hack, the suspicion existed that the specific targets possessed computer systems, but it was not wholly clear which computer systems, and how many, would be discovered. One example is the request for authorisation to hack all computer systems to be found at a certain location.

In view of the one-off nature and, thus, the generally short duration of the use of the powers, it is understandable that not all computer systems discovered during physical hacking operations are added to the request at a later time. However, in the majority of the reviewed operations, and in particular those performed by the AIVD, the computer systems discovered and broken into were not properly

[5] Assessment framework (section 4.2, p. 10 of Appendix II)

recorded. This information was often not registered in the designated systems in an unambiguous and/or accessible manner. The CTIVD's own investigation did not, however, identify cases where the authorisation granted was exceeded or that necessitated the performance of a further proportionality test in any other way. This lacking recording therefore constitutes negligent conduct. The services are advised to lay down the duty to record in a working instruction.

Remote hacks

The substantiation to requests for remote hacks usually explained why broad authorisation was sought. In general, the operations concerned related to situations where the threat level and/or the expected dynamics were such as to require the services to be able to act quickly and efficiently. Examples include operations in which there were indications that concrete violent action was imminent or where a target was intentionally frequently switching to new computer systems.

Both the AIVD and the MIVD have made use of this type of broad authorisation. They each time clearly specified the target in their substantiation, stating what information was aimed to be obtained by the operation. For an addition to be made, the system must be clearly linked to the target. This means that, in practice, the operations were sufficiently limited to lead to the conclusion that they were proportional as well as necessary and in line with the requirement of subsidiarity. The procedures of the AIVD and the MIVD are, therefore, deemed to be lawful in this regard.

Additions to broad authorisations

While the practice of adding newly identified linked computer systems is, in itself, lawful, it is still essential that a critical assessment is made in each case whether the addition is covered by the authorisation granted. If such is not the case, authorisation must separately be sought before a break-in is permissible.

AIVD

In a number of operations the AIVD added computer systems to previous requests where no broad authorisation was granted. In these cases, the initial request only referred to a specific computer system and not to computer systems yet to be identified. One example was an operation where a separate Internet account was added to the authorisation to hack a laptop belonging to the same target. In another operation, multiple e-mail accounts were added, even though authorisation had been requested for hacking one specific e-mail account only. In one case, the internal request for authorisation referred to the breaking into connected e-mail accounts as yet to be identified, but this phrase was not included in the summary of the request submitted to the Minister – and thus was also lacking in the Minister's authorisation.

While most additions were authorised by the Minister by way of the authorisation to extend the operation, the breaking into these computer systems prior to that authorisation was unlawful, as the service had, in doing so, exceeded the authorisation initially granted by the Minister.

MIVD

With respect to the MIVD, one operation was identified where broad authorisation was granted but the added computer systems belonging to third parties were not covered by the specification. After these computer systems had been broken into, they were added to the request by the analyst concerned, in consultation with the performer of the hack, such by way of amending the broad authorisation. This addition was authorised by the Director of the MIVD in the authorisation to extend the operation. The Minister was not informed of this. The MIVD acted unlawfully in this operation by exceeding the authorisation granted by the Minister. The CTIVD recommends that the MIVD, at any rate, set up a procedure where authorisation for an addition must be granted at a level that is hierarchically higher than that of the individual staff member, namely, at the level of the head of the bureau.

4.5 The request for authorisation to use the hacking power against organisations

As the law provides for conducting investigations into both persons and organisations, it is also possible to exercise investigatory powers against organisations. A distinction is made in this connection between "solid" and "fluid" organisations. A "solid" organisation is an organisation featuring a – more or less – fixed structure and staff composition, while a "fluid" organisation is more informal in terms of composition and time. Special requirements are set for the substantiation for the use of the hacking power against organisations.

Assessment framework (section 4.2.1, p. 11, of Appendix II):

- If the hacking power is used against an organisation or its members, the request for authorisation must substantiate why the term "organisation" is applicable and must state which category of members the hacking power may be used against, as well as the circumstances under which it will be used.

Use against solid organisations

More than applies to other powers, hacking is likely to be used against an organisation as a whole. Possible targets in this connection are organisations featuring a wholly independent infrastructure or network of computer systems relevant to the services' security or intelligence tasks. One example would be an official foundation involved in terrorist financing.

Findings

Both the AIVD and the MIVD have used the hacking power against this type of organisation. In the cases reviewed, the – substantiated – description clearly showed that the target was an organisation. In all cases, these clearly recognisable organisations became the subject of an investigation in connection with the proper exercise of the services' security or intelligence task.

The organisation concerned often possessed an extensive digital infrastructure that was, *a priori*, not or hardly transparent from the outside. The requests for authorisation therefore clearly detailed the information intended to be obtained and the computer systems, or parts thereof, that would (possibly) be found and would require investigation. Only after the systems were broken into was it possible to specify which parts of the systems were relevant for the services' purposes. Sufficient attention was provided in the substantiations for the extension of the operations to this further specification ("funnelling").

In those cases where the substantiation referred to specific persons or positions within the organisation, this was usually done to state which of the organisation's computer systems, or parts thereof, might contain information relevant in the context of the investigation. The positions listed were sufficiently specific for it to be clear which members of the organisation were referred to. These officials or positions were in each case relevant in the context of the security or intelligence task, either self-evidently so or as followed from the further substantiation.

The general procedure of the AIVD and the MIVD is deemed to be lawful in this connection. The scope of the use was in each case sufficiently limited by the connection to the target, specifically, the organisation concerned. When combined with the limitations to the use specified in the substantiations for the requests for extension, this means that the proportionality requirement was sufficiently taken account of during the operations. In the vast majority of the operations, the interest of national security outweighed the infringement of the fundamental rights and interests of the parties involved.

