Universiteit Leiden
The Netherlands

Investigating cybercrime

Oerlemans, J.J.

Citation

Oerlemans, J. J. (2017, January 10). *Investigating cybercrime*. *Meijers-reeks*. Meijers Research Institute and Graduate School of the Leiden Law School of Leiden University, Leiden. Retrieved from https://hdl.handle.net/1887/44879

Version:	Not Applicable (or Unknown)
License:	Licence agreement concerning inclusion of doctoral thesis in the Institutional Repository of the University of Leiden
Downloaded from:	https://hdl.handle.net/1887/44879

Note: To cite this publication please use the final published version (if applicable).

Cover Page

Universiteit Leiden

Leiden University Repository

The handle https://openaccess.leidenuniv.nl/handle/1887/44879 holds various files of this Leiden University dissertation

Author: Oerlemans, Jan-Jaap
Title: Investigating cybercrime
Issue Date: 2017-01-10

8 Performing hacking as an investigative method

This chapter aims to answer the fourth research question with regard to hacking as an investigative method (RQ 4d): *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate hacking as an investigative method?* Hacking as an investigative method is distinguished in this study as: (1) network searches, (2) remote searches, and (3) the use of policeware.

To answer this research question, the investigative method is placed within the Dutch legal framework and further analysed to determine whether the normative requirements for regulating investigative methods which flow forth from art. 8 ECHR are fulfilled. In chapter 3, the normative requirements were identified as follows: (1) accessibility, (2) foreseeability, and (3) the quality of the law.

The requirements for the regulation of this investigative method on the basis of art. 8 ECHR were formulated in subsection 4.4.3. The investigative method was compared to a computer search, i.e., a search at a place where computers (not connected to other computers or the Internet) are seized and their contents are analysed. Computer searches are themselves very intrusive investigative methods that merit detailed regulations with strong procedural safeguards, preferably a warrant from an investigative judge. Network searches are similar, but they go a step further, as this investigative method enables law enforcement officials to search computers elsewhere that are connected to a seized computer. Remote searches and the use of policeware are clearly more privacy intrusive than computer and network searches, given that they are applied covertly. In contrast, a network search is conducted during a search in the physical world. The suspect will be aware of the application of network search, but not necessarily which computers are remotely accessed. The suspect will likely not detect law enforcement officials when a remote search is conducted or policeware is used. As covert applications of investigative methods are accompanied by higher risks of abuse by law enforcement authorities, they merit strong procedural safeguards. Here again, a warrant from an investigative judge is desirable. The use of policeware should also be regulated in detail with added procedural safeguards in the form of restrictions concerning the duration and functionalities of policeware. With regards to hacking as an investigative method, the point of departure here is again that the requirements that flow forth from art. 8 ECHR are minimum standards and that Dutch criminal procedural law can impose a higher level of protection than art. 8 ECHR offers to the individuals involved.

Brief description of the applicable legal framework
Dutch criminal procedural law currently does not include any special investigative power that distinctly regulates the investigative power for remotely accessing computer systems after which a remote search can be conducted or policeware can be installed on the accessed computer (cf. Oerlemans 2011, p. 901-903). A special investigative power is available for network searches, which is examined extensively in sections 8.1.1 and 8.2.1. As explained in section 4.4, the investigative methods of remote searches and use of policeware are highly privacy intrusive. As explained in the introduction to chapter 5, as part of its regulation of investigative methods, Dutch law requires that investigative methods that interfere with the involved individuals' rights and freedoms in more than a minor manner or threaten the integrity of the criminal investigation are based in specific provisions in Dutch criminal procedural law. In December 2015, the Computer Crime Act III was published. This bill aims to explicitly regulate remote searches, the use of policeware, and other forms of hacking as an investigative method (but not network searches), as a special investigative power.

However, it can also be argued that the types of hacking identified as investigative methods within this study can be based on existing investigative powers (cf. Boek 2000 and Verbeek, de Roos & van den Herik 2000). These are the regulations for traditional searches (during which computers can be seized), sneak-and-peak operations, and the use of covert listening devices.[1] In Figure 8.1, these investigative methods are placed on the scale of gravity for privacy interferences with the accompanying quality of the law in the Dutch legal framework.

1 These investigative methods are considered extensively in sections 8.1 and 8.2.

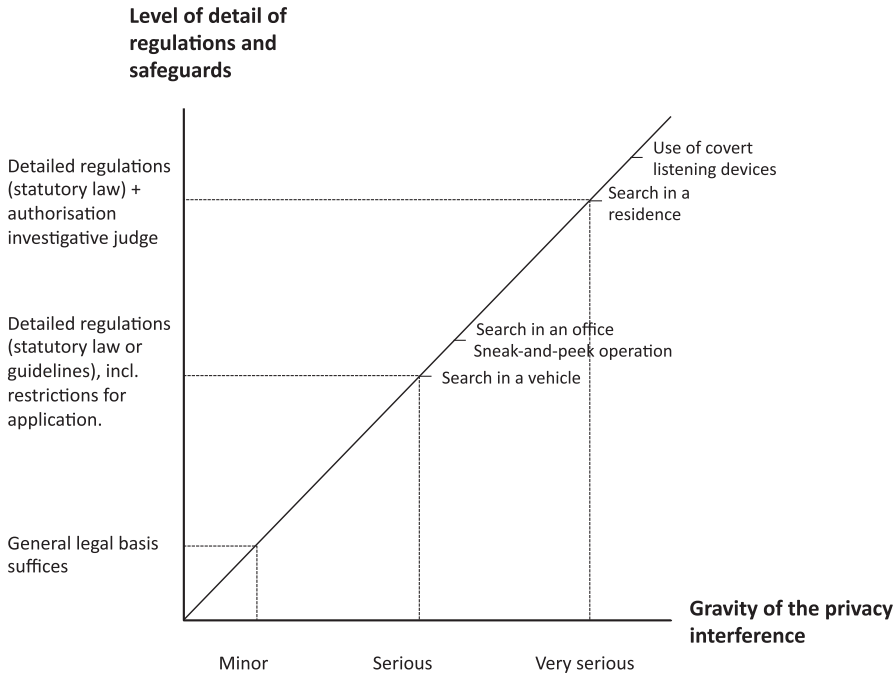

Figure 8.1: The Dutch scale of gravity for investigative methods that are mentioned as a possible legal basis for hacking as an investigative method.

Figure 8.1 illustrates how Dutch law regulates the above-mentioned investigative methods in detail and how different procedural safeguards are required when applying each method (which depend on the gravity of the investigative method)

This chapter further examines whether the identified types of hacking, that can be applied anywhere, can indeed be based on the existing provisions regulating the investigative methods mentioned above. If so, it is examined whether any amendments are required to these provisions to accommodate the identified types of hacking as an investigative method. If not, it is examined whether new distinct legal basis altogether are required for the three types of hacking.

The Dutch legal framework for hacking as an investigative method should fulfil the normative requirements of (1) being accessible, (2) being foreseeable, and (3) meeting the quality of the law that has been derived from art. 8 ECHR. The proposed special investigative power to regulate hacking as an investigative method is also considered in section 8.4. Section 8.4 specifically addresses the question how the Dutch legal framework can be improved to adequately regulate hacking as an investigative method.

Structure of the chapter
The structure of the chapter is as follows. In each section, all three types of hacking as an investigative method are discussed. To assess the accessibility and foreseeability of the Dutch legal framework with regard to the investigative methods, the same scheme of research is used as in chapters 5, 6 and 7. That research scheme consists of the examination of the following four sources of law: (A) statutory law, (B) legislative history, (C) case law, and (D) public guidelines. Thereafter, the requirements for regulations extracted from art. 8 ECHR in chapter 4 are compared to the Dutch legal framework. Based on the results of the analyses, recommendations to improve the Dutch legal framework are provided.

Thus, in section 8.1, the *accessibility* of the regulations for hacking as an investigative method in the Dutch legal framework is examined. Section 8.2 analyses to which extent hacking as an investigative method is regulated in a *foreseeable* manner in the Netherlands. Section 8.3 examines whether the Dutch legal framework for hacking as an investigative method meets the *desired quality of the law*. Based on the findings of section 8.1 to 8.3, section 8.4 will provide concrete suggestions on how Dutch criminal procedural law can be improved to adequately regulate hacking as an investigative method. Section 8.5 concludes the chapter with a summary of findings.

8.1 Accessibility

An accessible basis in law means that the law gives an adequate indication concerning the regulations for the use of investigative methods in a given case.[2] The examination of this normative requirement in relation to hacking as an investigative method will be conducted via analysis of the existing regulations of investigative methods, which may already serve as a legal basis for the digital investigative methods.[3] Subsections 8.1.1 to 8.1.3 present the analyses for all three types of hacking considered. Subsection 8.1.4 then provides conclusions regarding the accessibility of this investigative method in Dutch law.

8.1.1 Network searches

A network search is an investigative method that is used during a search at a particular place (in the physical world). For instance, law enforcement officials can seize a computer during a residence search. As part of a network search, law enforcement officials can then for instance examine an external hard drive or media player by accessing those devices from the previously seized computer through the (internal) network.

2 See subsection 3.2.2 under A.
3 This study does not examine the specific regulations for analysing privileged information, such as information from lawyers, physicians, and journalists.

Law enforcement officials can potentially also gain access to online services that an individual uses when they seize a running computer of the suspect (cf. Conings & Oerlemans 2013).[4] The prevalence of smartphone 'apps' with accompanying login credentials enable law enforcement officials to acquire login credentials when they seize computers (including smartphones). From that seized computer, and using these login credentials, law enforcement officials can access the same internet services that a suspect utilises.[5] A network search is also considered as a type of hacking as an investigative method, because law enforcement officials also gain remote access to computer systems, of which the suspect is not necessarily aware, when a network search is performed.

The accessibility of the legal basis for utilising a network search as an investigative method is examined below using the research scheme mentioned in the introduction to this chapter.

A Statutory law

Dutch criminal procedural law contains detailed regulations for the investigative method of a network search. The special investigative power in art. 125j(1) DCCP that regulates network searches reads as follows:

"In the event of a search, the data stored in a computer that is located elsewhere can be examined from the location that the search takes place, insofar this is reasonably required to uncover the truth. Data that is found, can be secured".[6]

The text of the special investigative power thus states that law enforcement officials can 'investigate data stored on a computer that is located elsewhere' during a search at a specific place (cf. Koops et al. 2012b, p. 59). It is emphasised here that the investigative method is conducted from a computer that has been previously seized by law enforcement authorities. For that reason, the investigative power refers back to the investigative powers for searching a place.

In order words, statutory law authorises law enforcement officials to gain remote access to an interconnected computer when they are conducting a search at a particular place. In the Netherlands, searches by law enforcement officials are regulated in detail in criminal procedural law. Different regulations and accompanying procedures and conditions may apply depending on where a search occurs, given that searches are more intrusive

4 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53, in which the Dutch Ministry of Security and Justice indicates that Dutch law enforcement officials can log in to a server of Gmail or Dropbox to access e-mails and documents stored in the cloud.

5 See subsection 2.4.3.

6 The special investigative power also indicates that the investigation cannot go further than those parts of a computer that the people who reside or work at the place where the search is conducted are authorised to access (see art. 125j(2) DCCP).

when they take place in certain locations. In the event of a criminal investigation related to the more serious crimes as defined in art. 67 DCCP, law enforcement officials can perform network searches on computers located:

(1) in a vehicle;
(2) any other place (except for residences or the offices of privileged professions), after acquiring authorisation from a public prosecutor; and
(3) at a residence, after acquiring authorisation from both a public prosecutor and an investigative judge (cf. Conings & Oerlemans 2013, p. 24).[7]

These three investigative powers were placed on a scale of gravity in Figure 8.1 in the introduction to this chapter. This figure illustrates that searches in vehicles are not considered as highly privacy intrusive and that law enforcement officials are not required to obtain authorisation from a higher authority, whereas residence searches are considered very privacy intrusive and require the procedural safeguard of a warrant from an investigative judge.

