The Police Hack Back

Legitimacy, Necessity and Privacy Implications of The Next Step in Fighting Cybercrime

RLD Pool & BHM Custers

Abstract. In an attempt to strengthen the position of the police to fight cybercrime, the Dutch government proposed new legislation giving police agencies new investigative powers on the Internet. This proposed legislation is controversial as it allows police agencies to hack into computers and install spyware. This paper examines the background and contents of the proposed legislation and tries to answer the question to what extent these new investigative powers may result in infringements of the right to privacy and other fundamental rights of citizens, and whether these infringements are justified. The framework for this evaluation, mainly based on the European Convention on Human Rights, focuses on the legitimacy and necessity of the proposed investigative powers. The most important considerations are that new investigative powers are introduced while existing powers are not used adequately and that there are serious doubts as to whether these new investigative powers will be effective.

Keywords: Cybercrime, ECHR, Hacking, Investigative Powers, Privacy, Technology in Policing

1. Introduction

Across Western countries, crime rates have been dropping for several years now.[1] Cybercrime may be an exception to this trend.[2] This may not be surprising, as cybercrime is a phenomenon of the last decades and therefore relatively new compared to other types of crime. Furthermore, criminals can make large amounts of money with several types of cybercrime, such as banking malware and ransomware.[3]
Since cybercrime is a relatively new phenomenon and is developing rather fast, in some cases investigative powers of the police may not be sufficient to fight this type of crime. For instance, in most countries police surveillance in the streets and neighbourhoods is, generally speaking, legitimate and accepted by citizens. However, internet surveillance is something

[1] J. van Dijk, A. Tseloni, and G. Farrell, *The International Crime Drop* (London: Palgrave Macmillan, 2012). For the US, the FBI crime statistics at https://www.fbi.gov/stats-services/crimestats. See also S.D. Levitt, 'Understanding Why Crime Fell in the 1990s: Four Factors that Explain the Decline and Six that Do Not', 18 *Journal of Economic Perspectives*, No. 1 (2004) pp. 163-190. For the EU, see the Eurostat crime statistics at http://ec.europa.eu/eurostat/statistics-explained/index.php/Crime_and_criminal_justice_statistics.

[2] According to security experts, statistics on cybercrime are unreliable due to failure to report, self-selection bias, no standard mechanisms for accounting for losses and undetected losses. See P. Hyman, 'Cybercrime: It's Serious, But Exactly How Serious', 56 *Communications of the ACM*, No. 3 (2013) pp. 18-19.

[3] Europol, The Internet Organised Crime Threat Assessment (iOCTA) 2015 (The Hague, 2015). See https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015. B. Krebs, 'Inside the $100M 'Business Club' Crime Gang' (5 August 2015). See http://krebsonsecurity.com/2015/08/inside-the-100m-business-club-crime-gang/

that is much more controversial, for instance, because of jurisdiction issues and user's privacy expectations.[4]

As a result of these developments, police agencies and prosecution services are experiencing pressure from politicians and the public to increase the fight against cybercrime, while at the same time feeling insufficiently equipped for this task.[5] In an attempt to strengthen the position of the police to fight cybercrime, the Dutch government proposed new legislation allowing police agencies new investigative powers on the Internet. This proposed Act on Cybercrime was unveiled by the Dutch government in May 2013 and displays a rather bold change in policy. While the Netherlands has always been relatively progressive when it comes to cybercrime legislation, the proposed legislation is controversial as it gives criminal investigators the right to (i) hack into computers ('hacking back') and install spyware and to (ii) destroy or disable access to files with the 'notice and take down' (NTD) order.

The proposed legislation, which was most recently discussed in December 2015 in the Dutch Parliament, aims to restore the balance between the criminal investigation technologies and technological developments of the past years. While the aim of the proposed legislation sounds very reasonable, the suggested powers have far-reaching consequences for citizens. The new investigative powers may interfere with the right to respect for private life and family life (Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, ECHR) and other human rights, including freedom of thought (Art. 9 ECHR), freedom of expression (Art. 10 ECHR) and freedom of assembly and association (Art. 11 ECHR). Next to the ECHR, which was adopted in the framework of the Council of Europe, the EU decided to put all rights in the Charter of Fundamental Rights of the European Union. While this Charter is consistent with the ECHR, it is less extensive on the right to privacy and other freedoms. The ECHR specifies that restrictions of and interferences with these rights can only be allowed in particular, exceptional circumstances. For instance, interference with the right to privacy by a public authority is only allowed in accordance with the law and when necessary for a limited number of reasons, including national security, public safety, or the prevention of crime. This leads to the key question of this paper: To what extent does allowing the police to hack back described in the proposed legislation in the Netherlands justify interference with the right to privacy and other human rights of citizens?

In order to answer this question, this paper starts with examining the background and contents of the proposed legislation in Section 2. Section 2 also provides some background on the cybercrime legislation in the Netherlands, in order to provide a full picture of the issues at stake. In Section 3 the normative legal framework is put forward to assess justifications of interferences with the right to privacy and other human rights of citizens. This framework, mainly based on the ECHR, focuses on the legitimacy, necessity and effectiveness of the investigative powers of police agencies. Next, in Section 4, the proposed legislation (specifically the proposed investigative powers for police agencies to hack back) is assessed against the normative legal framework. The focus will be on the right to privacy, as this right plays a central role in the analysis of the investigative power of the police to hack back. Section 5 provides conclusions.