The scope of the use was found to be insufficiently limited in one operation conducted by the AIVD and two conducted by the MIVD. In all three cases, the description of the organisation was too abstract or the types or number of computer systems to be targeted were insufficiently clearly detailed. As the actual performance of the hacking operations did not exceed the acceptable limits, no use was in fact made of this – overly – broad authorisation, meaning that no unlawful infringement occurred in practice. For this reason, the conduct was not deemed to be unlawful, but negligent.

The nature of these organisations and the positions of its members are detailed in the secret appendix.

Use against fluid organisations

In addition to the use of the hacking power against clearly structured organisations, it can also be used against so-called "fluid" organisations. These organisations include (ever-changing) groups of supporters of an ideological movement who have united without having adopted a clear organisational or functional structure, for instance on a jihadist web forum.[6] Within the parameters of the present review investigation, only the AIVD has used the hacking power against this type of organisations.

Assessment framework (section 4.2.1, p. 11, of Appendix II):

- In the case of a fluid (informal)organisation, separate substantiation is required for the addition of a person.

Findings

The AIVD has used the hacking power against two fluid organisations. These organisations self-evidently constituted such. In addition to the clearly described roles or backgrounds persons could have to be deemed a member, the requests for authorisation stated that the power would also be used against "supporters who, in view of their actions, might in the future seek to join the organisation". The CTIVD finds that this is insufficient reason to be deemed to be a member of an organisation. Including such vague relationships in the request is negligent and promotes unlawful conduct.

It must be stated in this connection that the teams have noted that they, themselves, also believe this description to be too indistinct to deem a person a member. The CTIVD's own investigation showed that this approach was used when the hacking power was exercised: concrete indications existed for all persons added over the investigation period that they played a more substantial role, meaning that they could rightfully be deemed members of the organisation.

Additions

As is required in the context of fluid organisations, a separate substantiation for the use of the hacking power was provided for each member of the organisations later added. These substantiations stated the necessity, subsidiarity and proportionality for this use and, thus, met the applicable requirements. The authorisation was in each case granted at the level of the unit head, at the minimum.

In one case, there existed both indications and contraindications that the person in question was a member of the organisation. The CTIVD finds that if the link to the organisation is insufficiently clear, the person concerned may not be added to the request. An investigation to determine whether a person is a member of an organisation requires separate authorisation from the Minister. This means that the authorisation was, in this case, not granted at the proper level. The AIVD's conduct was therefore unlawful in this context.

[6] It may also occur that the organisation running the forum is as yet structured hierarchically, featuring some key persons who act as moderator and monitor compliance with the rules applicable within the forum.

4.6 The request for authorisation to use the hacking power against persons entitled to professional privilege

In its investigation the CTIVD provided particular attention to both the direct and indirect hacking of persons entitled to professional privilege. This concerns persons holding a position in society that involves confidentiality, in the sense that everyone must be able to communicate with these persons confidentially. Examples include doctors and lawyers. In view of this position, communications to and with these persons are more extensively protected.

Assessment framework (section 4.2.2, p. 13, of Appendix II):[7]

- When persons entitled to professional privilege are subjected to direct hacking, a strengthened proportionality test generally applies: significant operational interests that outweigh the right to professional privilege must exist in the specific case. Significant operational interests include, for example, situations where concrete indications exist that the national security is in direct danger. The authorisation is valid for no longer than one month.
- If it is likely, when performing an indirect hack against a person entitled to professional privilege, that the use of the hacking power would result in gaining access to information that the right of professional privilege applies to, the services must explicitly point this out in the substantiation for the request for authorisation and, where relevant, for extension.
- Writing out data that falls under the right of privilege, in the context of both direct and indirect hacks, is only authorised if the strengthened proportionality test is met. Evidence that this is so must be submitted in writing. The head of the team (AIVD) or of the bureau (MIVD) must be involved in this assessment and must grant their approval to the writing out of such data.
- Reproduced (copied) data that falls under the right of privilege and that fails to meet the strengthened proportionality test must be immediately removed and destroyed.

Findings

The CTIVD did not find any unlawful or negligent conduct in its investigation of the AIVD and the MIVD's direct use of their hacking power against persons entitled to professional privilege, or the substantiation thereof. The same applies to cases of indirect hacking where it was, in advance, foreseeable that the operation might result in gaining access into communications and data protected under the right of professional privilege. No communications protected under the right of professional privilege derived from hacks were found in the services' systems used to store information considered to be relevant. This means that no indications exist that communications and data protected under the right of professional privilege derived from hacks were used in the operational process.

[7] On 1 January 2016, the Temporary Regulation for the Independent Assessment of the Use of Investigatory Powers under the ISS Act 2002 against Lawyers and Journalists entered into force. Pursuant to this Scheme, the Minister's authorisation to (also) use the hacking power against lawyers and journalists, to the extent such use is made for reasons of identifying the source of information, must also be submitted to the Temporary Assessment Committee for its advisory opinion. This situation has not occurred during the hacking operations reviewed and will therefore not be considered in this Report, which primarily concerns the use and extensions in the year 2015. In addition, a uniform assessment criterion applicable to all persons entitled to professional privilege was opted for. For the specific criterion applicable to lawyers and journalists, refer to Report No. 52 on the use of investigatory powers against lawyers and journalists.

4.7 The request for authorisation to use the hacking power against non-targets

In its investigation the CTIVD also paid particular attention to hacks of the computer systems of non-targets. Non-targets are generally persons from a target's (direct) environment, such as family, friends or acquaintances. These persons are not, themselves, the subject of an investigation by the services, but the use of the powers is directed at them. Their communications, information positions or actions are analysed in an attempt to obtain information on the target, such as the target's place of residence.