B Legislative history

The investigative power for a network search was first introduced by the Dutch legislature in 1992.[8] The legislature made it clear that during a search of a residence, law enforcement officials can seize devices on which data is stored and subsequently search that data.[9] It also found it necessary to create the special investigative power to search stored data on interconnected computers, since residence searches only authorise the search and seizure of computers located at a specific place.[10] Network searches enable data to be located on interconnected computers that are physically in different places.

From 1993-2005, law enforcement officials were only allowed to apply the investigative power to interconnecting computers when they were conducting a search at a residence. In 2005, the DCCP was amended to allow these officials to conduct network searches when they apply the investigative power to conduct a search in any (physical) place.[11]

7 In these three cases, the legal bases in Dutch criminal procedural law for conducting these investigative powers are respectively (1) art. 125j jo art. 96b DCCP, (2) art. 125j jo art. 96c DCCP, and (3) art. 125j jo art. 110 or 97 DCCP.

8 27 December 1992, *Stb.* 1993, 33.

9 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (Explanatory memorandum Computer Crime Act I), p. 11.

10 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (Explanatory memorandum Computer Crime Act I), p. 11-12. See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 11.

11 *Stb.* 2005, 390. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 19.

C Case law

Only *one* case that explicitly refers to the legal basis of a network search is available.[12] The Appeals Court of Amsterdam noted that that law enforcement officials can seize a computer in order to subsequently search that computer's stored contents. The special investigative power for conducting a search that is solely focused on retrieving data that is stored on computers (regulated in art. 125i DCCP) is applicable in this situation. The appeals court also noted that law enforcement officials can use the *"so-called network search"* (as specified in art. 125j DCCP).[13] The case did not provide any further information about how the investigative power for a network search is applied. With regard to the accessibility of the legal basis, it is clear that case law (also) provides an indication of the legal basis for the investigative method.

D Public guidelines

The Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations[14] and the Guideline for the Seizure of Objects[15] of the Public Prosecutors Service, do not mention the use of the special investigative power for network searches to gather evidence in a criminal investigation. The Guidelines for Child Pornography Investigations and the Seizure of Objects solely mention the possibility to seize computers during a search, after which the data stored on those computers may be examined for evidence-gathering purposes.[16] The Guideline for the Seizure of Objects only specifies the legal basis for the seizure of computers in detail in its Appendix I.[17] Thus, none of the guidelines indicates the legal basis for network searches.

8.1.2 Remote searches

The investigative method of a remote search refers to an evidence-gathering activity in which law enforcement officials remotely access a computer (through hacking) and search the data that is stored on it (cf. Brenner 2012). Law enforcement officials can take screen shots of the remotely accessed computer, prepare a written record of the evidence-gathering activities, or even copy relevant data for evidence-gathering purposes (cf. Oerlemans

12 Hof Amsterdam, 24 February 2016, ECLI:NL:GHAMS:2016:579.
13 Hof Amsterdam, 24 February 2016, ECLI:NL:GHAMS:2016:579.
14 *Stcrt.* 2016, 19415.
15 *Stcrt.* 2014, 18598.
16 For child pornography investigations, the guideline recommends seizing all devices and examining their contents. The guideline notes that the data may reveal *"insights in the behaviour of the suspect with regard to child pornography. Contacts, networks of child pornography users or clues that the suspect has abused children may [also] be determined by examining the contents on seized computers"* (translated by the author).
17 Under section B9.

2011, p. 892).[18] This investigative method can enable law enforcement officials to overcome the challenges of anonymity and encryption. Remote searches can be a powerful technique to identify suspects by determining the location and contents stored on a computer, even when a suspect obfuscates his originating (public) IP address with anonymising techniques or services.[19] The investigative method can also enable law enforcement officials to gain access a computer before a suspect is able to encrypt stored information. Law enforcement officials can also remotely access an online account by gaining remote access to a server with acquired login credentials and then copying relevant data.[20]

The accessibility of the legal basis for performing remote searches as an investigative method is examined below using the announced research scheme.

A Statutory law

No specific distinct provisions for remote searches are available in Dutch criminal procedural law. Three options thus arise: (1) the investigative method can be applied under the statutory duty of law enforcement officials to investigate crimes (art. 3 of the Dutch Police Act), (2) the investigative method can be based on an existing special investigative power, or (3) there is currently no legal basis for this method under Dutch law.

With regard to the first option, it is not likely that the investigative method of a remote search can be based on art. 3 of the Dutch Police Act. As explained in subsection 4.4.2, remote searches seriously interfere with the right to privacy as defined in art. 8 ECHR. As such, both ECtHR case law and the Dutch criminal procedural legality principle require that this investigative method be regulated in a specific provision in de DCCP. It is thus appropriate to regulate the investigative method as a special investigative power with adequate procedural safeguards (cf. Oerlemans 2011, p. 901).

With regard to the second option, only one author has argued that certain forms of hacking as an investigative method can be applied on an existing legal basis. Boek argued in 2000 that a remote search of a suspect's webmail account can be regarded as the digital equivalent of a 'sneak-and-peek operation'[21] (Boek 2000, p. 592).[22] Art. 126k DCCP regulates sneak-and-peek operations. The relevant provision reads as follows:

18 It should be noted that this application of a remote search also requires the use of policeware.
19 See subsection 2.3.3.
20 See subsection 2.4.3.
21 In Dutch: '*inkijkoperatie*'.
22 See art. 126k DCCP.

"In case of reasonable suspicion of a crime as defined in art. 67(1) DCCP and insofar it is in the interest of the investigation, a public prosecutor can order a law enforcement official to enter a private place without permission of the right holder, insofar it is not a residence, or to utilise a technical device to:

a. record the place;
b. secure evidence, or;
c. place a technical device in order to determine the presence or movements of an object."[23]

When law enforcement officials perform a sneak-and-peak operation in the physical world, they often slide a flexible camera under a doorpost to briefly observe a private place. In the explanatory memorandum to the Special Investigative Powers Act, the Dutch legislature described a 'private place' as a physical place, such as an office space or a garage. It also made it clear that a sneak-and-peek operation in a residence is considered a disproportionate investigative method for which no basis has been created in criminal procedural law.[24] A sneak-and-peek operation in a residence is thus not permissible. Boek argued that a 'hard disk' could also be regarded as a private place and thus that a sneak-and-peek operation could take place by hacking a computer (Boek 2000, p. 592).

However, I agree with Schermer (2003, p. 53), who regards viewing a computer as a private place in the context of a sneak-and-peek operation as a too extensive interpretation of art. 126k DCCP. I believe that the legislature clearly did not have the hacking of online accounts in mind when it created the investigative power for a sneak-and-peek operation (cf. Oerlemans 2011, p. 901-902). Remote searches interfere with the right to privacy in an entirely different manner than when a sneak-and-peek operation is applied. Furthermore, a remote search can also take place in a computer located at a residence. In contrast, art. 126k(1) DCCP explicitly excludes the possibility to conduct a sneak-and-peek operation inside a residence. The extensive interpretation of investigative powers to suit the needs of law enforcement authorities is not permitted and conflicts both with art. 8 ECHR and with the Dutch criminal procedural legality principle.

In 2002, the Dutch legislature explicitly created hacking powers for Dutch national security and intelligence services.[25] The Dutch legislator did not mention its intent to create such powers for criminal law enforcement authorities. As Koops and Buruma (2007, p. 118 in: Koops 2007) rightfully point out, legislative history thus strongly suggests that hacking powers (such as the possibility to conduct remote searches) have not been created for law enforcement authorities.

---

23 Translated by the author.

24 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 40, 43 and 70.

25 See art. 24 of the Intelligence and Security Services Act of 2002, *Stb.* 2002, 148.

In conclusion, option 3 mentioned above – that the Dutch legislature did not intend to provide Dutch law enforcement authorities with the power to hack computers – is most appropriate.

B Legislative history

Dutch legislative history does not indicate which legal basis is appropriate for a remote search. This investigative method is not mentioned in the explanatory memoranda to the Special Investigative Powers Act or both Computer Crime Acts.

C Case law

Only *one* judgment that deals with the legitimacy of the legal basis for conducting a remote search is available. This case has already been extensively considered in subsections 2.5.4 and 6.1.4.[26] The judgement of the Court of Rotterdam involves the remote access of a webmail account by a Dutch law enforcement official after acquiring authorisation from a public prosecutor. The legal basis for this operation is not made clear in the judgment. The public prosecutor deemed the remote search necessary to determine where a shipment of cocaine was delivered. The public prosecutor did not want to wait for the results of a mutual legal assistance request to acquire the contents of the webmail account using a data production order as meant in art. 126ng(2) DCCP, presumably as doing so would have created an unacceptable delay in the investigation. After remote access to the webmail account was obtained using login credentials previously acquired from an informant, information in e-mails revealed the location of the cocaine shipment (i.e., the port of Rotterdam).

In the first instance of the case, the judges noted that the data should have been obtained through a data production order instead of remotely accessing the online account.[27]

In second instance of the case, the judges did not comment on the legal basis for applying the investigative method. They instead simply stated that the webmail account did not belong (exclusively) to the suspect. For that reason, the suspect was not 'directly infringed in his interests' and no sanction was provided to the supposed procedural default.[28]

Taking the above facts of the case into account, the corresponding judgement ultimately does not provide an indication of the legal basis for gaining remote access to online accounts (technically to a server of the company that provides the webmail service).

---

26 See Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520 and Hof Den Haag, 27 April 2011, ECLI:NL:GHSGR:2011:BR6836.

27 Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520.

28 See Hof Den Haag, 27 April 2011, ECLI:NL:GHSGR:2011:BR6836. See further Oerlemans 2011, p. 894-896. That procedural default was not sanctioned can be explained by the Dutch '*Schutznorm*'. The concept of sanctioning procedural defaults is related to the right to fair trial in art. 6 ECHR. As this study is restricted to art. 8 ECHR, this concept is not further examined.

Indications of hacking as an investigative method in the media

Several news articles in the media and press releases issued by the Dutch Public Prosecution Service indicate that Dutch law enforcement officials have used remote searches as an investigative method at least four times.[29] Two cases are further examined below to analyse the legal basis that was used to conduct these operations.

In 2010, Dutch law enforcement authorities 'took over' the Bredolab botnet. As explained in subsection 2.1.1, a botnet is a network of infected computers (in this case infected by Bredolab malware) that can be controlled by a person (in this case, the suspect). The IT infrastructure of the botnet was located at a Dutch hosting provider. The infrastructure was complex and consisted of several VPN servers and proxy services in an attempt to obtain more anonymity by obscuring the IP address and several command-and-control servers. This convenient location and the cooperation of the hosting provider enabled Dutch law enforcement authorities to conduct a search at the hosting provider and 'take over' the infrastructure of the botnet (once they had hacked several servers and gained remote access to the botnet's command-and-control servers). Dutch law enforcement authorities located the suspect and sent a warning to computer users infected by the Bredolab malware, urging them to clean their computers and report the crime.[30] The suspect was located in Armenia and successfully prosecuted by that State.[31]

In 2011, Dutch law enforcement authorities obtained remote access to four Tor hidden services that were hosting child pornography. As explained in subsection 2.3.2, Tor not only permits individuals to use the Internet more anonymously; it also enables them to access services that are only accessible through Tor, which are called Tor hidden services. Websites or online forums that are only available via Tor sometimes offer child pornography materials to Tor users. In this criminal investigation, Dutch law enforcement officials

29 See Landelijk Parket, 'Dutch National Crime Squad announces takedown of dangerous botnet', 25 October 2010. Available at: https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/, Landelijk Parket, 'Kinderporno op anonieme, diep verborgen websites', 31 August 2011. Available at: http://www.om.nl/onderwerpen/zeden-kinderporno/@156657/kinderporno-anonieme/, Joost Schellevis, 'OM: politie brak in op router vanwege 'acute dreiging'', *Tweakers*, 6 November 2014. Available at: http://tweakers.net/nieuws/92427/om-politie-brak-in-op-router-vanwege-acute-dreiging.html, and see Landelijk Parket, 'Wereldwijde actie politie en justitie tegen hackers'. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie (last visited on 21 December 2014).