---

[4] M. Hosenball and J. Whitesides, 'Reports on surveillance of Americans fuel debate over privacy, security', *Reuters* (7 June 2013), http://www.reuters.com/article/us-usa-wiretaps-verizon-idUSBRE95502920130607. J. Stanley, and B. Steinhardt, *Bigger Monster, Weaker Chains; The Growth of an American Surveillance Society*, (New York: ACLU, 2003). For more on user's privacy expectations, see, for instance, B. Custers, S. van der Hof, B. Schermer, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies', 6 *Policy & Internet*, No. 3 (2014) pp. 268-295.

[5] For police needs and experiences regarding technologies, see B. Custers, B. Vergouw, 'Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies', *Computer Law & Security Review*, 31 (2015) pp. 518-526.

2. A Short History of the Cybercrime Legislation

The internet has become a cross-border tool for criminals to commit a range of criminal activities. This is related to the fact that the internet is deterritorialised, flexible and developing at a very fast rate.[6] In this section we discuss the history of cybercrime legislation in the Netherlands, in order to provide some more background for better understanding the legislation that is now proposed.

2.1 The beginning of the Dutch Cybercrime Legislation

The introduction of the Computer Crime Act (*Wet Computercriminaliteit*) in 1993 marks the beginning of cybercrime legislation in the Netherlands.[7] From then onwards, new measures were introduced to specifically tackle cybercrime. The Computer Crime Act, rather than being an act in itself, changed the Dutch Criminal Code (*Wetboek van Strafrecht*, hereafter: DCC) and the Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*, hereafter: DCCP), by adding new articles specifically addressing cybercrime and amending some existing articles in order to ensure cybercrime is in their scope. The instigation of the Computer Crime Act was at least partially the result of the Computer Crime Committee (*Commissie Computercriminaliteit*) in 1985, also known as the Commissie Franken. In 1987 an extensive report with recommendations was presented.[8] This led to the Computer Crime Act that was submitted to parliament in 1990. This Act largely followed the committee's recommendations, except for the search and seizure provisions. The Computer Crime Act of 1993 regulates criminal investigation of digitalized information and computer networks. It also makes a criminal offence of computer trespass. Various amendments and a debate in Parliament led to the final version of the Computer Crime Act that came into effect on 1 March 1993. Leading up to the Computer Crime Act there was a heated discussion about the legal qualifications of data, particularly whether to consider this a commodity or not. After all, a commodity in criminal law concerns a unique object, whereas data can be multiple and can be duplicated. This can be clarified with the example of theft: under Dutch criminal law, theft is usually defined as something like 'taking away an object from someone else'. However, when 'taking away' data from someone else, the data is usually copied and the original owner still has the data. The Dutch legislator decided that computer data were not to be considered as chattels. In 1996 a case reached the Dutch Supreme Court for a final verdict on the matter and it was confirmed by the court that data indeed are not chattels.[9]

The Computer Crime Act of 1993 was followed by the Computer Crime Act II, which was proposed in 1999 to the parliament.[10] This Act was intended to refine and update several provisions of the Computer Crime Act suggesting new changes and additions to the DCC and the DCCP. The parliamentary processing of this Act was slowed down because of the drafting of the Budapest Cybercrime Convention (hereafter: CCC), since it was considered better to integrate the Computer Crime Act II with the implementation of this convention. The CCC

[6] D.D. Denning & W.E. Baugh Jr, 'Hiding Crimes in Cyberspace,' in D. Thomas and B.D. Loader, eds., *Cybercrime: law enforcement, security and surveillance in the information age*, 3rd ed. (London: Routledge, 2000). See also: M.E.A. Goodwin & B.J. Koops, *Cyberspace, the cloud and cross-border criminal investigation. The limits and possibilities of international law.* (The Hague: WODC/TILT, 2015).

[7] It should be pointed out that in the Netherlands the term to indicate crimes committed with computers as a target or tool is 'computer crime' rather than cybercrime, as the latter term was not yet in use at the time Dutch legislation was initiated in the 1980s.

[8] Report *Informatietechniek en Strafrecht* 1987.

[9] Dutch Supreme Court 3 december 1996, *NJ* 1997, 574.

[10] Parliamentary Papers II (*Kamerstukken II)* 1998/99, 26 671, nr. 1-3.

was the first international treaty on crimes committed via the internet. The main objective was to harmonise criminal policy and foster international cooperation.[11] In 2005, a bill to ratify the Cybercrime Convention was submitted to parliament, and shortly after that a Memorandum of Amendments to the Computer Crime Act II was published, that implemented, where necessary, the CCC. The Computer Crime Act II (*Wet Computercriminaliteit II*) was accepted by parliament on 1 June 2006 and is effective since 1 September 2006. The Cybercrime Convention Ratification Act was accepted at the same time; it is effective in the Netherlands since March 2007. The Computer Crime Act II regulates, among other things, decryption of data in criminal investigations, the distinction between stored data and streaming data, investigation of e-mail and investigation of public computer networks. Furthermore, it makes criminal offences of serious forms of spam and of changing, deleting or rendering inaccessible data in some situations.
With respect to the subject of this paper, one change in the Computer Crime Act II is of particular importance, namely that of computer trespass. This basically refers to 'hacking' although it should be pointed out that the term 'hacking' is never used in the DCC. In the old Art. 138a DCC computer trespass depended on any form of security being breached. In 2006, with the introduction of the Computer Crime Act II, that requirement has been changed. The present provision (Art. 138ab DCC) designates any intentional intrusion to be punishable in the Netherlands and it is not necessary for the hacker to know that his conduct was unlawful.