Assessment framework (section 4.2.3, p. 14, of Appendix II):

- The substantiation of the request for authorisation must show that the hack will be performed on a non-target.
- A strengthened proportionality test applies to the hacking of non-targets: significant operational interests that outweigh the protection of the fundamental rights and interests of the non-target must exit. Significant operational interests include, for example, situations where one or more concrete indications exist that the ultimate target poses a direct danger to the national security. This assessment of interests must be reflected in the substantiation for the request for authorisation and for any extensions.
- Data that does not, or cannot, provide further information about the target will not be written out. The existence of this precondition must also become evident from the request for authorisation.[8]

Findings

The MIVD did not perform any hacks on non-targets over the investigation period. The AIVD did so in a limited number of cases only. Generally speaking, in each case concrete signs existed that the ultimate target posed a direct danger to national security, while it was not possible for the services to obtain intelligence on this danger by directly investigating the target. Examples include investigations into persons leaving for or (possibly) returning from Jihadist conflict zones in cases where the services had no other leads for conducting the investigation than the contacts these targets had with the persons in their surroundings.

In three hacking operations performed against a non-target there was no question of direct danger, but of an otherwise legally relevant significant operational interest. Each of the requests for authorisation to conduct these operations provided reasons why significant operational interests with respect to national security existed. In each case, the substantiation addressed the need to obtain intelligence reflecting the urgent operational necessity of possessing the information concerned. It explained to which parts of the organisation and to which (types of) operations the access to this information was crucial. In addition, the limited risks to the parties involved and the degree to which the integrity of the systems of the parties involved would be impacted was extensively addressed. The operational interests in obtaining access to the data were sufficiently significant to justify the infringement of the fundamental rights and interests of the parties involved.

The nature and background of these significant operational interests is further detailed in the secret appendix.

[8] Data not relevant to the security and intelligence tasks must be removed and destroyed. This (general) data processing condition will be addressed in Chapter 7.

In almost all cases, the fact that the computer system to be broken into belonged to a non-target was sufficiently clearly stated. The information the operational team was searching for and the conditions for this information to be written out – albeit abstractly phrased in some cases – were also provided. The investigation into the exercise of the hacking power showed that the systems the services use to store relevant information only contained data related to the target, or to the investigation into the target.

With respect to one operation, the substantiation only implicitly stated that the hack was to be performed on a non-target, while it was insufficiently clear that the hack was to be performed exclusively to obtain a better image of the target. So as to prevent the parties granting the authorisation, including the Minister, and the parties performing the hack from misunderstanding the request, this should have been stated explicitly. Further investigation has shown that the required assessment of interests did take place internally, within the team, and that only data related to the ultimate target and the investigation into this target had been written out. This operation did not, therefore, result in unjustified infringements. The lack of an explicit mention of the objective of the operation in the request for authorisation is therefore deemed to be negligent instead of unlawful.

4.8 The request for authorisation to use the hacking power against third parties

Third parties, too, may be subjected to hacking by the services. In contrast to non-targets, third parties are not themselves the object of an operation, but merely a means to get to the target. The use of the hacking power is not directed at them. In accordance with the ISS Act 20.. and the explanation thereto, "third parties" are defined as technically related parties whose computer systems are used to break into the computer system of the target. The services may, for instance, use the computer system of a third party as a sort of "stepping stone" to the computer system of the target, for example by using a network connection existing between both systems. In addition, the services may also hack a computer system of a third party on which technical data is stored that can be used to break into the computer system of the target, such as an IP address or password. In its View on the ISS Act 20.., the CTIVD noted that the assessment framework referred to in the below should be applied and incorporated in the new Act.[9]

Assessment framework (section 4.2.4, p. 15, of Appendix II):

- A strengthened subsidiarity test applies to breaking into the computer system of a third party for the purposes of breaking into the computer system of the target. A break-in of the computer system of the third party is permissible only if and to the extent this is required for breaking into the system of the target: no other realistic option may be available. All such must be evidenced by the substantiation of the request for authorisation.
- If any data of the third party is copied that neither relates to the breaking into the computer system of the target nor is relevant to the investigation in the context of which it was obtained, such data may not be written out.[10]

[9] The CTIVD's View on the ISS Act 20.. Bill, Appendix I (November 2016) , p. 29-30, available on www.ctivd.nl

[10] In addition, such data must be removed and destroyed. This data processing condition will be addressed in Chapter 6.

Findings

Both the AIVD and the MIVD have hacked computer systems of third parties for reasons of ultimately breaking into those of targets during the period covered by this Report. Hacking by way of the computer system of a third party took place to a limited extent and only following a substantiated assessment of the interests at play. In contrast to the concerns often expressed in the responses to the ISS Act 20.., none of these third parties were individual citizens.

In all investigations reviewed, the JSCU first performed a preliminary investigation to determine the feasibility and possible risks of a direct hack of the target. Only when such was found to be impossible or difficult to realise, for instance because a direct hack would require the use of exceptionally disproportionate capacity or would entail major risks, the services used the computer system of a third party to do so. Such risks include the process to break through complex security taking (too) long, the real likelihood that a direct hack would cause system damage, or the realistic expectation that the hack would be identified.

In some cases, the computer system of the third party was used as a stepping stone only. In other cases, data was also copied. In those cases where data was copied during the hack, this in all cases concerned data required to break into the ultimate target's system. In a couple of cases, data was copied from stepping-stone systems. This concerned data the substance of which was relevant to the investigation into the target and that was stored both technically and factually in the target's environment. Having assessed these hacks in terms of their being unavoidable, the CTIVD is of the opinion that the AIVD and the MIVD acted lawfully when breaking into the computer systems of third parties.

5 Authorisation

Before the hacking power may be used, the request for authorisation must be granted at the proper level.