30 See Landelijk Parket, 'Dutch National Crime Squad announces takedown of dangerous botnet', 25 October 2010. Available at: https://www.om.nl/actueel/nieuwsberichten/@28332/dutch-national-crime/ (last visited on 21 December 2014). Regarding the more technical details of the operation, see De Graaf, Shosha, and Gladyshev 2012. For a legal analysis of the case, see most notably Koning 2012.

31 See also Josh Halliday, 'Suspected Bredolab worm mastermind arrested in Armenia', *The Guardian*, 26 October 2012. Available at: https://www.theguardian.com/technology/2010/oct/26/bredolab-worm-suspect-arrested-armenia (last visited on 13 November 2015).

gained remote access to the webservers of these websites by hacking. They then replaced 220,000 pornographic images of children with the logo of the Dutch police. They also posted the following message on these websites warning Tor-users as follows: *"This site is under criminal investigation, by the Dutch National Police, you are not anonymous, we know who you are"*. It is not clear whether any suspects were prosecuted following the operation.[32]

These cybercrime investigations that utilised hacking as an investigative method led to the Dutch parliament posing questions to the Dutch Minister of Security and Justice in 2014. In his letter of response, the minister stated that Dutch law enforcement authorities had indeed obtained 'remote access to computers' in several criminal investigations.[33] He noted that in these special circumstances, the investigative power 'to search a place in order to secure data stored on a data carrier' (as articulated in art. 125i DCCP), grants Dutch law enforcement officials with the authority to gain remote computer access. Art. 125i DCCP, reads as follows:

"The investigative judge, the public prosecutor, the deputy public prosecutor and the investigating law enforcement officials are authorised – under the same conditions as provided in articles 96b, 96c(1)(2)(3), 97(1)(2)(3)(4), and 110(1)(2) – to search a place in order to secure data located at this place that is stored or recorded on a data carrier. This data can be secured in the interest of the investigation. (…)" [34]

Art. 125i DCCP thus authorises the appropriate authorities to secure data that is stored on computers under the existing legal basis to search a place. As these legal bases are already examined under A in subsection 8.1.1, it is not further considered here. The regulations for these searches are also illustrated in Figure 8.1 in the introduction. This author was able to review the dossier files of the Bredolab and Tor investigations and confirm that the special investigative power to search a place and secure data that is stored on computer was indeed utilised as a legal basis.[35] In both cases, Dutch law enforcement authorities obtained a warrant from an investigative judge to conduct the operation, although the legal basis that was used (art. 96c DCCP) does not require such a warrant.

---

32 See Landelijk Parket, 'Kinderporno op anonieme, diep verborgen websites', 31 August 2011. Available at: http://www.om.nl/onderwerpen/zeden-kinderporno/@156657/kinderporno-anonieme/. See also Wil Thijssen, 'De digitale onderwereld', *Volkskrant* 10 March 2012. Available at: http://www.volkskrant.nl/vk/nl/2844/Archief/archief/article/detail/3223214/2012/03/10/De-digitale-onderwereld.dhtml (last visited on 8 August 2014).

33 See the document 'Answers of parliamentary questions with regard to the hacking of servers by the police' on 17 October 2014. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha (last visited on 23 December 2014).

34 Translated by the author.

35 Based on art. 125i DCCP jo. 96c DCCP.

To conclude, no judgments in the Netherlands have indicated the legal basis for remote searches. However, news articles in the media and a press release from the Public Prosecution Service have made it clear that Dutch law enforcement authorities have utilised hacking as an investigative method at least four times in the past six years. The legal basis that was used for these investigations stems from the investigative power for searching a place and securing data that is stored on a computer in art. 125i DCCP. For that reason, it can be argued that an accessible legal basis is available for the investigative method of a remote search. However, as argued under A, after an analysis of the Dutch criminal procedural law, the conclusion should be that the DCCP does not provide a legal basis to conduct a *remote* search. The special investigative power in art. 125i DCCP should be read *in conjunction with the power for searching a place* and not be interpreted so extensively that it provides law enforcement authorities the power for remotely accessing a computer.[36] During a remote search, an entirely different investigative method is applied with its own specific interference with the right to privacy. The law is in my view interpreted too extensively by Dutch law enforcement authorities and the Minister of Security and Justice. Nevertheless, the legal basis for the investigative method is apparently the search and seizure of a place to secure data in computers in art. 125i DCCP. Therefore, the law should be considered as accessible.

D Public guidelines

The Public Prosecution Service's Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations, and the Guideline for the Seizure of Objects do not mention the use of a remote search. They thus provide no indication regarding the legal basis for this investigative method.

8.1.3 The use of policeware

Policeware is software that enables law enforcement officials to remotely and secretly turn a computer's functionalities on to gather evidence in a criminal investigation. For example, law enforcement officials can overcome the challenge of encryption in transit by intercepting an individual's communications 'at the source' before encryption is enabled. The use of policeware makes this possible by remotely turning a microphone on and intercepting keystrokes. The intercepted data is then returned to the law enforcement officials at a later point in time. Policeware can also be used to create a 'back door' that enables officials to remotely access a computer. Law enforcement officials can then view the computer screen through the eyes of a suspect by taking screenshots. Policeware can also be used to

36 See also J.J. Oerlemans, 'Hacking without a legal basis', LeidenLawBlog, 30 October 2014. Available at: http://leidenlawblog.nl/articles/hacking-without-a-legal-basis (last visited on 21 July 2014).

overcome the challenge of anonymity in cybercrime investigations. Once law enforcement officials gained remote access to a computer and installed the software, the software can be directed to send law enforcement officials the originating (public) IP address of the computer and other identification information.[37]

The accessibility of the legal basis for using policeware as an investigative method is examined below utilising the announced research scheme.

A Statutory law

Arguably, Dutch law enforcement authorities can install policeware on a suspect's computer using the legal basis of the special investigative power for recording private communications with a technical device.[38] Art. 126l(1) DCCP reads as follows:

"In case of suspicion of a crime as defined in art. 67(1) DCCP considering its nature and cohesion with other crimes the suspect committed seriously interfere with the legal order, a public prosecutor can, insofar the interest of investigation demands it, order a law enforcement official as meant in art. 141(b)(c), to record private communications with a technical device"[39]

This special investigative power allows law enforcement officials to record private communications using a 'technical device'. The wording of the text itself does not exclude the possibility that policeware is regarded as a technical device for recording private communications. However, as explained in the introduction to this subsection, policeware can have functionalities that go beyond just recording private communications. Therefore, if art. 126l DCCP is broadly interpreted, it can be argued that this special investigative power provides a legal basis for using policeware insofar as the policeware only records private communications (cf. Verbeek, De Roos & Van den Herik 2000, p. 155 and Koops & Buruma, p. 118 in: Koops 2007).

B Legislative history

In 1997, the Dutch legislature stated in its explanatory memorandum to the Special Investigative Powers Act that on the basis of art. 126l DCCP (recording private communications with a technical device), Dutch law enforcement officials can install a 'bug' on (1) a keyboard (to intercept keystrokes)

37 See subsection 2.4.3.

38 See art. 126l DCCP. The special investigative power for intercepting communications from public electronic communication service providers without the cooperation of the provider (see art. 126m DCCP) is not applicable, since that investigative power does not allow law enforcement officials to enter a private place in order to intercept the communications. The Dutch legislature has only made this possible for recording private communications under art. 126l DCCP (cf. Koops 2010, p. 2465).

39 Translated by the author.

and (2) a computer mouse (to intercept clicks).[40] Legislative history thus indicates that the functionalities of recording keystrokes or mouse clicks are permitted under the special investigative power for recording private communications.

Furthermore, in 2014 the Dutch Minister of Security and Justice explained in a letter to Dutch Parliament about the use of 'spyware' by Dutch law enforcement authorities that they are permitted to 'physically install' software on a computer on the legal basis of the special investigative power for recording private communications.[41] 'Physically installing the software' likely means that a (physical) search is conducted at a place, after which law enforcement officials install policeware on a computer. He further explained that the functionalities of the software are limited to recording private communications.

To conclude, legislative history indicates that the special investigative power for art. 126l DCCP to record private communications can provide a legal basis for using policeware, insofar as the software's functionalities are restricted to intercepting private communications.

C Case law

In the Netherlands, no judgments are available with regard to the practical use of policeware.[42] Several news articles have suggested that Dutch law enforcement officials utilised policeware in a child abuse investigation,[43] but the legal basis that was used to apply the investigative method has not been mentioned. It can therefore be concluded that case law does not provide an indication concerning the legal basis for this investigative method.

D Public guidelines

The Guideline for Special Investigative Powers specifies which procedures apply to the special investigative power for the interception of private communications.[44] It does not state that *software* can be used to intercept private communications, but it also does not exclude that possibility in that it consistently refers broadly to using 'a technical device'.

---

40 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 35.

41 *Kamerstukken* II 2013/14 (Proceedings of the Second Chamber), 7 October 2014, no. 202 (Answers to parliamentary questions of the Parliamentary Member Gesthuizen regarding the use of controversial spyware by the Dutch Police). Available at: https://zoek.officielebekendmakingen.nl/ah-tk-20142015-202.html (last visited on 14 May 2016). See also J.J. Oerlemans, 'Antwoord Kamervragen over het gebruik van omstreden spionagesoftware', *Computerrecht* 2014/211.

42 However, as explained in subsection 8.2.3, indications that such software is utilised in practice do exist.

43 See, e.g., NOS.nl, 'OM zette keylogger in bij Todd-zaak', 25 June 2014. Available at: http://nos.nl/artikel/666433-om-zette-keylogger-in-bij-toddzaak.html (last visited on 11 August 2014).

44 See most notably section 2.4 of the Guideline for Special Investigative Powers.

8.1.4 Section conclusion

The analyses conducted in subsections 8.1.1 to 8.1.3 can be used to assess the accessibility of the Dutch legal framework for the types of hacking as investigative methods. The results are presented below.

The investigative method of a network search is regulated as a special investigative power in the Netherlands. Network searches can be applied on the same legal basis that is used to search a place in order to gather evidence in a criminal investigation. An indication about the applicable regulations for the investigative method is thus provided. As a result, the Dutch legal framework for this investigative method is considered to be *accessible*. However, only one case that refers to the investigative method is available and the investigative method is not elaborated upon in the examined guidelines.

The investigative method of a remote search is not regulated as a special investigative power in the Netherlands. Nevertheless, a 2012 letter of the Minister of Security and Justice (following several news articles about Dutch law enforcement authorities' practical use of remote searches) indicated that the digital investigative method can be based on the investigative power to search a place in order to secure data stored on a data carrier (regulated in art. 125i DCCP). The law is considered *accessible*, since apparently the legal basis in art. 125i DCCP is used to conduct remote searches in the Netherlands.

The legal basis of the special investigative power for recording private communications is formulated in a technologically neutral manner and leaves room for the interpretation that policeware can also be used as a 'technical device' to record private communications. The explanatory memorandum to the Special Investigative Powers Act and a letter from the Dutch Minister of Security and Justice to the parliament supports the view that policeware can be applied on the legal basis of the special investigative power for recording private communications, insofar as the investigative method is restricted to that. The Dutch legal framework for this investigative method is therefore considered to be *accessible*, insofar as the method does not go beyond recording private conversations.