2.2 The Proposed Computer Crime Act III

Cybercrime is developing along with new technologies.[12] Obviously, criminal law and criminal procedure law need to be up to date with these developments in order to be able to address cybercrime properly. In an attempt to restore the balance between technological developments and investigative powers, the Dutch government proposed the Computer Crime Act III to the parliament in December 2015. This Act was part of a set of four new bills that were sent to parliament as part of the Anti-terrorism action plan.[13]
The Computer Crime Act III proposes to change the DCC and the DCCP. The most important changes are the newly proposed investigative powers for police and law enforcement agencies to (i) hack into computers ('hacking back') and install spyware and to (ii) destroy or disable access to files with the 'notice and take down' (NTD)-order. In this paper we focus on the power that probably has most consequences for the rights of citizens, namely the right to hack back.
The right to hack back (criminal investigation in digitalized information and computer networks) would be allowed for criminal investigation officers in cases of suspicion of a serious offence (listed in the proposed legislation) when ordered by the public prosecutor. The purposes for which this investigative power can be used are limited and include establishing characteristics of the data, the computer system or the user (including identity and location), for placing taps and for 'finding the truth'.
The Explanatory Memorandum to the proposed Computer Crime Act III mentions three developments that call for the introduction of this investigative power: (1) the encryption of electronic data, (2) the use of wireless networks, and (3) the use of cloud services. Below we will briefly examine these developments in order to give a picture of how the legislator views these developments.

[11] Full text available here: www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561
[12] For recent developments in cybercrime, see Europol, *The Internet Organised Crime Threat Assessment (iOCTA) 2015* (The Hague, 2015). See https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2015.
[13] Parliamentary Papers II (*Kamerstukken II*) 2015/16, 34 372, no. 4.

The first development, the encryption of electronic data, is relevant with regard to tapping. It is already possible to tap internet traffic from a specific IP address.[14] Recent figures from the Ministry of Security and Justice in the Netherlands show that nearly 17,000 Internet connections were tapped in 2012. That was about five times as many connections as in 2011, when some 3,300 connections were tapped. The reason for this growth is the increase in the number of smartphones, for which both a telephone and IP-tap is required.[15] To add some perspective, the figures for telephone taps increased only slightly from 25,487 in 2012 to 26,150 in 2013. From 2014 onwards telephone and internet taps are no longer reported separately. Only the aggregated tapped connections are reported - total 25,181 in 2014.[16]
The encryption of electronic data is a growing problem for police agencies. Encryption makes data unreadable by means of an algorithm and the data can only be made readable again with a so-called decryption key. As a result, encryption makes it impossible to read the tapped internet traffic. Only unencrypted traffic can be inspected. In fact, more communications services, such as Twitter and Gmail, are already using encryption as a standard. Other services like Facebook and Outlook.com also provide the option for encryption. In the case of an internet tap this would mean that internet traffic from 'http://www.website.com' is visible, whereas for 'https://www.website.com' the traffic is encrypted. In addition, 'https' websites allow for the authentication of the website and server, which in turn provides privacy and integrity of exchanged data. However, there are restrictions to such internet taps because (i) the Internet Service Provider (ISP) in many cases cannot decrypt (despite the requirement in Art. 126m paragraph 6 DCCP), (ii) the intermediate provider does not fall under the definition, or (iii) the intermediate provider is located abroad. Furthermore, the Explanatory Memorandum mentions the use of the TOR network (The Onion Router) as a problem. The Onion Router is a piece of software, which enables surfing anonymously on the internet. By connecting through a series of virtual IP-addresses one is protected from privacy compromises and internet traffic analysis.
The second reason is related to the ability to intercept communications. With the use of wireless networks the Explanatory Memorandum mainly refers to the use of *different* wireless networks. Today, wireless connectivity is available in many public spaces, such as (offered for free) in restaurants and trains. When using the Internet via a wireless connection, it is difficult for the investigative authorities to intercept a communication. Also other forms of communication, such as optical communication, raise challenges for tapping.[17] An internet tap is issued for a specific IP address and a user cannot be traced when he connects to another router. It is the telecommunications infrastructure of today that makes it practically impossible to tap someone constantly. The current investigative powers extend no further than intercepting and recording traffic from an access point. Besides the fact that this makes it virtually impossible to monitor the full communication of the suspect, a tap on a router also implies that all the data of persons who are not suspected of a crime are tapped. The possible infringement of the privacy of these third parties is a crucial aspect and the Explanatory Memorandum seems to have a good starting point for new investigative powers. According to the explanation, there is now a need for the ability to penetrate into computers to identify the machine of the suspect. In this way investigative authorities can conduct a more focused search for information and it is also possible to monitor a user more constantly.
The third development discussed in the Explanatory Memorandum is the increased use of cloud services. These include, amongst others, storage services like Dropbox and Google

[14] Art. 126m DCCP.
[15] Parliamentary Papers II (*Kamerstukken II)* 2013-2014, 33 930 VI, nr. 1, p. 50.
[16] Parliamentary Papers II *(Kamerstukken II*) 2013–2014, 33 930 VI, no. 1, Appendix, p. 17.
[17] B.H.M. Custers, 'Tapping and Data Retention in Ultrafast Communication Networks', 3 *Journal of International Commercial Law and Technology*, Issue 2, (2008) pp. 94-100.