Initial requests for authorisation

Assessment framework (section 4.3, p. 17, of Appendix II):

- Requests for authorisation submitted by the AIVD must be granted by the Minister in case of a remote hack and by the Director involved in case of a physical hack.
- Requests for authorisation submitted by the MIVD must be granted by the Minister in case of both remote and physical hacks.

Findings

Lawfulness is promoted by having the power to grant authorisation for the initial use of the hacking power be vested at the highest possible level – i.e., by the Minister – in almost all cases, as this does justice to the fact that a hack may constitute a serious infringement of the fundamental rights and interests of the parties involved.

Only in the case of physical hacks performed by the AIVD is authorisation by a Director deemed to suffice. The requests for authorisation in these cases are not submitted to the Minister. Even though this procedure is not contrary to the law and has not resulted in unlawful conduct in practice, the arguments presented by the AIVD to have authorisation for physical hacks be granted at a lower level is not convincing. While the one-off nature of a physical hack does provide a certain limitation, this does not mean that the use of this power is less of an infringement of the fundamental rights and interests of the parties involved. On the contrary: during its investigations, the CTIVD discovered operations where the infringement of rights and interests were at least comparable in nature and scope to that associated with remote hacks. The CTIVD therefore recommends that the AIVD, in anticipation of the ISS Act 20.., has the Minister decide on all requests for authorisation to perform hacks.

Requests for extension of authorisation

Assessment framework (section 4.3, p. 17, of Appendix II):

- Requests for extension of the authorisation for remote hacks submitted by the AIVD must be granted by the Minister.
- Requests for extension of the authorisation for remote hacks submitted by the MIVD must be granted by a Director or substitute Director.

Findings

In addition to having reviewed all initial requests for authorisation, the CTIVD also reviewed the requests for extension of the selected hacking operations. It finds that both the AIVD and the MIVD provide sufficient attention to the necessity, proportionality and subsidiarity of the extension, stating the possible results. However, some criticism can be levied against both the AIVD and the MIVD with respect to the procedures used when extending hacking operations.

AIVD

The AIVD's administrative process is structured in such a way as to submit the requests for extension of the authorisation for the use of hacking powers to the Minister in combination with all other requests for the (extension of the) use of investigatory powers in ongoing investigations, wherever possible. In practice, this means that the Minister is provided with a bundle of all requests – including for extensions of the use of the hacking power – that have been very briefly summarised by the Legal Affairs Department once every three months. So as to be able to have all requests summarised and bundled in time, the Legal Affairs Department has set a term within which the requests must be submitted to it. The deadline is set some six weeks prior to the start date of the extensions.

This procedure means that the teams are forced to submit a request for extension only shortly after having drafted the initial request for authorisation. At that stage, the hacking operation has only recently been started up and has usually not produced any results. In practice, this means that the substantiation provided for the extension is nearly identical to that for the initial request. If the teams were required to draft a request for extension only shortly before the lapse of the authorisation – which is granted for a term of three months – such would result in requests that are more properly substantiated than is currently the case. For, at that time, more information will be available on the results of the hack in question, allowing for focusing the substantiation for the extension accordingly. At the moment, the first extension has very little added value as concerns its substance, meaning that the Minister is provided with a request that has only limited substantiation. As a result, the Minster is, in principle, provided with insufficient information to be able to decide on the request for extension, which may cause unlawful conduct. Incidentally, no concrete cases of unlawful conduct have actually been discovered.

This procedure is negligent. The CTIVD recommends that the procedure is revised in such a fashion as to ensure that the substance of the requests for extension of the authorisation is as current as is reasonably possible. Incidentally, the AIVD has let the CTIVD know that the procedure is currently being reviewed.

MIVD

The MIVD does not submit the requests for extension to the Minister, but to the Director. The MIVD's administrative process with respect to extension is structured so as to provide the Director with the full request. The MIVD's administrative process also allows for including the latest information on the course and results of the operation in the request at a relatively late point prior to submission. By submitting the full request to the Director, the latter is able to become familiar with all facts and circumstances on which the request is based. This means that the authorisation cannot deviate from the substance of the request for extension. This procedure is in line with the principle of due care.

The decision of the MIVD not to submit the extensions to the Minister is, formally, not contrary to the law or the Mandate Regulations. Nonetheless, this practice does give rise to unlawful conduct. For, while the objective of the operations may not change during the process, the ways used to achieve this objective may. This means that it is possible for the course, nature or focus of the operation to change, over time, and to deviate from what the Minister had originally authorised.

In the opinion of the CTIVD, the changes made to the course of one operation were significant enough that they should have been submitted to the Minister (at the time the extension was requested), as this would have allowed the Minister to reassess the consequences thereof to the subsidiarity and proportionality of the operations and to decide whether authorisation was (still) justified. The CTIVD therefore recommends that the MIVD, in anticipation of the ISS Act 20.., amend the Mandate Regulations and/or its policy in such a fashion as to ensure that all requests for extension of hacking operations are submitted to the Minister.

6 Execution

The execution

Once authorisation has been granted at the proper level, the JSCU staff can perform the hack. Any description of the method used to perform the hack by definition affects the interest of national security, as it would provide insight into the modus operandi of the services. The CTIVD therefore only provides some generalised findings in this Report.

Findings

As a rule, the progress of the (technical) performance of a hack is individually and manually logged by the JSCU staff member involved. When the further performance of the hack requires operational knowledge, the JSCU consults with the operational team. The operational team manually keeps a log, stating how it assists the performer and which information it has obtained from the performer over the course of the operation. The (internal) monitoring of the performance relies mainly on the accuracy of the reports made by the JSCU and operational team staff. This would not be necessary if a continuous, automated and comprehensive log of the data on the performance and the technical actions carried out in the context of a hack would be kept. By analogy with the Computer Crime Act III Bill, it is necessary to provide for automatised logging in the future for reasons of having the exercise of the hacking power become fully transparent and objectively verifiable.