8.2 Foreseeability

A legal framework that is foreseeable prescribes with sufficient clarity (1) the scope of the power conferred on the competent authorities and (2) the manner in which the investigative method is exercised.[45] With regard to remote searches and the use of policeware, the fact that these investigative methods are applied covertly is important. As explained in subsection 4.4.2, the ECtHR requires that the regulation of the use of covert investigative methods must be: *"sufficiently clear in its terms to give individuals an adequate indication*

45 See subsection 3.2.2 under B.

as to the circumstances in which and the conditions on which public authorities are entitled to resort to such covert measures".[46] Network searches cannot be applied in a covert manner. The investigative method requires law enforcement officials to conduct a search at a specific place, after which the data that is stored on interconnecting computers can be searched. At least this first part of the network search is visible to the individuals that are present at the location the initial search is conducted. Nevertheless, network search are also privacy intrusive and require detailed regulations in statutory law as a legal basis.

The analysis in section 8.1 showed that an indication is provided concerning the applicable legal basis for all three types of hacking as an investigative method. Subsections 8.2.1 to 8.2.3 now explore whether these legal bases indicate the scope of these investigative methods and the manner in which each method should be applied with sufficient clarity. Subsection 8.2.4 then draws conclusions regarding the foreseeability of this investigative method in Dutch law.

8.2.1 Network searches

The foreseeability of the legal basis for preforming network searches as an investigative method is examined below using the announced research scheme.

A Statutory law

The special investigative power for conducting a network search authorises law enforcement officials to 'investigate stored data on a computer that is located elsewhere' during a search at a specific place.[47] As explained in subsection 8.1.1, this investigative power refers back to the regulations for searches that are conducted by law enforcement officials in criminal investigations. Statutory law thus indicates the conditions that apply when conducting a network search at a particular place, which are based on where the search takes place.

However, the scope of the investigative power and the manner in which the investigative power is applied remains unclear. The special investigative power does not indicate clearly how data located on other computers can be searched when a network search is conducted. For instance, it does not specify whether law enforcement officials can use smartphone apps to search for evidence or a web browser on a suspect's computer to attempt to log in to his webmail account. The Dutch Ministry of Security and Justice stated in a report that law enforcement officials are indeed authorised to use a network search to 'log in to a server of Gmail or Dropbox to access e-mails and documents stored "in the cloud" '.[48] The special investigative power itself is for-

46 See specifically ECtHR 12 May 2000, *Khan v. The United Kingdom*, appl. no. 35394/97, § 26.
47 See art. 125j DCCP.
48 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53.

mulated so broadly, i.e., "to search for data that is located elsewhere, from the location that the search takes place, insofar this is reasonably required to uncover the truth", that the scope of the investigative method cannot be said to be indicated with precision. It is imaginable that the provision itself is formulated in such a broad manner. Yet, it requires that the scope of the investigative method is clearly restricted in other legal sources.

B Legislative history

When the special investigative power for network searches was proposed to the Dutch parliament in 1990, the Dutch legislature must have envisioned that law enforcement officials would be enabled to search computers in an internal computer network within a residence.[49] This investigative power allows these officials to access data stored on a connected external hard drive or media player during a residence search (cf. Conings & Oerlemans 2013, p. 24).

However, cloud computing and the multitudes of online services that are offered today create new dimensions for this investigative power. Network searches can now act as an alternative to data production orders, because a network search enables law enforcement officials to directly access data from a device seized from a suspect, instead of ordering the relevant online communication provider to disclose the data to them. To obtain evidence from residents of the investigating State that is located on the servers of online service providers, it may be more straightforward for law enforcement authorities to gather evidence by use of a network search than to send data production orders to online service providers that are located on foreign territory. The reason is the use of mutual legal assistance mechanisms to obtain information from online service providers on foreign territory may take several months; with a cross-border unilateral network search, the evidence can be obtained directly. This subject and the legal questions that arise are further examined in chapter 9.

The explanatory memoranda to the two Computer Crime Acts do not provide concrete examples of this special investigative power. The explanatory memorandum to the Computer Crime Act I only emphasises that the power can only be applied insofar as the persons or employees located at the place where the search is conducted are authorised to access the data stored on the interconnected computers.[50]

It can therefore be concluded that the scope of this investigative power and the manner in which the power is applied are not made clear in legislative history.

49 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90 21 551, no. 3 (explanatory memorandum Computer Crime Act I).

50 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90, 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 27.

C Case law

No current case law discusses or evaluates the scope of the special investigative power to conduct a network search or the manner in which the special investigative power is applied. Only *one* judgment of the Appeals Court of Amsterdam has specified that using a network search may be appropriate when that search is focused solely on retrieving data that is stored on computers. This court further noted in this case that the regular regulations for the seizure of objects during a search are also appropriate for seizing computers.[51] Once law enforcement officials have seized computers, they can subsequently analyse data that is stored on them to gather evidence. No indication is provided in the judgement as to how network searches are applied in practice.

D Public guidelines

The Public Prosecution Service's Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations, and the Guideline for the Seizure of Objects, do not mention the use of a network search as an investigative method. The examined guidelines therefore do not indicate the scope of the investigative method or the manner in which the method is applied in practice.

This is remarkable. Digital evidence that consists of stored data on computers is of growing importance in criminal investigations. This is illustrated by a growing body of case law with regard to criminal investigations that features very different types of crimes.[52] As part of their evidence-gathering activities, I would expect law enforcement officials to also look for evidence on interconnected devices. Due to developments in cloud computing techniques, a substantial amount of information is stored on the servers of online service providers. Law enforcement officials should be interested in gaining access to that evidence, which they may be able to do through a computer (often that they have seized). As already pointed out under A above, only the discussion documents on search and seizure published by the Dutch Ministry of Security and Justice in 2014 mentions a broader interpretation

51 Based on art. 94 DCCP.

52 With regard to child pornography investigations, see, e.g., Rb. Maastricht 29 June 2012, ECLI:NL:RBMAA:2012:BW9971, Rb. Gelderland, 23 August 2013, ECLI:NL:RBGEL:2013:2569, Hof Leeuwarden, 1 April 2016, ECLI:NL:GHARL:2016:2600. With regard to a drug investigation, see Rb. Gelderland, 7 April 2015, ECLI:NL:RBGEL:2015:2313. With regard to a burglary and money laundering investigation, see Rb. 27 September 2013, ECLI:NL:RBDHA:2013:12297. With regard to a murder investigation, see, e.g., Hof Arnhem, 4 May 2012, ECLI:NL:GHARN:2012:BW4764 and Rb. Noord-Holland, 11 February 2014, ECLI:NL:RBNHO:2014:1026. With regard to cybercrime investigations, see, e.g., Hof Arnhem, 21 November 2006, ECLI:NL:GHARN:2006:AZ4330 (a hacking investigation), Rb. Breda, 30 January 2007, ECLI:NL:RBBRE:2007:AZ7266 (a malware investigation), Hof 's-Hertogenbosch, 12 February 2007, ECLI:NL:GHSHE:2007:BA1891 (a malware investigation), Rb. Den Haag, 2 April 2010, ECLI:NL:RBSGR:2010:BM1481 (a death threat investigation), Rb. Amsterdam, 17 February 2015, ECLI:NL:RBMNE:2015:922 (a hacking and fraud investigation), and Rb. Noord-Holland, 11 February 2016, ECLI:NL:RBNHO:2016:1023 (a bomb threat investigation).

of a network search. The authors of these documents state that law enforcement officials can use a network search to gain access to (1) e-mail stored on a web server, such as Gmail, and (2) documents stored 'in the cloud', such as in Dropbox.[53] The statutory law that regulates the investigative power itself does not exclude these two possibilities. However, this interpretation of the law is not supported by any of the other examined legal sources. In other words, ambiguity exists with regard to the foreseeability of the scope of the investigative power to conduct a network search. Research shows that the scope of the investigative power is also not clear in practice (see Koops et al. 2012b, p. 38 and Mevis, Verbaan & Salverda 2016, p. 74). However, this ambiguity regarding the scope of the investigative method is explained by these authors in connection with uncertainty with regard to the territorial restrictions of the investigative power. These questions are addressed in subsection 9.5.1 in chapter 9.

8.2.2 Remote searches

The foreseeability of the legal basis for preforming remote searches as an investigative method is examined below using the announced research scheme.

A Statutory law

Remote searches are not regulated as a special investigative power in Dutch criminal procedural law. The analysis under C in subsection 8.1.2 has shown that, the legal basis of the investigative power to 'search a place in order to secure data stored on a data carrier' in art. 125i DCCP has been used in practice to apply the investigative method. This provision refers back to investigative powers that regulate the search of a place, during which the appropriate authorities can seize objects such as computers (cf. Mevis, Verbaan & Salverda 2016, p. 27).

As an investigative method, a remote search is substantially different to the search of a place and the seizure of objects. During a remote search, hacking techniques are used to covertly access computers and evidence is subsequently secured. During a regular search and seizure, law enforcement officials physically enter a place and gather evidence. The privacy interferences that accompany the covert application of this investigative method and the gathering of data from computers simply differ from those that arise when a physical search is conducted. In my view, this investigative method merits specific legislation and its own procedural safeguards. The law is interpreted too extensively, when remote searches are based on the investigative power for searching a place (cf. Oerlemans 2011. 907-908).[54]

53 See the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53.

54 It should be noted that here the normative requirements of foreseeability and the quality of the law again become intertwined.

B Legislative history

The explanatory memoranda to both Dutch Computer Crime Acts and the Special Investigative Powers Act do not provide clarity about the scope of the investigative method of a remote search and the manner in which this method is applied.

As mentioned under B in subsection 8.1.2, the Dutch Minister of Security and Justice noted in a 2014 letter to the Dutch parliament that Dutch law enforcement authorities have obtained 'remote access to computers' in several criminal investigations.[55] It thus appears that the minister and Dutch law enforcement authorities have adopted the same interpretation of art. 125i DCCP. According to the minister, the investigative power for searching a place to conduct a computer search only grants Dutch law enforcement officials the authority to gain remote access to computers in 'special circumstances'.

However, the aforementioned statements do not clearly indicate the scope of the investigative method. As I have argued under A above, the special investigative power in art. 125i DCCP does not provide an adequate legal basis for performing remote searches. The special investigative power described in art. 125i DCCP should be read *in conjunction with the power for searching a place* and not be interpreted so extensively that it provides law enforcement authorities the power for remotely accessing a computer.[56]

C Case law

The examined cases in subsection 8.1.2 have illustrated how remote searches have been conducted to gain remote access to (1) a webmail account to access private messages detailing the shipment of drugs, (2) several servers to take over a botnet, and (3) a server to replace child pornography images with the image of a police logo. Below, a fourth case is examined that further illustrates the scope of the investigative method.[57] The case involved a death threat that was published on the Internet and illustrates how a remote search was used to determine the location of a computer and a suspect.

On 20 April 2013, the following message was posted on 4Chan.org (an online forum):

"Tomorrow, I will shoot my Dutch teacher, and as many students as I can. It will be on the news tomorrow. It's a school in a dutch city called Leiden, and for more proof, I wil be using a 9mm Colt Defender. I will be carrying a note with me when I

55 See the document 'Answers of parliamentary questions with regard to the hacking of servers by the police' on 17 October 2014. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2014/10/18/antwoorden-kamervragen-over-het-hacken-van-servers-door-de-politie-terwijl-de-zogenaamde-hackwet-nog-niet-door-de-kamer-is-beha (last visited on 23 December 2014).

56 See also J.J. Oerlemans, 'Hacking without a legal basis', *LeidenLawBlog.nl*, 30 October 2014. Available at: http://leidenlawblog.nl/articles/hacking-without-a-legal-basis (last visited on 21 July 2014).