Drive. There is a tendency to keep information at hand at all times. Data is therefore stored increasingly in the cloud rather than on a hard drive of the computer. The problem is that this data is stored on servers which are often located abroad. According to the Dutch government the current powers are not sufficient to collect evidence from computers located abroad.[18]

3. Normative Framework of Fundamental Human Rights

Before elaborating on the investigative powers of the Computer Crime III Act, it is important to discuss the legal framework regarding human rights. Based on this framework it can then be determined whether there is a violation of fundamental human rights. One of the strongest arguments against the introduction of the new investigative powers is the protection of privacy. The right to privacy plays a central role in this section. In section 3.1 the right to privacy is examined and in section 3.2 the impact of the proposed investigative power to hack back on this right to privacy is analysed from a legal perspective.

3.1 The Right to Privacy

Whenever investigative powers are expanded, interference with the right to privacy may be a risk. It is possible to use the newly suggested investigative power of hacking for both perpetrated and planned criminal offences. In the Dutch Constitution the right to privacy is covered in Art. 10-13. Art. 10 states that 'everyone has […] the right to respect for his private life.' The legislation does not contain a specific definition of the concept of private life or privacy. Further elaboration of the concept of 'private life' therefore has become a task for the court.[19] In addition, Art. 11 (inviolability of the human body), Art. 12 (trespassing into a home) and Art. 13 (privacy of correspondence, telegraph and telephone) give a specification of the privacy provisions in the Constitution. However, it is not so much the articles in the Constitution but rather international treaties and conventions that determine the protection of privacy. The Dutch Supreme Court has determined that Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) plays a fundamental role when it comes to privacy judgments.[20]
The right to privacy is not absolute - in paragraph 2 of Art. 8 ECHR a number of conditions are imposed which may justify an infringement of the fundamental right. Looking at the second paragraph, there are three questions raised by the European Court of Human Rights (ECtHR) which ought to be assessed:

1. Is the interference in accordance with the law?
2. If so, does the interference have a legitimate aim?
3. Is the interference necessary in a democratic society?[21]

Case law shows that the ECtHR has never attempted to define privacy. In the early nineties the ECtHR even found that it was impossible and unnecessary to define the concept of privacy.[22] Instead the ECtHR looks at each case based on the three questions above to assess whether there is a breach of Art. 8 ECHR.
First, there must be a sufficiently clear basis in national law. This is marginally tested by the ECtHR because the national judge has a better insight into their own legislation. Case law

[18] Explanatory Memorandum, p. 10. Note that the proposed act also allows for access to systems located abroad, as long as this is in accordance with international laws, see: Explanatory Memorandum, p. 34-35.
[19] Parliamentary Papers II (*Kamerstukken II*) 1978/79, 13 872, nr. 3, p. 40.
[20] Dutch Supreme Court 9 January 1987, *NJ* 1987, 928.
[21] Parliamentary Papers II (*Kamerstukken II*) 1996/97, 25 403, nr. 3, p. 10.
[22] ECtHR 16 December 1992, nr. 13710/88 (*Niemietz v Germany*).

also shows that this question looks at the requirements of accessibility and foreseeability.[23] The accessibility relates to the fact that citizens should have knowledge of the law. For this, the law must be published.[24] The foreseeability refers to the possibility for citizens to determine when investigative powers are used and what safeguards there are to prevent arbitrary use. In *Amann v Switzerland* the ECtHR determined that:

'Tapping and other forms of interception of telephone conversations constitute a serious interference with private life and correspondence and must accordingly, be based on a 'law' that is particularly precise. It is essential to have clear, detailed rules on the subject especially as the technology available for use is increasingly becoming more sophisticated.'[25]

Second, a legitimate aim makes it possible to limit privacy. In paragraph 2 of Art. 8 ECHR, an exhaustive list of these legitimate aims is provided. This involves among other things the protection of national security, public safety or the economic well-being of the country, and the prevention of disorder or crime. The first and second question address legitimacy.
The third criterion is the necessity in a democratic society. In the *Sunday Times* judgment, the ECtHR stated that this is a *pressing social need* and that the measure should be *proportionate* to the aim pursued. For this reason, the necessity test is sometimes also referred to as a proportionality test, indicating that the focus is on balancing different interests.[26] However, since the ECtHR does not provide further structure in its rulings, [27] it is not clear how 'necessity in a democratic society' could or should be tested. A widely accepted approach is one proposed by Robert Alexy, who also calls this test a proportionality test and splits the test into suitability, necessity and proportionality *strictu sensu*.[28] The suitability is an assessment of the extent to which a measure actually contributes to realizing the set goals. In line with more recent publications, we will refer to this as *effectiveness*.[29] This term even more expresses the target oriented approach of the test and the different grades that may exist in achieving the set goals. The necessity, according to Alexy, assesses whether there are alternatives that interfere less with privacy and other human rights than the proposed measure. We will refer to this as *subsidiarity*, a common legal term that is less confusing than the term necessity that also is used for the three combined tests. Finally, the proportionality *strictu sensu* assesses the extent to which the impact of a measure is proportionate to the goals it aims to contribute to. We will refer to this simply as *proportionality*, since we do not use this term otherwise and no confusion can occur. In summary, the criterion 'necessary in a democratic society', is tested in the next section by assessing whether the investigative power (i.e., the power to hack back) actually contributes to combat crime (effectiveness), whether the same result could be achieved with less intrusive means (subsidiarity) and whether the interference with the right to privacy and other rights is proportionate to the goals (proportionality).