Vulnerabilities

So as to break into that part of a computer system that is not publicly accessible, some form of security must always be breached. Vulnerabilities existing in the computer system may be used for this purpose. This means that paths of entry not or only insufficiently blocked by the security of the system are capitalised on. Such openings can be inherent to the system or created by the party breaking into the system. The use of vulnerabilities was the subject of extensive discussion during the parliamentary debate.[11] Particular attention was provided in this connection to the use of vulnerabilities that are unknown to the general public and the manufacturer: the so-called “zero days” or “unknown vulnerabilities”.

Assessment framework (section 3.3, p. 7, of Appendix II):

- The AIVD and the MIVD must inform the interested parties about any unknown vulnerabilities discovered, unless legal or operational reasons (temporarily) prevent such. In deciding on whether to report such vulnerabilities, the justified interests of the services must be balanced against the risks of the continued existence of the vulnerabilities for all Internet users.

[11] For the locations of the parliamentary documents, refer to: Assessment framework, p. 7, of Appendix II

Findings

Performing a hack always involves searching for a certain vulnerability in the computer system to be hacked. In many cases, this concerns a vulnerability that has already been made public. In a number of cases, an unknown vulnerability is exploited. This vulnerability may be discovered by the hackers themselves, but information about its existence may also have been purchased. In addition, it is possible to purchase malware that works by exploiting (unknown) vulnerabilities.

The use of (unknown) vulnerabilities is further addressed in the secret appendix.

In principle, unknown vulnerabilities should be reported on the basis of the *Responsible Disclosure* Policy as laid down by the NCSC.[12] If an unknown vulnerability is identified during a hack, the JSCU staff – individually or in mutual consultation – balance the danger of the continued existence of the vulnerability against the operational and the legal reasons for not reporting it. For both types of reasons, this includes the protection of the current level of knowledge, a procedure, or sources. Attention should be provided in this assessment to whether the vulnerabilities exist in products commonly used by private individuals and businesses, or by the Dutch government. If so, the interested parties will be informed sooner. During the investigation period, no parties were so informed. This occurred once prior to that period.

The procedure to be followed by the JSCU in this connection is not laid down, however. In addition, the relevant considerations to be made have not been further specified or elaborated in internal policy. Nor were the results of the assessment centrally recorded. In practice, therefore, the decision on whether or not to report unknown vulnerabilities strongly depends on the considerations by the individual JSCU staff member, with little internal control and external oversight being possible of this assessment. It may also occur that vulnerabilities are not reported even after the operational interest in keeping them unknown has lapsed or become smaller. This procedure is negligent. Incidentally, in this review investigation the CTIVD did not identify any operations where the interested parties should, in its opinion, have been informed.

The JSCU, and therefore both the AIVD and the MIVD, are advised to develop policy and procedures specifying and laying down the relevant considerations deciding whether or not to inform interested parties about any unknown vulnerabilities discovered. In addition, the unknown vulnerabilities discovered and the assessment made with respect to them must be (centrally) recorded. A regular assessment term must be laid down for unknown vulnerabilities that have not been reported, by which time a reassessment must be made of whether the operational interest still prevails, if such is still expedient.

[12] The practice of the responsible disclosure of security breaches identified. The policy calls for agreements that usually entail the reporter not sharing information on the breach discovered with third parties until it has been remedied and the affected party not taking legal action against the reporter. More information is available on www.ncsc.nl

7 Reproducing, assessing and destroying data

The previous chapters detailed how the hacking power is used, and against whom, providing particular attention to special categories of persons and/or organisations so affected. It was also noted that the data present on the hacked computer systems is copied and stored on the AIVD and the MIVD's systems (the reproduction of data). This Chapter uses a system oversight approach to detail the organisation of the process used by the services to assess the relevance of such data. This includes addressing how methods of separation of functions and compartmentalisation are employed in connection with observing the need-to-know restrictions applicable to the operational process and how data that has been found, during processing, to not or no longer be relevant, or that have not been assessed at all, are stored and destroyed. One consequence of this approach is that the conclusions and recommendations mainly relate to amending and/or implementing (computerised) procedures.

7.1 Reproducing data

The hacking power is used with the goal of obtaining information relevant to the services' security and intelligence tasks. This goal is achieved by reproducing data from the hacked computer systems, i.e., by copying data from these systems and storing it on the services' systems. Such reproduction of data is a power explicitly conferred by Article 24 of the ISS Act 2002.

Assessment framework (section 5.1, pp. 17-18, of Appendix II):

- A strengthened proportionality test applies to the untargeted reproduction of data: the operational interests must outweigh the interest of protecting the fundamental rights and interests of, in particular, those persons or organisations whose information is present in the data and who are not the services' target. Significant operational interests include, for example, situations where one or more concrete indications exist that the national security is in direct danger. This assessment of interests must be reflected in the substantiation for the request for authorisation and for any extensions.

Findings

The data reproduced as a consequence of the use of the hacking power is not registered as such. So as to safeguard the traceability of the origin and the method used to reproduce the data, the process of reproducing the data, too, must be comprehensively logged. This would also allow for effecting (internal) oversight of this process. Despite the lack of logs, a general overview can be obtained of how the selection of the data to be reproduced (copied) takes place in practice on the basis of the manual records and further investigation. This overview shows a differentiation between a targeted and an untargeted method, both of which are applied as such in practice by the services. These two reproduction methods are further detailed in the below.