57 See Rb. Den Haag, 19 November 2013, ECLI:NL:RBDHA:2013:15617.

go into the school which will explain why I did it. If the message of the note will not be published, a friend of mine with the post here on 4chan a day later. Oh, and I'm using a proxy, the police is not gonna find me before tomorrow."[58]

Dutch law enforcement authorities took this death threat seriously and launched an investigation. Here it is important to note that 4Chan is a so-called 'image board' where individuals can post messages without disclosing their real names or nicknames; the above message was also signed 'anonymous'. However, these online services do log the IP addresses of users who post to the image board. Law enforcement authorities can obtain this information by issuing a data production order.[59] In this case, the IP address was assigned to a router at a youth hostel in Costa Rica (not a proxy server, as the author claimed in the message).[60] However, officials felt it was necessary to obtain remote access to the router to validate that the IP address belonged to the hostel. They reportedly accessed the router using 'admin' as both the login name and password.[61] The suspect turned himself in and flew back to the Netherlands, after which he was arrested and successfully prosecuted by Dutch law enforcement authorities.[62] In the judgement, the Dutch judges did not address the lacking legal basis for the remote search that was conducted.[63] The trial lawyers did not object to this investigative activity.

When all of the above information and the examined cases in subsection 8.1.2 are taken into account, it can be concluded that case law shows that a remote search has been conducted to remotely access (1) an online account, (2) a router of a youth hostel, (3) a botnet's command-and-control server, and (4) hidden services on Tor. It is thus clear that this investigative method is currently being applied to access many different types of computers for a variety of purposes in the absence of detailed regulations to restrict its scope. This research result suggests that the Dutch legal framework is currently not foreseeable in the context of this investigative method.

58 The original message was mentioned in the judgment (including spelling and grammar errors). See Rb. Den Haag, 19 November 2013, ECLI:NL:RBDHA:2013:15617.

59 See chapter 6. In this case, mutual legal assistance may have been required to obtain data from a foreign hosting provider.

60 See Joost Schellevis, 'OM: politie brak in op router vanwege "acute dreiging" ', *Tweakers*, 6 November 2014. Available at: http://tweakers.net/nieuws/92427/om-politie-brak-in-op-router-vanwege-acute-dreiging.html (last visited on 14 April 2014). It should be noted that jurisdictional issues may be involved with this investigative activity. These issues are further addressed in chapter 9.

61 See Joost Schellevis, 'OM: politie brak in op router vanwege "acute dreiging" ', *Tweakers*, 6 November 2014. Available at: http://tweakers.net/nieuws/92427/om-politie-brak-in-op-router-vanwege-acute-dreiging.html (last visited on 14 April 2014).

62 See RTLNieuws.nl, 'Verdachte Leiden gevonden in Costa Rica', 26 April 2013. Available at: http://www.rtlnieuws.nl/nieuws/binnenland/verdachte-leiden-gevonden-costa-rica (last visited on 26 April 2016).

63 See Rb. Den Haag, 19 November 2013, ECLI:NL:RBDHA:2013:15617.

D Public guidelines

As explained in subsection 8.1.2, the Public Prosecution Service's Guideline for Special Investigative Powers, the Guideline for Child Pornography Investigations, and the Guideline for the Seizure of Objects do not mention remote searches as an investigative method. Therefore, no indication regarding the scope of the investigative method or the manner in which the method is applied is available in the examined guidelines.

8.2.3 The use of policeware

The foreseeability of the legal basis for using policeware as an investigative method is examined below utilising the announced research scheme.

A Statutory law

In Dutch criminal procedural law, the special investigative power for intercepting private communications allows law enforcement officials to record private communications using a 'technical device'.[64] This power specifies in detail under which conditions it can be applied. Additional requirements are applicable when a technical device is installed inside a residence. A Dutch public prosecutor can order the application of the special investigative power for intercepting private communications using a technical device outside of a residence after obtaining a warrant from an investigative judge. The power can be applied for a maximum period of four weeks, which can be extended for another four weeks.[65] In addition, the individual involved must be suspected of a crime as defined in art. 67(1) DCCP that seriously infringes upon the legal order. The application of this investigative method must also be essential to furthering the criminal investigation.[66] When a technical device is to be installed within a residence, the relevant crime must also be sanctioned by a prison sentence of at least eight years.[67]

With regard to the scope of the investigative method, it is important to note that statutory law does not clarify what a technical device entails. Statutory law also does not indicate in which manner the investigative method can be applied. However, it is clear that a physical technical device can be installed by breaking into a place. Policeware can be installed in a similar manner by 'breaking into' (i.e., hacking) a computer.

To conclude, this special investigative power indicates under which conditions it can be applied, but not the investigative power's scope or the manner in which the investigative method can be applied in a digital context.

64 See art. 126l DCCP. See also subsection 8.1.3 under A.
65 See art. 126l DCCP.
66 See art. 126l(1) DCCP.
67 See art. 126l(2) DCCP.

B Legislative history

In 1997, the Dutch legislature stated in its explanatory memorandum to the Special Investigative Powers Act that Dutch law enforcement officials can install technical devices on keyboards (to intercept keystrokes) and computer mice (to intercept mouse clicks).[68] This special investigative power can only be applied insofar as private communications are recorded for evidence-gathering purposes. The explanatory memorandum explains that the term 'private communications' is interpreted broadly, namely to include data that is sent between two parties.[69] When a computer is connected to the Internet, law enforcement officials can thus intercept network traffic that takes place between computers that is then regarded as private communications. The technical device that is utilised to apply this special investigative power must meet specifications included in lower regulations. These specifications require Dutch law enforcement officials to, for instance, send the intercepted communications through a secure connection and store the data in a secure place to avoid data manipulation.[70]

Interestingly, the explanatory memorandum explicitly mentions how a technical device can enable law enforcement officials to intercept communications between two parties *before* the information is encrypted.[71] This description resembles an important functionality of policeware, which can be used to intercept data (in the form of keystrokes or voice messages), before it is encrypted by online service providers.[72] However, the explanatory memorandum does not explicitly mention that *software* can be utilised to intercept private communications.

Taking the above into account, it can be concluded that legislative history provides information regarding the scope of the investigative method and the manner in which the investigative method can be applied. Although this legislative history is over 20 years old, the text is formulated in a technologically neutral manner and may cover certain functionalities of using policeware as an investigative method. However, certain questions remain unaddressed, such as whether the software's capacity to take screen shots with policeware can be used as part of the special investigative power for recording private communications.

C Case law

As explained in subsection 8.1.3, no judgments concerning the legitimacy of the use of policeware are available. However, news articles in the media about a pending case reveal that Dutch law enforcement officials report-

68 See also subsection 8.1.3.

69 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 37.

70 See art. 13 and 14 of the Besluit technische hulpmiddelen, *Stb.* 2013, 49.

71 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 36.

72 See subsection 2.4.3.

edly used policeware in an online child abuse case.[73] The use of policeware enabled them to (1) log chat conversations by intercepting keystrokes and (2) take screenshots of the suspect's computer screen.[74] After analysing leaked documents, journalists concluded that Dutch law enforcement authorities purchased 'FinFisher' policeware from the German company Gamma International.[75] FinFisher software indeed has the capacity to log keystrokes and take screen shots. In addition, the software reportedly has an option that allows law enforcement officials to turn a computer's microphone on and monitor Skype conversations before information is encrypted, thereby overcoming the obstacle of encryption in transit in criminal investigations.[76] The software reportedly even allows officials to extract files from a hard disk and gain remote access to a computer system for 'live remote forensics'.[77]

As of the time of writing (October 2016), it is unclear whether the policeware was remotely installed on the suspect's computer and which of the software's functionalities were utilised, although news articles suggest that screen shots were taken. This functionality appears to be broader than the Dutch legislator anticipated within the special investigative power for recording private communications under art. 126l DCCP.

D Public guidelines

The Guideline for Special Investigative Powers devotes an entire section (section 2.5) to the application of and procedures which to apply the special investigative power for the recording private communications.[78] The guideline largely repeats the relevant parts of legislative history. It also specifies that when a technical device is installed in a residence, a public prosecutor must consult the Public Prosecution Service's special advisory commis-

---

73 The case concerned a suspect who enticed under-aged girls to perform sexual activities over the Internet. One of these girls committed suicide, which led to unrest in her home country of Canada. See, e.g., Patrick White and Jane Taber, 'Dutch police arrest suspect in the Amanda Todd case', *The Globe and Mail*, 17 April 2014. Available at: http://www.theglobeandmail.com/news/british-columbia/amanda-todd/article18055474/ (last visited on 11 August 2014).

74 See, e.g., NOS.nl, 'OM zette keylogger in bij Todd-zaak', 25 June 2014. Available at: http://nos.nl/artikel/666433-om-zette-keylogger-in-bij-toddzaak.html (last visited on 11 August 2014).

75 See Michael Persson, 'Politie gebruikt mogelijk omstreden spionagesoftware', *Volkskrant*, 8 August 2014. Available at: http://www.volkskrant.nl/vk/nl/2694/Tech-Media/article/detail/3715207/2014/08/08/Politie-gebruikt-mogelijk-omstreden-spionagesoftware.dhtml (last visited on 11 August 2014).

76 See subsection 2.4.1 with regard to the challenge of encryption in transit in criminal investigations. Skype encrypts network traffic by default. Law enforcement officials are presumably unable to read the contents of Skype conversations when the information is intercepted using a wiretap at a public telecommunication service provider (cf. Oerlemans 2012, p. 27).

77 See Morgan Marquis-Boire, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', *Citizen Lab*, 25 July 2012. Available at: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (last visited on 10 July 2014).

78 See section 2.5 of the guideline for special investigative powers of 2014.

sion.[79] This commission will then advise on the desirability of using this special investigative power in a particular case. The Guideline for Special Investigative Powers does not mention whether policeware is understood as a technical device and provides no specifications with regard to the functionalities of technical devices. The guideline therefore only provides additional information about the manner in which the investigative method is applied by explaining that it is necessary to consult the special advisory commission.

8.2.4 Section conclusion

The analyses conducted in subsections 8.2.1 to 8.2.3 can be used to assess the foreseeability of the Dutch legal framework in criminal procedural law with regard to the examined types of hacking as an investigative method. The results are summarised below.

Despite the detailed provisions that exist in Dutch criminal procedural law concerning the application of network searches as an investigative method, the legal basis of this investigative method is considered *not foreseeable*. The reason is that none of the examined sources in law indicate the scope of network search or the manner in which the investigative method is applied in practice. A discussion document from the Dutch Ministry of Security and Justice boldly stated that network searches also enables law enforcement officials to access online accounts. However, the examined legal sources do not indicate that this application is possible. Most of the information available is from legislative history that is over 25 years old. This leaves ambiguity with regard to the scope of network searches and the manner in which the investigative method is applied in practice.

The legal basis for performing a remote search is considered *not foreseeable*. Dutch law does not explicitly indicate the legal basis for this investigative method. According to the Dutch Minister of Security and Justice at the time, this method can be based on the investigative power to search a place in order to secure data stored on a data carrier. However, this investigative power refers back to an existing power for searching places and seizing objects that are located in that place. Remote searches go a significant step further, given that computers are accessed covertly. The power for searching places and seizing objects is meant for the physical world. I argued that the referenced provisions in Dutch criminal procedural law do not authorise law enforcement officials to hack into computers and secure evidence remotely. Furthermore, the privacy interferences that accompany

79 In a particularly pressing situation, a public prosecutor can choose to apply the special investigative power without advice form the special commission after obtaining a warrant from an investigative judge. A special team of the Dutch police that is tasked with installing the device will then examine whether its installation is feasible from technical and tactical perspectives.

remote searches are also different from those that accompany regular computer searches. As such, remote searches as an investigative method should be regulated in distinct specific provisions in the DCCP.