3.2 Hacking Back and the Suspect's Privacy

[23] ECtHR 26 April 1979, nr. 6538/74 (*Sunday times v United Kingdom*).
[24] ECtHR 30 March 1989, nr. 10461/83, § 56 (*Chappell v United Kingdom*).
[25] ECtHR 16 February 2000, nr. 27798/95 (*Amann v Switzerland*).
[26] Or, in other words, the conditions of effectiveness and subsidiarity are regarded as part of the proportionality test. P. Craig and G. De Burca, *EU Law* (Oxford: Oxford University Press, 2011).
[27] See also J. Gerards, 'How to improve the necessity test of the European Court of Human Rights', 11 *International Journal of Constitutional Law*, No. 2 (2013) pp. 466-490.
[28] R. Alexy, 'Constitutional Rights, Balancing and Rationality', 16 *Ratio Juris*, No, 2 (2003) pp. 131-140.
[29] See, for instance, J. Gerards, 'How to improve the necessity test of the European Court of Human Rights', 11 *International Journal of Constitutional Law*, No. 2 (2013) pp. 466-490.

The investigative power of hacking back is aimed at collecting information about persons or criminal activities. People often assume that the integrity of their personal computer is guaranteed. In an important judgment of February 22, 2011, the Supreme Court in the Netherlands affirmed that data on a computer that has unlawfully been accessed through a hack cannot be seen as openly available information.[30] It is striking that there is no case law of the ECtHR on the personal computer as an extension of the private domain, especially in view of the role digital technology plays in our society and sensitive data being stored. The treaty text of the ECHR does not elaborate on it either. However, with regard to the integrity of computer systems and privacy, the ECtHR has determined that:

'The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of Article [8 of the Convention]. The need for such safeguards is greater when the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes.'[31]

Furthermore, the ECtHR has also confirmed that the interception of communications and recording of confidential communications under certain circumstances can be considered a violation of Article 8 ECHR.[32] According to the ECtHR no distinction should be made between forms of eavesdropping and also found a breach of privacy law in this case. Given the technology used for tapping, the importance of clear legislation was again stressed in the judgment:

'The Court does not consider that the domestic law at the relevant time indicated with sufficient clarity so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicant's rights under Article 8 was not, therefore, "in accordance with the law".'[33]

All in all, the intrusion into a computerised device, without the consent of the owner, can result in a significant infringement of the right to privacy. This also applies to a suspect of a crime. A suspect of a crime also has a right to privacy. By excluding this right in advance the government would renounce its duty of care to guard fundamental rights of all citizens.
As a result, there will be a violation of the right to privacy to some extent in most cases in which computers are hacked. It is clear that this will not be different when the police hack into systems. In all cases, the main rule is that the infringement of the right to privacy of the subject is only justified when the cumulative requirements under Article 8 paragraph 2 of the ECHR are met.

4. Legitimacy and Necessity of Hacking Back

Using the legal normative framework set out in the previous section, the legitimacy (i.e., accordance with the law and legitimate aims) and necessity (i.e., the effectiveness, proportionality and subsidiarity) of the proposed investigative power to hack back can be

[30] Dutch Supreme Court 22 February 2011, *LJN* BN9287.
[31] ECtHR 4 December 2008, nr. 30562/04, § 103 (*S. and Marper v United Kingdom*), ECtHR 17 December 2009, nr. 22115/06, § 53 (*M.B. v France*).
[32] E.g.: ECtHR 2 August 1984, nr. 8691/79 (*Malone*), ECtHR 12 May 2000, nr. 35394/97 (*Khan v United Kingdom*), ECtHR 1 July 2008, nr. 58243/00, § 69 (*Liberty v United Kingdom*).
[33] ECtHR 1 July 2008, nr. 58243/00, § 69 (*Liberty v United Kingdom*).

assessed. As is shown in the ECHR and European case law, the use of investigative powers must be fully justified by the law. Over the years, the rule of thumb was developed that all investigative methods should have a clear legal basis in order to be legitimate. For this reason, the Dutch government proposed the Computer Crime Act III as a clear legal basis for the investigative power to hack back. By proposing this Act, the first condition (accordance with the law) will be met.
The second condition (legitimate aim) requires looking at the limited number of reasons for which interference by a public authority with the right to privacy may be allowed. These reasons are mentioned explicitly in paragraph 2 of Art. 8 ECHR and include national security, public safety, or the prevention of crime. The aim of the proposed legislation, i.e., fighting cybercrime, seems in line with the interests of national security, public safety and the prevention of crime. Hence, the second condition is also met.
The third condition (necessity in a democratic society) can be assessed by looking at the effectiveness and the subsidiarity and proportionality of the proposed measures. The *effectiveness* relates to the extent to which a measure, in this case an investigative power, contributes to realizing the set goals. Hence, in this case the question is whether the investigative power to hack back contributes to preventing or solving crime or yields any evidence that may be used in court. If this is not the case, i.e., when hacking back is unlikely to help criminal investigation, the proposed investigative power cannot be necessary. The *proportionality* relates to the extent to which the impact of a measure, i.e., the extent to which it may interfere with the interests of a suspect and others, is proportionate to the goals that measure aims to contribute to. Hence, the proportionality test asks the question whether a measure, in this case hacking back, is reasonable when considering competing interests. Finally, the *subsidiarity* relates to the extent to which the set goals could also be achieved in other ways that perhaps interfere less with the interests of a suspect and others. If there are other investigative powers available that interfere less with human rights, they are preferable to use and render the investigative power to hack back unnecessary. In the sections below we will discuss the effectiveness, the proportionality and the subsidiarity of the proposed investigative power for the police to hack back.