The targeted reproduction of data

In some cases, it is possible to copy only that information that is of interest to the operational team. An example would be only copying some specific messages requested by the operational team from an e-mail account. However, in many cases, the available security does not allow for only reproducing the data relevant to the investigation, in view of the activities and manipulations that are in this connection to be performed in the computer systems broken into. In addition, the JSCU staff member performing the hack often lacks sufficient operational knowledge to determine which information the operational team is specifically looking for. In the vast majority of cases, therefore, a *rough selection* is made of the data to be reproduced that may be relevant to the investigation, sometimes in consultation with the team. One example of such a selection is only copying the files belonging to the target from a laptop that is also used by flatmates. Another is the copying of all messages in an e-mail account exclusively used by a target. The CTIVD considers this practicable and lawful procedure to be sufficiently focused on obtaining selected data that it deems it to constitute targeted reproduction.

The untargeted reproduction of data
In principle, the reproduction of data must be as targeted as is reasonably possible. However, in some situations, data is reproduced *comprehensively* (in bulk). In those cases, it is impossible to determine in advance which data in the computer system can be related to the target and/or the investigation, or might be possibly relevant in this connection. In these operations it is, however, often clear in advance that the vast majority of the data to be comprehensively reproduced relates to persons and/or organisations that are *not* the targets of the services. Examples include a general web forum on which persons communicate who are suspected of preparing terrorist attacks, or reproducing all the data on an entire e-mail server which includes e-mail accounts that are used to commit a cyber attack.

The AIVD effected the untargeted reproduction of data in two operations, the MIVD in one. In all cases, it was not reasonably possible to reproduce the data in a more targeted fashion. In each case, a direct threat to national security existed – specifically, the threat of a terrorist attack and a cyber attack – that necessitated reproducing the data. The interest of national security prevailed over the interest of protecting the fundamental rights and interests of the persons or organisations whose information is present in the data and who are not the services' target. These operations were therefore found to be lawful.

These operations are further detailed in the secret appendix.

7.2 Making unevaluated data available for the operational process

As was shown in the foregoing, the data has, at the moment it is reproduced, not been assessed on its relevance to the security and intelligence task. This means it constitutes unevaluated data. So as to assess the unevaluated data on its relevance, it must be made available to the operational teams. To have the associated infringement of the fundamental rights and interests of the parties involved remain within tolerable limits, access to this unevaluated data must be subject to further conditions.

Assessment framework (section 5.2, p. 18, of Appendix II):

- The services must observe the condition that staff only has access to such unevaluated data to the extent required for the proper performance of the duties assigned to them (need-to-know).
- If the unevaluated data has been untargetedly reproduced and (is expected to) mainly concern data not relevant to the proper performance of the services' tasks, the additional condition of the separation of functions and/or duties must also be applied. This precondition must become evident from the request for authorisation.

Findings

Authorisation for access to unevaluated data
The JSCU as a rule makes use of AIVD systems also available to the MIVD to make the unevaluated data available to the operational teams. These internal systems are protected, placed behind walls and not accessible to (internal) third parties. In the vast majority of cases, that data is stored in applications

(software) already present on these systems. For some operations, new applications or methods are developed to allow access to the data in a specific case.

Operational team staff must possess prior authorisation to have access to these applications. Within the AIVD, such authorisation is granted by the head of the team and, within the MIVD, by or on behalf of the head of the department. In practice, this means that access to an application and the data stored therein is granted only to those staff requiring such to perform their work. This generally concerns the processers or analysts who had requested the hacking operation.

Some applications allow for the data to be searched by members of other operational teams on a "hit/ no hit" system basis: the staff member concerned is informed only of the fact that certain data may contain relevant information and must request authorisation for the use of this data via the regular channels. Certain applications allow an individual member of staff using certain unevaluated data – who, in practice, is generally a processer or analyst – to authorise other staff, including members of other operational teams.

In principle, these procedures form an implementation of the need-to-know requirement that accords to the principle of due care. For, as is the case in connection with the conditions in place for the use of other investigatory powers, the unevaluated data is accessible only to those members of staff charged with assessing its relevance. This is similar to the procedure in place with respect to the power of targeted interception (e.g., telephone tapping), by which the operational team members involved have access to all unevaluated conversations recorded for reasons of assessing them for their relevance.

The CTIVD is, however, critical of those cases where authorisation for the use of certain unevaluated data can be granted at the level of the individual staff member. In view of the importance attached to the need-to-know condition when working with unevaluated data, it is recommended that the power to grant authorisation is, in such cases, vested at a higher level, specifically, that of the head of the team or bureau.

Separation of functions and duties with respect to reproduced unevaluated data
By analogy with the conditions for the use of untargetedly intercepted data (satellite communications), additional internal procedures for the separation of functions and duties must be followed in the context of data deriving from a hack that has been untargetedly reproduced, such in addition to the requirement that proper authorisation is granted. These procedures must prevent, to the extent possible, that information from or on persons or organisations that are not targets enter the operational process.

Within the AIVD, only a small number of JSCU technical managers and specialists have full access to all untargetedly reproduced data. While the processers of the team requesting the hack are authorised for limited access to the data, this authorisation does not include direct access. The application (software) used to provide processers with access to the data works on a search and query basis. Data with respect to persons or organisations not related to the investigation concerned can therefore not be used in the operational process. These preconditions set to the use of the data are also, albeit abstractly, stated in the requests for authorisation. The AIVD has therefore implemented the preconditions of the separation of functions and tasks with respect to the use of untargetedly reproduced data deriving from a hack in accordance with the principle of due care.

Within the MIVD, the untargetedly reproduced data is assessed as to its relevance by the JSCU on the instructions of the analysts of the operational team. Only that data that is (possibly) relevant to the investigation is reported to the team. As a result of this procedure, a technical separation exists between the systems used by the JSCU to store unevaluated data and the systems used by the MIVD to store relevant data. This separation prevents the MIVD operational teams from using all of the untargetedly reproduced data. However, this lawful procedure is not mentioned in the request for authorisation, or for the extension thereof, as a precondition. The CTIVD finds this to be negligent.