Based on statutory law and the explanatory memorandum to the Special Investigative Powers Act, it can be argued that policeware can based on the special investigative power to record private communications. The examined legal sources however do not clarify which functionalities of policeware can be applied. For example, it remains unclear whether the special investigative power authorises law enforcement officials to take over a suspect's computer and subsequently take screen shots or gain remote access to a computer system and conduct a remote search. The legal basis for this investigative method in Dutch law is therefore considered *not foreseeable* for this investigative method.

8.3 Quality of the law

The normative requirement regarding the quality of the law, means that the ECtHR can specify the level of detail required for the description the investigative power and the minimum procedural safeguards that must be implemented vis-à-vis a particular method that interferes with the right to privacy. The detail that the ECtHR requires in the law and procedural safeguards depends on the gravity of the privacy interference that takes place.[80]

The desired quality of the law for hacking as an investigative method, was determined in subsection 4.4.4. An overview of the desired quality of the law for all three types of hacking as an investigative method is provided in Figure 8.2.

80 See subsection 3.2.2 under C.

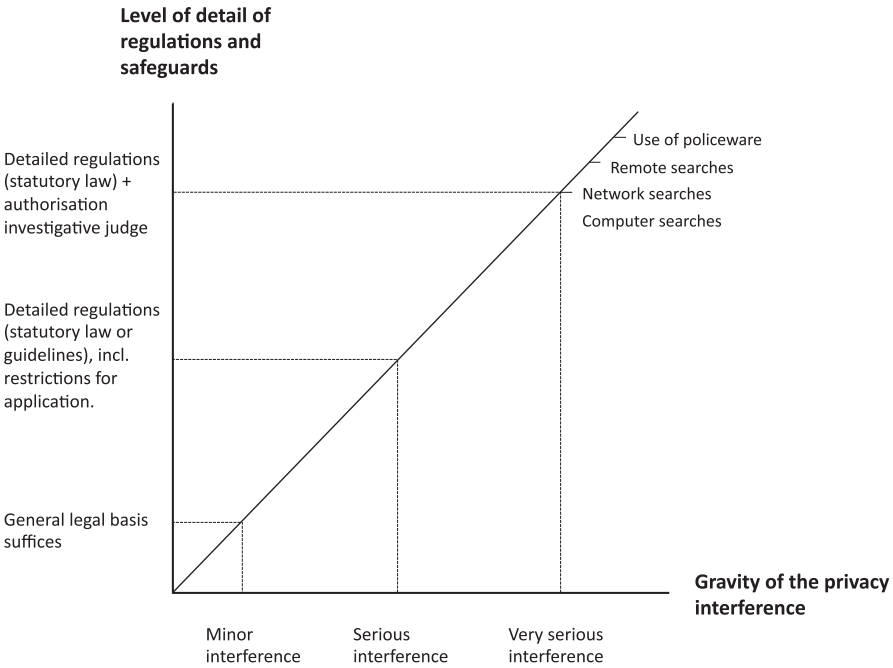

Figure 8.2: The quality of the law for hacking as an investigative method.

Figure 8.2 illustrates how all types of hacking as an investigative method are considered as highly privacy intrusive investigative methods that require detailed regulations in statutory law with at the procedural safeguards of authorisation of an investigative judge. More specifically, the analysis showed that network searches are very intrusive investigative methods, because computers within a network can contain large amounts of personal information of individuals. Remote searches and the use of policeware are more privacy intrusive than network searches, given that they are applied covertly. As covert applications of investigative methods are accompanied by higher risks of abuse by law enforcement authorities, they merit stronger procedural safeguards (more specifically, a warrant from an investigative judge). The use of policeware is the most intrusive investigative method that is examined in this study, because it combines several intrusive investigative methods in one. The investigative method can be considered as a combination of a computer search, sneak-and-peek operation, and wiretapping. The high intrusiveness of the investigative method and broad scope of the investigative method merit that the investigative method is regulated in detail with the procedural safeguard of a warrant, with clear restrictions concerning the duration and functionalities of the policeware.

In subsections 8.3.1 to 8.3.3, the quality of the law of the Dutch legal framework with regard to the three types of hacking as an investigative method is compared to the desired quality of the law. Subsection 8.3.4 then draws conclusions as to whether the Dutch legal framework for hacking as an investigative method meets the desired quality of the law.

8.3.1 Network searches

The desirable quality of the law for network searches has been identified as detailed regulations in statutory law, with the procedural safeguard of a warrant that is issued by an investigative judge.[81]

As defined in Dutch criminal procedural law, the special investigative power for a network search refers back to existing investigative powers to conduct a search at a particular place. The same conditions thus apply to both network searches and searches of particular places and the subsequent seizure (and analysis) of computers. Different regulations and conditions from Dutch criminal procedural law apply depending on where a search is conducted.[82]

This differentiated legal regime for searching computers based on their location is not appropriate (cf. Koops et al. 2012b, p. 59 and Conings & Oerlemans 2013, p. 26). Computers are not regular objects that can be seized during a search of a place. They often store large amounts of personal information that can be analysed with software. Seizing a computer and subsequently searching the data stored they contain therefore heavily interferes in an individual's private life (cf. Groothuis & de Jong 2010, p. 280 and Conings & Oerlemans 2013, p. 26). Individuals should be protected from arbitrary governmental interference during computer and network searches, no matter where the computer is located. The Dutch legal framework for network searches therefore does not currently meet the desired quality of the law. The special investigative power for network searches (which should not refer back to investigative powers for conducting searches at particular places) also requires the procedural safeguard of an investigative judge to help determine which computers should be accessed and balance the purpose for

81 See subsection 4.4.4.

82 See subsection 8.1.1. See also Figure 8.1 in the introduction. In two cases, Dutch judges found that the current Dutch regulations to search a place, seize computers, and subsequently search the data stored on computers were in violation with art. 8 ECHR. See Hof Arnhem-Leeuwarden, 22 April 2015, ECLI:NL:GHARL:2015:2954, m.nt. J.J. Oerlemans, *Computerrecht* 2015/127 and Rb. Noord-Holland, 4 June 2015, ECLI:NL:RBNHO:2015:4660. However, a majority of Dutch courts have since stated that the Dutch regulations for computer searches, more specifically art. 94 DCCP, clearly provides a legal basis for seizing computers (during a search) and subsequently analysing the data stored on them. See, e.g., Rb. Amsterdam, 18 June 2015, ECLI:NL:RBAMS:2015:4024, Hof Amsterdam, 13 November 2015, ECLI:NL:GHAMS:2015:5007, Rb. Overijssel, 1 March 2016, ECLI:NL:RBOVE:2016:708. Interestingly, the Court of Amsterdam stated that the possibility for suspects to object to a computer search suffices to meet the preferred involvement of an investigative judge by the ECtHR (see Hof Amsterdam, 24 February 2016, ECLI:NL:GHAMS:2016:579). In my view, the ECtHR prefers a warrant from an investigative judge as a procedural safeguard for computer searches. It is possible the Dutch Supreme Court will decide on the issue, insofar as the Dutch legislature does not amend the law sooner. See further J.J. Oerlemans, 'Rechtspraak verdeeld over rechtmatigheid van het doorzoeken van smartphones', *Computerrecht* 2016, no. 3, p. 204-205.

gathering evidence with the interference to the involved individual's rights and freedoms, regardless of where computers have been seized.

It is worth noting that when the special investigative power for network searches was proposed to the Dutch parliament in 1990, the power was described as '*the most far reaching investigative power with regard to computer investigations*' in criminal procedural law.[83] Despite the emphasis on this investigative power's intrusiveness in terms of privacy, *no* examples of the concrete application of this method are provided in legislative history and almost no relevant case law is available. Considering both how technology has advanced and the recent case law of the ECtHR on computer searches, it appears appropriate to rethink the Dutch legal regime for computer and network searches.

8.3.2 Remote searches

The desirable quality of the law for remote searches has been identified as detailed regulations in statutory law, with the procedural safeguard of a warrant issued by an investigative judge.[84]

A specific legal basis in the DCCP is required for remote searches, given that the investigative method interferes with an individual's right to privacy in a very serious manner. The covert use of investigative methods poses greater risks of a governmental abuse of power. Bearing both the serious privacy interference and the criminal procedural legality principle in mind, it follows that the Dutch legislature should regulate this investigative method as a special investigative power in Dutch criminal procedural law (cf. Oerlemans 2011, p. 899-901).[85] Currently (as of October 2016), no such special investigative power is available in the DCCP. The Dutch legal framework regulating remote searches therefore does not currently meet the desired quality of the law.

8.3.3 The use of policeware

The desirable quality of the law for using policeware consists of (1) detailed regulations for the investigative method, (2) a warrant requirement, and (3) restriction of the duration and functionalities as procedural safeguards (cf. Oerlemans 2011, p. 908).[86]

Within the Dutch legal framework, stringent conditions already apply for applying the special investigative power for recording private communications with a technical device. The Dutch legislature reasoned at the time (1996) that applying this special investigative power seriously interferes

83 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1989/90 21 551, no. 3 (explanatory memorandum Computer Crime Act I), p. 27.
84 See subsection 4.4.4.
85 See subsection 4.4.4.
86 See subsection 4.4.4.

with the right to privacy.[87] Although the Dutch legislator may have had the application of a different investigative method in mind, the strict requirements to apply the special investigative power appear also suitable for the use of policeware. In other words, the procedural safeguards that apply to the use of the special investigative power for recording private communications meet the desired quality of the law in relation to the use of policeware. A warrant must be obtained and the application of the investigative method is restricted in duration. The heightened proportionality principle that applies to this power should be translated in practical terms to restrictions concerning which functionalities of policeware may be used by law enforcement authorities.

However, note that the special investigative power for recording private communications does not indicate the scope of the use of policeware and the manner in which this software can be used in sufficient detail. Here, the normative requirements of foreseeability and the quality of the law are clearly intertwined. When all of the normative requirements are taken into consideration, the current regulations are therefore still not in 'accordance with the law', as meant in art. 8 ECHR.

8.3.4 Section conclusion

This section compared the quality of the law of the Dutch legal framework for criminal procedural law with the desirable quality of the law as determined in subsection 4.4.3. The desired quality of the law for the investigative method was visualised in Figure 8.2 in the introduction of this section. The results concerning whether the Dutch legal framework for hacking as investigative method meets the desired quality of the law are summarised below.

The Dutch legal framework for network searches *does not meet the desirable quality of the law*. The detailed regulations and corresponding procedural safeguards that apply for network searches are differentiated based on the location that network searches are conducted, which is undesirable. Computers are not regular objects, as they can contain large amounts of diverse information that should be sufficiently protected. A single investigative power should therefore apply for network searches with a warrant requirement as a procedural safeguard, regardless of where a computer was seized.

No specific legal basis for remote searches exists in Dutch criminal procedural law. Instead, the investigative power for searching a place and conducting computer searches in art. 125i DCCP refers back to existing powers for searching a place and seizing computers. These procedural safeguards in these regular search and seizure power differentiate based upon the location of the place the search is conducted. The investigative method should be regulated by a single investigative power with the procedural safeguard of a warrant from an investigative judge. Since this quality of the law is not

87 *Kamerstukken II* (Proceedings of the Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 38.

met, the Dutch legal framework for the investigative method *does not meet the desirable quality of the law*.

The Dutch legal framework for the use of policeware cannot be considered 'in accordance with the law' as meant in art. 8 ECHR, due to ambiguity with regard to the scope of the use of policeware and the manner in which this software is utilised. However, *the quality of the law is adequate*, since a single special investigative power currently applies to using the investigative method using the maximum safeguards available in Dutch criminal procedural law. The procedural safeguards include a restriction of the duration of the use of policeware and a heightened proportionality principle that translates to a restriction of the functionalities of policeware that can be used.