4.1 Effectiveness

The starting point, according to the Explanatory Memorandum of the proposed legislation, for assessing the necessity, and particularly the effectiveness, of the investigative power to hack back are the three technological developments (i.e., encryption, wireless communication and cloud computing) which play an increasingly important role and, with the global nature of the Internet, further complicate criminal investigations. The main argument is that due to these technological developments, the police are insufficiently equipped to fight cybercrime. When testing the effectiveness of the proposed investigative power for the police to hack back, the question is: would this investigative power help the police to do a better job fighting cybercrime?
Research in this area indicates that it is not mainly a lack of adequate investigative powers that hinders the police in fighting cybercrime. On the contrary, the available research seems to suggest that the police make insufficient use of existing investigative powers. One Dutch study identifies three issues, namely the lack of operational capacity, control and situational awareness.[34] Another Dutch study concludes that the fight against cybercrime could be

[34] R. Prins, 'Polderen tegen cybercrime', *Security Management,* 6 (2011) p. 28.

improved when centralised.[35] And in fact, even the government has admitted that it lacks the knowledge and capacity to effectively fight cybercrime.[36]
When looking at the question to the extent to which the proposed investigative power for the police to hack back is able to overcome problems encountered with regard to encryption, wireless communication and cloud computing, it is questionable whether these issues will be solved.[37] In cases of weak encryption the police may be able to decrypt information, but in the case of strong encryption this may turn out to be difficult. Furthermore, cybercriminals often work via TOR networks to protect themselves and use hidden services on the Dark Web.[38]
The other two technological developments, wireless communication and cloud computing, are more related to interception problems than to hacking. Here the key issue is where to intercept or tap information rather than the legitimacy of hacking back. There may be jurisdiction issues involved in wireless communication and cloud computing, but these are not likely to be influenced by the investigative power to hack back, because the applicability of the law depends on the state where the computer or other automated deviceis located.[39] The Dutch legislator specified in the Cybercrime Act I that if a computer system is located abroad the use of investigative powers is not allowed, unless there is consent of the other state.[40] Case law indicates that the consent can be ad-hoc (also implicitly) or given by a treaty.[41] This principle can also be found in Art. 539a paragraph 3 DCCP. According to the Explanatory Memorandum to the Cybercrime Act II, using data as evidence would be admissible if the location of the server is unknown. However, how this works in practice remains unclear.[42]
The Explanatory Memorandum is not quite convincing that the proposed investigative measures will be effective. The problems are discussed but there is no clarification how the new investigative power to hack back can address the three technological developments that would make this investigative power necessary. Looking at the proposed measures and the set goals, it is questionable how effective the power to hack back will be as an investigative method. The fact is that there is still a lack of knowledge. Alternatively, it is important that knowledge on the effective use of the current investigative powers is evaluated first. This may better ensure that existing investigative powers are used to their maximum potential.

4.2 Proportionality

As discussed in Section 3, the right to privacy is not absolute. Both the Dutch Constitution and the ECHR provide exceptions that may justify interference with the right to privacy. However, restrictions to the right to privacy and other fundamental rights must be proportionate to the set goals. When there is no proportionality, a proposed measure is not considered to be necessary (or rather: desirable) in a democratic society. Hence, the

[35] N. Struiksma, C.N.J. De Vey Mestdagh & H.B. Winter, *De organisatie van de opsporing van cybercrime door de Nederlandse politie* (Amsterdam: Reed Business, 2012).
[36] Parliamentary Papers [*Kamerstukken II*] 2012/13, 29 911, nr . 79, 13 March 2013.
[37] S.D. Moitra, 'Developing Policies for Cybercrime', 13 *European Journal of Crime, Criminal Law and Criminal Justice*, Issue 3 (2003) pp. 435 –464.
[38] D. Moore & T. Rid, 'Cryptopolitik and the Darknet', *58 Survival: Global Politics and Strategy,* Issue 1 (2016), pp. 7-38.
[39] A.H. Klip, 'Soevereiniteit in het strafrecht', in: G.J.M. Corstens & M.S. Groenhuijsen, eds., *Rede en Recht: opstellen ter gelegenheid van het afscheid van prof. mr. N. Keijzer van de Katholieke Universiteit Brabant* (Deventer: Gouda Quint, 2000) p. 140.
[40] Parliamentary Papers [*Kamerstukken II*] 1989/90, 21 551, nr 3, p. 11-12.
[41] M.E.A. Goodwin & B.J. Koops, *Cyberspace, the cloud and cross-border criminal investigation. The limits and possibilities of international law.* (The Hague: WODC/TILT, 2015). See: Dutch Supreme Court 16 april 1985, *NJ* 1986, 769; Dutch Supreme Court 7 juni 1988, *NJ* 1988, 987.
[42] Parliamentary Papers [*Kamerstukken II*] 2004/05, 26 671, nr. 10, p. 23.