7.3 Assessing, storing and destroying data

Assessment framework (section 5.3, pp. 18-19, of Appendix II):

- The writing out of data is permissible only if it has been deemed to be relevant for the investigation in connection with which it has been reproduced or in the context of another ongoing investigation conducted in the performance of the security or intelligence task.
- Data deemed not to be relevant must be immediately removed and destroyed.
- Data that has been deemed to be relevant at any point in time but has been processed erroneously or – with the passage of time – has lost its relevance, must immediately be removed and destroyed, unless the regulations on storing data prevent such.

Findings

Not all data stored in the applications is assessed as to its relevance by the operational teams. The significant amount of data available means that, in general, it is more efficient to simply use search terms and only assess the results produced on their relevance. Data that is deemed to be evidently relevant is generally exported to the appropriate systems. In the systems used to store data found to be relevant, no data deriving from a hack has been identified that should not have been deemed as such at the moment the assessment was made.

The CTIVD found that neither the AIVD nor the MIVD have any policy – let alone procedures – in force to remove and destroy the collected data, either immediately or after the lapse of some term. This applies both to data derived from hacks that has been assessed as to its relevance at some point and to such data that has not been assessed at all.

For this last category, the unevaluated data, no retention periods are in force at all. This means that all data that has not been assessed is kept. The same applies to data derived from non-targets, third parties and untargetedly reproduced data. This practice is contrary to the promise made by the Minister of BZK to the House of Representatives in 2014 to, in the run-up to the new Act (ISS Act 20..), establish (extralegal) retention periods.[13]

Erroneously processed data is not destroyed, either. For instance, during one operation by the AIVD, the operational team at one point found that two hacked e-mail accounts did not belong to the target. Upon this discovery, the team immediately requested the JSCU to stop the operation. The JSCU was not requested to destroy the data, which, consequently, did not happen. Data derived from these e-mail accounts was also retained in the systems containing relevant information. The AIVD acted unlawfully in this operation (Article 43(2) of the ISS Act 2002).

In one operation conducted by the MIVD the hack was continued while the authorisation for the operation had not been extended. The moment the MIVD discovered this, the JSCU was immediately requested to stop the operation. The log of this operation states that the MIVD did not access this data. However, the JSCU was not requested to destroy it. This data, too, is still available in the JSCU systems. This constitutes unlawful conduct by the MIVD (Article 43(2) of the ISS Act 2002).

[13] In response to Review Report 38, refer to Assessment framework, p. 19, of Appendix II

The failure by both services to have a procedure and practice in force for the destruction of data, including the failure to immediately destroy not relevant and erroneously processed data is unreservedly unlawful. Specifically with respect to the AIVD, this failure is compounded by the fact that it failed to do so even though the House of Representatives had in 2014 been promised that retention terms would be established for unevaluated data.

In anticipation of the new Act (ISS Act 20..), the CTIVD – again – recommends that the AIVD, but also the MIVD, establish and enforce retention terms of no more than one year for unevaluated data. Such internal enforcement of the retention terms must be comprehensive and verifiable. An effective procedure would be to label the data by its origin (i.e., the source and time) and to combine this with automated destruction of this data and logging of such destruction. Such a procedure may constitute an essential element of the duty of due care with respect to computerised data processing as detailed in the CTIVD's View on the ISS Act 20..[14]

In addition, both services must develop a policy and/or working instructions laying down the procedure and the responsible members of staff for the removal and destruction of not relevant and erroneously processed data. The same applies to data that has lost its initial relevance. Subsequently, internal monitoring must take place of whether the data earmarked for immediate destruction is in fact so destroyed.

[14] The CTIVD's View on the ISS Act 20.. Bill, Appendix I (November 2016), pp. 23-25, available on www.ctivd.nl

8 Provision of unevaluated data

Explicit attention was provided in this investigation to the provision to foreign services of unevaluated data deriving from hacks that has not yet been assessed for its relevance. In the context of hacking, this may concern, for instance, an entire web forum, but also the data on a server or computer.

Assessment framework (Chapter 6, p. 20, of Appendix II):

- The provision of unevaluated data to a foreign service requires prior authorisation by the Minister.

Findings

The AIVD did not, in the context of the operations under review, provide unevaluated data deriving from a hack to foreign services. The MIVD did so once.

In this operation, the MIVD provided unevaluated data deriving from a hack to two foreign partner services in the context of a joint operation. While the Minister was informed of the (close) cooperation with these foreign services by way of the request for authorisation, this mere fact did not allow for also sharing unevaluated data. Nor was such explicitly stated in the request. The MIVD, therefore, has not requested prior authorisation to provide unevaluated data, while it should have done so. The MIVD's conduct in this instance was therefore unlawful.

9 Conclusions

The CTIVD draws the following conclusions in this report:

Chapter 2: Overall view and effectiveness

The AIVD and the MIVD have the legal power to “hack”, that is, to break into computer systems. Hacking is in general found to be an effective power: in most cases, its use produced results that were in the interest of national security and could not have been obtained in any other way.

In the vast majority of the dozens of hacking operations reviewed that were conducted in 2015, the AIVD and the MIVD acted in accordance with the law and the principle of due care when using their hacking power. The services are aware of the seriousness of the interference with the rights and interests of the parties involved associated with the use of the hacking power. This first and foremost concerns the right to protection of privacy, but also the importance of safeguarding the integrity of IT systems, for instance. The services therefore generally exercise due care when using this investigatory power and properly balance the interest of national security and the interests of the parties involved.