8.4 Improving the legal framework

This section discusses the extent to which the DCCP can be improved in order to provide an adequate legal framework for regulating hacking as an investigative method. A legal framework is considered adequate when (1) it is accessible, (2) it is foreseeable, and (3) the desired quality of the law is met. The results of the analyses of the three normative requirements in sections 8.1 to 8.3 are summarised in Table 8.1.

Normative requirement	**Network searches**	**Remote searches**	**The use of policeware**
Accessible	✓	✓	✓
Foreseeable	✗	✗	✗
Meets the desirable quality of the law	✗	✗	✓

Table 8.1: Representation of the research results in sections 8.1 to 8.3 (✓ = adequate, ✗ = not adequate).

Table 8.1 shows that foreseeability is lacking in relation to the application of the three types of hacking examined in this chapter. The current regulations on which the various types of hacking are based were developed over two decades ago, and are now being applied in a different era. In 1997, the Dutch legislature stated in its explanatory memorandum to the Special Investigative Powers Act that *"new investigative methods will be developed that interfere with the right to privacy in new manners"*.[88] The use of a hacking is one such new investigative method that interferes with the right to privacy in a serious and novel manner.

88 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 11.

Furthermore, recent ECtHR case law with regard to computer searches indicates that detailed regulations are desirable for computer searches and that a warrant from an investigative judge is preferably applicable. Given that hacking as investigative method is even more privacy infringing than computer searches, it is necessary to amend the Dutch legal framework to adequately regulate its application.

Subsections 8.4.1 to 8.4.3 further examine the three types of hacking used as investigative methods and identify how each should be regulated.

8.4.1 Network searches

Network searches are regulated as a special investigative power within a specific provision of Dutch criminal procedural law. The Dutch legal framework can thus be considered as accessible. However, the scope of the investigative methods and the manner in which they are executed are unclear, due to an outdated description of the investigative method in legislative history, lack of case law, and no direction from guidelines. Currently, the procedural safeguards depend on the location the investigative method is applied, which is not desirable. It would be appropriate to incorporate a requirement for a warrant from an investigative judge in connection with the special investigative power for conducting network searches. Therefore, the special investigative power for a network search should be amended and incorporate warrant from an investigative judge as a procedural safeguard, regardless of where a computer was seized (*Recommendation 1).*

In 2015, the Dutch Minister of Security and Justice made clear that he does not regard the current legal regime for computer searches as adequate.[89] Considering the large amounts of information that are stored on computers and the software that is available to quickly analyse all of the available data, the Dutch minister suggested that a legal threshold that involves a 'higher authority' than a law enforcement official is appropriate.[90] Such an amendment may also lead to higher procedural safeguards for network searches, given that the regulations for computer and network searches are so closely intertwined.

However, due to objections from the Dutch police and Public Prosecution Service concerning the reform of the legal regime for computer searches, further research was deemed desirable to examine the 'consequences

89 Letter of 30 September 2015 regarding the modernisation of the DCCP, p. 83. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/09/30/brief-aan-de-tweede-kamer-modernisering-wetboek-van-strafvordering-plus-contourennota (last visited on 3 October 2015).

90 Letter of 30 September 2015 regarding the modernisation of the DCCP, p. 83. The threshold of a law enforcement official only applies when a computer is seized after a vehicle is searched (see art. 94b DCCP).

for law enforcement practice'.[91] The report that followed from Mevis, Verbaan, & Salverda (2016) noted that in current Dutch law enforcement practice, computers are seized as regular objects during the search of a place. Most often, a public prosecutor or investigative judge authorises the search and seizure of computers (see Mevis, Verbaan, & Salverda 2016, p. 52). The report's authors conclude that no uniform policy exists with regard to the seizure and analysis of data that is stored on computers in the Netherlands (Mevis, Verbaan, & Salverda 2016, p. 78). As a result, the investigative method is applied in diverse manners. The authors of the report recommend that the Dutch legislature should create extra safeguards for computer searches when they deem it necessary (see Mevis, Verbaan, & Salverda 2016, p. 79).

The report does not extensively describe developments in digital forensic technology that enable law enforcement authorities to thoroughly analyse all of a computer's stored contents, as this was beyond its mandate. The report also did not take into consideration future developments or provide new information regarding the application of network searches and the possibilities of gathering information from cloud services. A basic understanding of these factors and their impact on both evidence-gathering activities and the involved individuals' rights and freedoms is required to adequately assess how Dutch law can regulate computer and network searches.

Nevertheless, it appears that the legislature will propose new regulations for computer searches based on the report's results.[92] The contents of these regulations are still unclear. The Dutch Minister of Security and Justice has not stated that the heightened procedural safeguard of a warrant from an investigative judge will be introduced for computer searches or that authorisation of a public prosecutor will suffice.

Considering recent developments in ECtHR case law with regard to computer searches – to which the Dutch legislature does not refer in official documentation regarding its plans – the procedural safeguard of a warrant requirement appears appropriate from a human rights perspective. Of course, a higher administrative burden for law enforcement officials is expected if a warrant from an investigative judge is required to seize and analyse a computer. However, an investigative judge can check whether public prosecutors have taken sufficient measures to narrow a search down to relevant information. It is imaginable that the evidence must be first secured and filtered using software before the actual search is conducted.

91 Letter of 30 September 2015 regarding the modernisation of the DCCP, p. 84. See also page 8 of the advice of the Dutch police with regard to the proposal to modernise the DCCP. Available at: https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2015/09/30/tk-modernisering-wetboek-van-strafvordering-advies-politie/tk-modernisering-wetboek-van-strafvordering-advies-politie.pdf (last visited on 30 September 2015).

92 See the letter of 29 June 2016 to the Dutch parliament (*Kamerstukken II* 2015/16, 29279, no. 331) concerning the legislation program of Modernising Criminal Procedural Law.

An investigative judge may have more distance with regard to the criminal case and may thus be able to help balance the interests involved. The Dutch Prosecution Service should also consider developing more detailed procedures for computer and network searches to include in its guidelines.[93]

8.4.2 Remote searches

Efforts to regulate remote searches in the DCCP began as early as 2009. The Dutch Minister of Security and Justice stated that investigating cybercrime had become 'extraordinarily difficult' due to encryption techniques and anonymising software.[94] In November 2010, the minister promised to regulate hacking as an investigative method within the Dutch national legal framework and to introduce a new bill.[95] However, no bill was introduced in the following years. In 2013, a concept bill for a new Computer Crime Act (i.e., the Computer Crime Act III) was published, with an accompanying explanatory memorandum that detailed the plans of the Dutch legislature to introduce hacking as a special investigative power in Dutch criminal procedural.[96] The proposal for the Computer Crime Act III was published on 22 December 2015.[97] The regulations for network searches in the DCCP remain untouched in the bill.

The Computer Crime Act III aims to regulate hacking as an investigative method by introducing a new special investigative power in art. 126nba DCCP. This article is supposed to provide a new legal basis for remotely accessing 'automated devices' (computers). Under the proposed investigative power, law enforcement officials can gain remote access to a computer and then conduct the following investigative activities:

(1) ascertain or identify the characteristics of a computer or computer user;
(2) intercept private communications and generated network traffic;
(3) observe the movements of a computer and its user by monitoring GPS data;

93 Inspiration can be drawn from the guideline of the Dutch Consumer and Market Authority ('Autoriteit Consument en Markt'). See 'ACM Werkwijze digitaal onderzoek 2014', 11 February 2014. Available at: https://www.acm.nl/nl/publicaties/publicatie/12594/ACM-Werkwijze-digitaal-onderzoek-2014/ (last visited on 7 May 2016).

94 *Kamerstukken II* 2008/09 (Proceedings of the Second Chamber), 28 684, no. 232, p. 2-3.

95 *Kamerstukken II* 2010/11, 25 November 2010, Answers to parliamentary questions of Recourt, no. 2010Z15331.

96 See the article on the official website of the Dutch government 'Opstelten versterkt aanpak computercriminaliteit', 1 May 2013. Available at: http://www.rijksoverheid.nl/nieuws/2013/05/02/opstelten-versterkt-aanpak-computercriminaliteit.html (last visited on 4 January 2014).

97 See 'Wetsvoorstel Computercriminaliteit III'. Available at: https://www.rijksoverheid.nl/documenten/kamerstukken/2015/12/23/wetsvoorstel-computercriminaliteit-iii (last visited on 30 December 2015).

(4) conduct a remote search and copy data; and
(5) make data remotely inaccessible.[98]

If the bill is eventually adopted as legislation, an *accessible* legal basis for applying a remote search as an investigative method will be available in Dutch criminal procedural law.

However, the current proposal can be criticised with regard to its *foreseeability*, more particularly the *scope* of the proposed special investigative power. For example, one can argue that the term 'automated devices' – to which law enforcement officials can gain access – is rather broad. Automated devices encompass a wide range of items, such as (a) personal computers, (b) smartphones (which are also essentially computers), (c) wearable computing devices, (d) smart refrigerators, and (d) interconnected cars.[99]

At the same time, the rapid pace of technological developments means that new legislation must also be technologically neutral. Specifically with regard to the term 'computer', it will be complicated – if not impossible – to narrow the scope of the definition. For example, restricting the special investigative power to *personal* computers creates uncertainty concerning the question which computers are regarded as 'personal'. For instance, individuals will regard e-mails stored on the servers of a webmail provider as personal, but are those servers – which are owned by a private company – considered 'personal computers'? As a result, the technologically neutral term of 'automated device' is ultimately preferable.

Nevertheless, if the rapid advancements of new technologies and the list of investigative activities provided above are taken into account, it is imaginable that law enforcement officials may find it necessary to hack all kinds of computers (1) for identification purposes, (2) to intercept communications, (3) to track the movements of individuals, (4) to secure data as evidence, or (5) to make data (and thereby possibly computers themselves) inaccessible. It is thus difficult to oversee the scope of this investigative method in the (near) future. Of course, the rationale for creating the proposed special investigative power is essentially to (1) overcome the challenge of anonymity in cybercrime investigation, (2) overcome the challenges of encryption, and (3) collect data that is located 'in the cloud' (i.e., on servers from online service providers that are often housed on foreign territory).[100] The issue is that the proposed special investigative power for hacking as an investigative method is not restricted to overcome these challenges, but leave room for other applications. The proposed special investigative power is not

98 See the proposed art. 126nba DCCP, *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 2, p. 5-6 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 21-31.

99 See section 2.1 with regard to the definition of computers.

100 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 6-15.

restricted to the distinction made for hacking as an investigative method, which subdivides the method into (1) network searches, (2) remote searches, and (3) the use of policeware.

Taking the above observations with regard to the foreseeability of the proposed investigative power into account, my view is that it is desirable to narrow the scope of the investigative method (*Recommendation 2).* The special investigative power can be limited to those applications of hacking that the Dutch legislature truly deems 'necessary in a democratic society'. These applications should then be explained more concretely in legislative history and lower regulations. Furthermore, guidelines from the Public Prosecution Service can indicate the scope of the special investigative power and the manner in which it is applied in a concrete manner.[101]

The proposed new special investigative power in art. 126nba DCCP *meets the desirable quality of the law* for regulating remote searches. This special investigative power is restricted by only allowing its application for crimes stipulated in art. 67 DCCP that 'seriously infringe the legal order' and 'only insofar essential to furthering the criminal investigation'.[102] A public prosecutor must authorise the application of the investigative method. In addition, a special commission of the Public Prosecution Service must be consulted by a public prosecutor before the proposed special investigative power can be applied. Furthermore, a warrant from an investigative judge is required and the warrant's authorisation for applying the special investigative power for remotely accessing computers is restricted to a maximum period of four weeks, which can be extended for another four weeks.[103]

8.4.3 The use of policeware

The use of policeware can arguably already be based on the legal basis of the special investigative power for recording private communications under Dutch law. As such, the regulations for this investigative method are considered accessible. However, the applications of policeware are potentially broader than the special investigative power for recording private communications, since they can also enable law enforcement officials to take a sus-

101 The answer to this question is also political in nature. Based on chapter 2, it can be argued that (1) network searches, (2) remote searches, and (3) the use of policeware, are necessary instruments for law enforcement authorities to overcome the challenges of anonymity and encryption in cybercrime investigations. Whether other applications of hacking can be considered as 'necessary' requires further analysis (including of their backgrounds).