proportionality test is a reasonableness test, as it asks whether hacking back is reasonable when considering competing interests.
Obviously it is difficult to balance these competing interests as they are different in their size and nature. The benefits of the proposed legislation for the police are mainly constituted by its effectiveness (see above). Other benefits may consist of increased efficiency, which will be discussed below. When looking at competing interests, i.e., the interests of citizens, it is clear that the proposed investigative powers deeply affect the fundamental human rights of citizens.
There are several measures that are included in the proposed legislation to make the proposed power to hack back more proportionate. For instance, the use of the new investigative power is subject to prior approval by the Central Review Committee (*Centrale Toetsingscommissie* - CTC). The CTC is a Dutch national advisory body of the Public Prosecution Service and advises on the proportionality and subsidiarity of special investigative techniques. The public prosecutor needs permission from this committee before special investigative powers may be exercised in a particular criminal investigation. In addition, the public prosecutor requires a written authorization from the court. Although the checks of the CTC and the court offer additional protection for citizens, some Dutch authors call for a specialised court to handle these matters.[43] These plans are not apparent from the Explanatory Memorandum, but it is of fundamental importance that courts examining these issues are knowledgeable on the subject and make reasonable assessments of the impact of digital infringements and assess whether there are less intrusive methods available.
Another measure mentioned in the Explanatory Memorandum is that the technical aids used must comply with specified norms in the 'Decree on technical aids in criminal procedure'.[44] The device used has to "show a certain degree of predictability and the authenticity and integrity of the data collected through the technical aid has to be guaranteed." The injunction also states the period during which the technical aid is used and indicates which part of the automated work will be examined. The maximum duration of the mandate is four weeks and may, however, be extended with four weeks every time.
A third measure addressing proportionality is that the proposed investigative power can only be used when investigating particular types of crime. The Explanatory Memorandum emphasizes that this power should be used only when there is the suspicion of a crime that constitutes a serious breach of the law. However, these crimes are not limited to cybercrime, but also include crimes such as mild forms of assault, drug-related crimes or squatting. Generally, these offenses are unrelated to cybercrime, which would not justify the use of the investigative power to hack back. Obviously, here the proposed investigative powers are not proportionate, as abuse of an investigative power will lead to a so-called function creep..
Apart from these measures, an important issue remains the risk of abuse of this proposed investigative power. Once hacked into the computer there are also countless activities that can be performed by the police. Examples range from the installation of a keylogger to enable the webcam on a computer, eavesdropping on conversations and searching through directories on a hard drive. This may result in so-called function creep, where an investigative power is used for other purposes than its authorised purpose.[45] For example, it could be used to intercept communication.
Another risk is that, the moment the police start to hack into computers, the line between passive and active interference will become blurred. Until now the police have always had a passive role when it comes to data collection. Internet taps may be an example, where the

[43] R. Prins, 'Cyber security in Nederland op de agenda!' (2012) http://blog.fox-it.com/2012/11/28/cyber-security-in-nederland-op-de-agenda/
[44] Decree on technical aids in criminal procedure [*Besluit technische hulpmiddelen strafvordering*], http://wetten.overheid.nl/BWBR0020444/2013-03-15
[45] S. Halink & T. Siedsma, 'Reactie op consultatie Wetsvoorstel Computercriminaliteit III', *BOF* (2013), p. 4.

service provider is instructed to collect the data and then pass it on to the police.[46] When the police take a more active role, it may be questioned whether this leads to potential entrapment. Furthermore, if the police install software, this may lead to identity and liability issues as the distinction between the actions of the accused and the police could get lost.[47]
In summary, the proposed legislation surely attempts to restrict the scope of the investigative power to hack back. This increases the proportionality of the proposed investigative power to hack back. However, proportionality is still hampered by the fact that the investigative power to hack back is also allowed for several types of crime that are not cybercrime. Furthermore, several risks remain, including potential abuse of the investigative power, entrapment issues and identity and liability issues.

4.3 Subsidiarity

The subsidiarity test focuses on the relationship between the proposed measure and other measures. These other measures can be existing measures or hypothetical measures (i.e., better proposals). In each comparison, the question is which measure (in this case: which investigative power) interferes the least with the interests of the people involved and may therefore be preferable.
When looking at existing investigative powers, the most important comparison is with the internet tap. As an internet tap can only be placed on a single IP address, internet taps are becoming less effective because of the large amount of data and the increasing number of devices on a single connection.[48] In addition, with the use of wireless networks it becomes increasingly difficult to follow a suspect. It is practically impossible to put a tap on all network and service providers used by a suspect. Hence, to better fight cybercrime, the police may need different investigative powers. Of course the question remains whether the investigative power to hack back is effective (see above) but it may be more effective than internet taps. However, it might also be experienced as a more privacy-invasive method.
The proposed legislation can also be compared with the possibilities provided by the Convention on Cybercrime (CoC) for accessing computer systems abroad. Under Article 32 CoC there are two possibilities for cross-border criminal investigations and data access. While Art. 32 (a) CoC provides access to public data, Art. 32 (b) CoC focuses on access to data in another country with the lawful and voluntary consent of the authorized person. Although this could be the citizen who has legal access to the data,[49] the Explanatory Memorandum claims this could also refer to the provider of a service. Although the possibilities provided by the CoC for accessing computer systems abroad may be limited, these do exist, contrary to what is suggested in the proposed legislation. Since the proposed investigative powers cannot be exercised abroad, the CoC seems to provide more possibilities, but these may also interfere more with the interests of others.
The proposed legislation can also be compared with other proposals. An alternative suggested in literature is to allow the police to use the power to hack only to disrupt.[50] The advantage is that this proposal is in any case a lot less invasive and avoids the abovementioned risks of potential entrapment and identity and (some) liability issues. Perhaps the most fundamental