Chapter 4: Drafting the request for authorisation

The performance of the so-called technical preliminary investigation, aimed at exploring the technical feasibility of the hack for reasons of the internal decision-making process, is lawful. As a rule, the requests for authorisation for the use of the hacking power are carefully substantiated and state which computer systems of which persons or organisations will be subjected to the hack, which purpose is served by the use of the investigatory power and which information is sought by doing so. In a limited number of cases, the AIVD and the MIVD have broken into or added computer systems not covered by the initial authorisation. This is unlawful. In addition, in those cases where it was not possible to list the persons or organisations the hacking power would be used against at the time the request for authorisation was made, both services failed to provide separate notification to the Minister once those identities did become known at a later point. The CTIVD finds this to be negligent. Moreover, both services fail to properly record the performance of physical hacks. This is negligent.

The procedure followed by the services with respect to the use of the hacking power against organisations or their members is, as a whole, lawful. In a limited number of cases, the scope of the substantiation, and thus, of the authorisation, was insufficiently limited, as the description of the organisations or their members or of the computer systems to be broken into was overly general. As the use made of the authorisation granted during the exercise of the powers remained within acceptable boundaries, the CTIVD deems this conduct to have been negligent instead of unlawful.

No negligent or unlawful conduct was identified with respect to performing direct or indirect hacks of persons entitled to professional privilege.

The AIVD only to a limited extent hacked non-targets during the investigation period. This only occurred when concrete indications that the ultimate target posed a direct danger to national security or other significant operational interests existed. This AIVD procedure is lawful. For one operation, the request for authorisation should have more explicitly stated the object of the operation. As, in the end, only data related to the target in question was reproduced, this conduct is found to be negligent.

The AIVD and the MIVD acted lawfully when breaking into computer systems of third parties. In all cases reviewed, such break-ins were unavoidable if the services were to be able to break into the computer system of the ultimate target. The hacking power was not used against individual citizens, being third parties in this context, over the investigation period.

Chapter 5: Authorisation

Due to the organisation of the administrative processes within the AIVD, requests for extension of the use of the hacking power must internally be drafted at such an early time that the authorisation procedure for the extension cannot reflect the most recent state of affairs of the investigation. This is negligent.

The MIVD does not submit requests for the extension of the use of the hacking power to the Minister for approval. This means that it is possible for the course or the nature of the operation to come to deviate, over time, from what the Minister had authorised. In one case, this resulted in unlawful conduct.

Chapter 6: Execution

Both the procedure to be followed and the relevant assessments to be made when deciding whether to report unknown vulnerabilities (*zero days*) have not been internally detailed and laid down. In addition, the assessments made are not being centrally recorded, rendering both internal control and external review of these assessments difficult. It may also occur that vulnerabilities are not reported even after the interest in keeping the unknown has lapsed or become less pertinent. This is negligent.

Chapter 7: Assessing, storing and destroying data

Data is, as a rule, made accessible to staff during the operational process in a careful fashion. The MIVD did not include the separation of functions and duties as a precondition for making untargetedly reproduced data accessible in its request for authorisation for the use of the hacking power. This is negligent.

The failure by both services to have a procedure and practice in force for the destruction of data, including the failure to immediately destroy not relevant and erroneously processed data is unreservedly unlawful. In addition, specifically with respect to the AIVD, the failure to establish retention terms for unevaluated data, even though the House of Representatives had in 2014 been promised by the Minister that such would be (extralegally) effected, is unlawful.

Chapter 8: Provision of unevaluated data

In one joint operation the MIVD failed to expressly request the Minister's authorisation for the provision of unevaluated data to a foreign service. This is unlawful.

10 Recommendations

The CTIVD makes the following recommendations in this Report:

Chapter 4: Drafting the request for authorisation

1. The AIVD and the MIVD must ensure that their procedures conform to the commitments previously made by the Ministers with respect to the immediate and separate notification of the party granting the authorisation upon learning identities not known at the time the authorisation was granted.

2. The services must include the obligation to record the computer systems broken into during physical hacks in working instructions.

3. The MIVD must implement a procedure by which authorisation for additions is granted at a level higher than that of the individual member of staff.

Chapter 5: Authorisation

4. The AIVD must, in anticipation of the new Act (ISS Act 20..), vest the power to grant authorisation for physical hacks at the ministerial level.

5. The MIVD must, in anticipation of the ISS Act 20.., amend its Mandate Regulations and/or policy in such a fashion as to have all requests for extension for a hacking operation submitted to the Minister, as well.

Chapter 6: Execution

6. Both the AIVD and the MIVD must log (continuously, automatically and comprehensively record all data related to) the exercise of the hacking power and the technical activities performed in this connection.

7. The services must develop policies and procedures specifying and laying down the relevant considerations with respect to the decision whether to inform the interested parties in case of unknown vulnerabilities (zero days) being identified. In addition, the unknown vulnerabilities discovered and the assessment made with respect to them must be (centrally) recorded. A regular assessment term must be laid down for unknown vulnerabilities that have not been reported, by which time a reassessment must be made of whether the operational interest still prevails, if such is still expedient.

Chapter 7: Reproducing, assessing and destroying data

8. The AIVD and the MIVD must in all cases vest the power to grant the authorisation with respect to the internal use of unevaluated data deriving from hacks at the level of the head of the team or the bureau, instead of at the level of the processer or analyst.

9. Both services must, in anticipation of the new Act (ISS Act 20..), establish extralegal retention terms of no more than one year for unevaluated data and expressly enforce them.

10. The AIVD and the MIVD must develop a policy and/or working instructions laying down the method to be used for the removal and destruction of data found to be not relevant or processed erroneously. The same applies to data that has lost its initial relevance

T 070 315 58 20 | **F** 070 381 71 68
E info@ctivd.nl | www.ctivd.nl