102 Specifically, the applications of remotely turning a GPS signal on and making data remotely inaccessible are restricted to criminal investigations with regard to crimes with a minimum prison sentence of at least eight years and crimes stipulated by lower regulations, such as hacking, malware, distributing child pornography, and grooming. See art. 126nba(1)(c) DCCP and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 29.

103 See the proposed art. 126nba DCCP and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 31-34.

pect's computer over and subsequently take screen shots or gain remote access to the computer system to enable a remote search. It is therefore appropriate to place the use of policeware under the proposed special investigative power for hacking described above as an investigative method.

The use of policeware (as regulated in the proposed special investigative power) can significantly contribute to law enforcement officials' arsenal for overcoming the challenges related to anonymity and encryption. The use of policeware can enable law enforcement officials to overcome the challenge of anonymity, because the software can be directed to send the originating IP address and other identification information about the suspects' computer to law enforcement officials.[104] This investigative power can also enable officials to monitor a suspect's computer behaviours at the source, before network traffic is encrypted (cf. Abate 2011, p. 124).[105] In addition, the keylogging functionality can enable officials to acquire the password a suspect uses to encrypt data and access online services (cf. Fox 2007, p. 828),[106] which they can subsequently use to decrypt data and access information that may not be obtained using other investigative methods. The proposal creates an *accessible* legal basis for the use of policeware with the (additional) functionalities to overcome the challenges of anonymity and encryption in cybercrime investigations.

However, the *foreseeability* of the proposed special investigative power can be improved. Throughout the explanatory memorandum to the Computer Crime Act III, it is implied that policeware will have the following functionalities: (1) recording sounds (by remotely turning a computer's microphone on), (2) logging keystrokes, (3) taking screenshots, (4) remotely gaining access to computers and searching files and folders, and (5) turning a device's GPS signal on.[107] However, the explanatory memorandum also leaves room for other functionalities. Instead, a limited list of functionalities of policeware should be provided by the legislator (*Recommendation 3*). The explanatory memorandum should further elaborate these functionalities (in terms of both their scope and the manner in which they are applied). Furthermore, the functionalities of policeware should be mentioned in both Public Prosecution Service guidelines and lower regulations concerning the use of technical devices. This would ensure that the scope of the special investigative power and the manner in which the power is applied are adequately regulated.

104 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 19-20.

105 See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 10.

106 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 21.

107 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 23, 25-26, 28-30, and 34.

The proposed special investigative power in art. 126nba DCCP *meets the desirable quality of the law* for the use of policeware. As explained in subsection 8.4.2, stringent requirements apply for utilising the proposed investigative power. In relation to the warrant from an investigative judge and the proportionality test, it is important that Dutch law enforcement authorities explain which functionalities of policeware they are going to use. The explanatory memorandum to the Computer Crime Act III indeed confirms that a public prosecutor's request for a warrant to use policeware must state which functionalities of the deployed policeware will be used.[108]

8.5 Chapter conclusion

The aim of this chapter was to determine how the legal framework in Dutch criminal procedural law can be improved to adequately regulate hacking as an investigative method (RQ 4d). To answer the research question, the Dutch legal framework regulating hacking as an investigative method was tested with regard to its (1) accessibility, (2) foreseeability, and (3) desired quality of the law.

The analysis in this chapter has shown that hacking as an investigative method is not regulated in a foreseeable manner in the Netherlands. The legal basis for this investigative method does not adequately restrict the scope of the investigative method and the examples in legislative history appear heavily outdated compared to the current state of technology and application of the investigative method in practice. Technological developments in cloud computing and 'encryption by default' of communications and devices have changed the investigative environment for law enforcement authorities. Hacking as an investigative method offers ways to overcome these challenges under the right conditions, but interferes with the right to privacy in new and intrusive manners. Therefore, hacking should be adequately regulated in order to both (1) provide law enforcement authorities with an instrument for gathering evidence in cybercrime investigations and (2) adequately protect the individuals involved.

The results of the adequacy of the Dutch regulations for this investigative method in terms of the three normative requirements are summarised in subsection 8.5.1. The specific recommendations that stem from these results are then presented in subsection 8.5.2.

8.5.1 Summary of conclusions

Section 8.1 presented an analysis of the accessibility of Dutch regulations for hacking as an investigative method. This analysis showed that detailed regulations are implemented in Dutch criminal procedural law for network

108 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 34.

searches. Based on case law and a letter from the Dutch Minister of Security and Justice, it can also be argued that an accessible legal basis is available for performing remote searches. The use of policeware can be derived from the legal basis of the special investigative power for recording private communications.

In section 8.2, the foreseeability of the Dutch legal framework for hacking as an investigative method was examined. This analysis has shown how modern investigative techniques are based on regulations that were created in the past with different applications in mind. This situation creates ambiguity with regard to the scope of the investigative methods. As a result, the foreseeability of all three types of hacking as investigative methods should be improved.

With regard to network searches, the analysis showed that the investigative method is regulated as a special investigative power in Dutch law. However, the scope of the investigative power and the manner in which the investigative power is applied are not adequately explained in the legal sources. The description of the investigative method in legislative history appears outdated and the investigative method is not even mentioned in guidelines or case law (at least in terms of its practical application). Technology has significantly progressed since the investigative power was first introduced in Dutch criminal procedural law in the early 1990s. As a result, new applications – such as accessing information that is stored in the cloud – are not only imaginable, indications in official documents are that they also take place. The Dutch legislature and Public Prosecution Service should provide clarity about the scope of the investigative method and the manner in which the method can be applied, while at the same time adequately protecting the individuals involved.

With regard to remote searches, Dutch law enforcement authorities have used an extensive interpretation of the special investigative power in art. 125i DCCP that regulates computer searches to apply remote searches. However, remote searches differ substantially from regular searches as they are applied remotely through the Internet instead of during a search in the physical world. In addition, since remote searches are applied covertly, they interfere with the right to privacy in a different – and more intrusive – manner. Dutch law enforcement authorities may therefore have overstepped their legal boundaries in basing remote searches on art. 125i DCCP. A better indication of the legal basis for this investigative method and adequate protection for the individuals involved are therefore merited in Dutch law.

With regard to the use policeware, the legal basis of the special investigative power for recording private communications applies. However, news articles indicate that functionalities of policeware have been used in practice that go beyond 'recording private communications', which creates ambiguity with regard to (1) the scope of the investigative method and (2) the manner in which policeware is now actually being used. For that reason, the investigative method is not regulated in a foreseeable manner.

Section 8.3 investigated whether the regulations for hacking as an investigative method meet the desired quality of the law. Detailed regulations and a warrant requirement were identified as an appropriate quality of the law for regulating the investigative method of network and remote searches. Currently, the applicable procedural safeguards for network and remote searches depend on where a search takes place. These regulations do not meet the desired quality of the law. Instead, the procedural safeguard of a warrant from an investigative judge should always apply. The detailed regulations and corresponding stringent procedural safeguards that apply to using the special investigative power for recording private communications meet the desired quality of the law.

8.5.2 Recommendations

Section 8.4 presented three recommendations to improve the Dutch legal framework for hacking as in investigative method. These recommendations followed the analysis of the adequacy of the Dutch legal framework based on the three normative requirements section 8.1 to 8.3. These recommendations are as follows.

1. Network searches seriously interfere with the involved individuals' right to privacy. Therefore, the existing special investigative power for network searches (art. 125j DCCP) should be amended and incorporate the requirement of a warrant from an investigative judge as a procedural safeguard.
2. A new special investigative power that enables law enforcement officials to remotely access computers as an investigative method should be created in Dutch criminal procedural law. In this context, the unique and intrusive privacy interferences that arise when this investigative method is applied merit a distinct legal basis. The proposed special investigative power for hacking as an investigative method in the Computer Crime Act III is a step in the right direction. However, the Dutch legislature should carefully scrutinise the scope of the proposed investigative power. The investigative method's current particularly broad formulation corrodes its foreseeability. Therefore, it is desirable to narrow its scope and explain the applications of this special investigative power more concretely in the explanatory memorandum and lower regulations. Furthermore, Public Prosecution Service guidelines can indicate the scope of the special investigative power and the manner in which it is applied in a concrete manner.
3. Dutch criminal procedural law should be amended to introduce a special investigative power that authorises law enforcement authorities to use policeware. As this investigative method is intrusive in terms of privacy and has many functionalities, specific provisions and appropriate procedural safeguards are justified. The proposed special investigative power for hacking as an investigate method could provide an adequate

a legal basis for this method. Due to its strict application requirements, the special investigative power meets the desired quality of the law. However, in order to meet the foreseeably requirement, a limited list of the functionalities of policeware should be provided by the legislator. The scope and the manner in which these functionalities are applied should be detailed in the explanatory memorandum. The software's functionalities should also be mentioned in both Public Prosecution Service guidelines and lower regulations concerning the use of technical devices.

Answer to research question 4

The answers to RQ4a to RQ4d in chapters 5 to 8 present an overview of the adequacy of the Dutch legal framework with regard to regulating the digital investigative methods identified in this study. As expected, the accessibility of the Dutch legal framework's regulations for these digital investigative methods did not pose major problems. The heightened criminal legality principle in Dutch criminal procedural law and the introduction of detailed regulations for special investigative methods with the Special investigative Powers Act in the late 1990s have contributed to a solid general legal basis for applying these investigative methods. However, the analyses of the two other normative requirements of foreseeability and the quality of the law produced results that are more significant. Two general observations regarding the adequacy of the Dutch legal framework vis-à-vis regulating digital investigative methods follow below.

First and foremost, *foreseeability* is lacking in relation to the regulation of digital investigative methods in the Dutch legal framework. The analyses in chapters 5 to 8 showed that Dutch law enforcement authorities have already been applying the identified investigative methods for years. However, the regulations for these investigative methods are either (1) non-existent or (2) ambiguous as to the scope and manner in which the methods are executed by law enforcement authorities. The Dutch legislature should urgently realise that evidence-gathering activities are taking place in an environment that is different from the one that existed a decade ago, when Dutch criminal procedural law was last updated to combat cybercrime. The analyses in chapters 5 to 8 have shown that the traditional investigative methods of (1) gathering open source information, (2) data production orders, (3) undercover investigations, and (4) computer searches have been transformed by the digitalisation of the environment in which law enforcement officials now conduct evidence-gathering activities. The Dutch legislature should thus move to update criminal procedural law to both (1) provide law enforcement authorities with the instruments they need to gather evidence and (2) adequately protect the individuals involved. In addition, the Public Prosecution Service has a responsibility to state the scope of and manner in which these novel investigative methods are applied in practice within (public) guidelines to contribute to a clear and foreseeable legal basis for digital investigative methods.

Second, the analyses in chapters 5 to 8 have shown that the *quality of the law* should be improved, particularly in relation to undercover investigative methods and hacking as an investigative method. The quality of the law can improved by implementing stricter procedural safeguards in the corresponding detailed regulations. The privacy interferences that accompany digital investigative methods must be interpreted in light of present-day standards (see chapter 3). As a result, the legal framework for investigative methods require amendments now, whilst the legal framework should also be continually monitored for amendments in light of new technological developments.