[46] B.P.F. Jacobs, 'Policeware', *NJB*, Issue 39 (2012).
[47] Ibid. See also: O. Kerr, 'Fascinating New Case on Legal Standards for Searching a Remote Computer With Unknown Location' (2013) http://volokh.com/2013/04/26/fascinating-new-case-on-legal-standards-for-searching-a-remote-computer-with-unknown-location/
[48] E.J. Koops & R. Bekkers, 'Interceptability of telecommunications: is US and Dutch law prepared for the future?', 31 *Telecommunications Policy*, (2007) pp. 45-67.
[49] H.W.K. Kaspersen, 'Jurisdiction in the Cybercrime Convention', in: E.J. Koops & S. Brenner, eds., *Cybercrime and Jurisdiction: a Global Survey* (Den Haag: West Nyack, 2006).
[50] B.P.F. Jacobs, 'Policeware', *NJB*, Issue 39 (2012) p. 2764.

aspect is that with this alternative the risks of cross-border hacking by the police are prevented. The chances of retaliation against investigative authorities are in fact considered to be quite large.
A more general question to raise when comparing the proposed legislation with alternatives is that of efficiency. If the proposed investigative powers are much more efficient than their alternatives, this may also be an important (though non-legal) argument in favour of the proposed legislation. Efficiency relates to efforts required to achieve the set goals. Can the police perhaps fight cybercrime with fewer costs, less time, less manpower or otherwise fewer efforts when they have the power to hack back? The Explanatory Memorandum indicates that "it can be expected that investigating computer systems possibly can replace other forms of police deployment and therefore save resources." However, this claim is not further substantiated and it remains to be seen whether this is the case. Given the fact that other investigative powers currently do not seem to be optimally used by the police, it may be doubted whether this will be the case for this new proposed investigative power. Several police agencies have indicated that there is a lack of expertise on how to use technology in policing.[51] When introducing new technologies, it is not likely this issue is suddenly solved.

5. Conclusion

In this paper we assessed the extent to which the investigative power for the police to hack into computer systems of suspected criminals ('hacking back') as proposed by the Dutch government interferes with the right to privacy and other human rights. Using the framework based on the European Convention on Human Rights (ECHR) this proposed legislation was analysed. The ECHR requires an explicit legal basis for interference with the right to privacy and other human rights, which is provided by the proposed legislation. The aim of the proposed investigative powers, i.e., criminal investigation and prosecution, is in line with the grounds mentioned in Art. 8 ECHR. For the assessment of whether the proposed investigative powers are necessary in a democratic society, the effectiveness, the proportionality and the subsidiarity were examined.
The effectiveness test shows that it is doubtful whether the proposed investigative power to hack back is actually effective (i.e., whether it will contribute to the set goals). The intended goal is to strengthen the police in fighting cybercrime. The technological developments that challenge the police in this task (encryption, wireless communication and cloud computing) are unlikely to be solved by the proposed legislation. Furthermore, previous research shows that current investigative powers are not optimally used, which leaves room for better use of existing investigative powers (and thus reducing necessity of the proposed investigative powers) and raises doubts whether the proposed investigative power to hack back will be used better. In short, there is a lack of knowledge on the expected effectiveness of the proposed legislation.
The proportionality test shows that although measures to mitigate risk are taken in the proposed legislation (including additional checks by independent authorities and restrictions to the scope of the proposed investigative powers), considerable risks remain that render the proposed investigative powers disproportionate. Among these risks are the potential abuse of the investigative powers and entrapment issues as well as identity and liability issues.
The subsidiarity test shows that, in comparison to existing investigative powers, internet tapping may be similarly or less privacy invasive but does not yield sufficient results and that the Convention on Cybercrime allows in some situations accessing computer systems abroad

[51] B. Custers & B. Vergouw, 'Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies', 31 *Computer Law & Security Review* (2015) pp. 518-526.

(which the proposed legislation does not allow), but may at the same time be more privacy invasive. The alternative proposal to allow the police to use the hack only to disrupt may avoid some of the problems mentioned above, including provocation and identity issues. Whether the proposed legislation will yield (cost and time) efficiency is uncertain.
Altogether, it can be seen that the proposed legislation meets most of the requirements in the ECHR, but not all. Perhaps the most serious consideration is why it is regarded as necessary to introduce new investigative powers when existing powers are not used adequately, especially when there are serious doubts as to whether these new investigative powers will be effective. In this respect, it is remarkable to see how the Dutch government has been guided by the technological developments mentioned. This causes the investigative power to hack back to be far-reaching and a potential infringement of human rights. In fact, it is likely that the investigative authorities will not find the criminals they are looking for and, while doing so, may instead infringe the rights of innocent citizens.
The proposed legislation is based on a kind of circular reasoning: "The necessity for immediate action makes this inevitable and according to international law."[52] However, there is a danger in giving the criminal investigative authorities the power that they want to fight. Already in 1928 Judge Louis Brandeis stated in the famous case of Olmstead v United States what the risks were of far-reaching investigative methods from the government:

"Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that in the administration of the criminal law the end justifies the means - to declare that the Government may commit crimes in order to secure the conviction or private criminal - would bring terrible retribution."[53]

In other words, the government must set a good example. It means that it is not sufficient that most of the criteria in the ECHR are met. Only if all the criteria mentioned in the ECHR are met, interferences with the right to privacy and other human rights are justified. As the proposed investigative power for the police to hack back does not meet all these criteria, the proposed legislation needs some further adjustment and argumentation.

[52] Explanatory Memorandum, p 36.
[53] A. O'Hehir, 'The empire strikes back: How Brandeis foreshadowed Snowden and Greenwald', *Salon* (2014) www.salon.com/2014/05/24/the_empire_strikes_back_greenwald_snowden_and_the_lessons_of_louis_brandeis/