Investigating cybercrime

Oerlemans, J.J.

1 Updating the legal framework

Investigating cybercrime is challenging. Criminals can take advantage of computers and the Internet to commit cybercrimes relatively anonymously and across State borders. They can also reach many computer users without much extra effort by automating their crimes. In cybercrime investigations, there are typically few leads available that law enforcement officials can follow in order to gather evidence and prosecute. Furthermore, computer users can take measures to conceal their identity and hide evidence. Law enforcement officials must overcome these challenges in order to gather evidence successfully. At the same time, law enforcement officials can also take advantage of computers and the Internet in their evidence-gathering activities. For example, they can interact with other computer users via the Internet under the disguise of a 'nickname' (a pseudonym) or hack into computers to gather data, and thereby obtain information that is relevant in a criminal investigation. In doing so, law enforcement officials can make use of the same anonymity and (global) scale that the Internet provides to criminals.

From a legal point of view, the first question that should be asked is whether the investigative methods that are used in an online context are adequately regulated in the domestic legal framework investigating law enforcement officials operate in. The legal frameworks for investigative methods are often designed to accommodate the application of investigative methods in a physical, territorial world that is confined by State borders. In contrast, evidence in cybercrime investigations is often gathered from computers in a borderless networked environment. The domestic legal framework of the investigating law enforcement officials may or may not indicate with sufficient clarity which regulations are applicable. In addition, when the digital application of investigative methods interferes with fundamental rights in a significantly different manner than the application of equivalent investigative methods in the physical world, it may be necessary to change the law accordingly, to accommodate differences.

The second question that should be addressed is whether the application of digital investigative methods has extraterritorial effects. The principle of the territorial restriction of enforcement jurisdiction governs the application of investigative methods, restricting the power to apply investigative methods to the territorial borders of a State. This principle protects the territorial sovereignty of States and ultimately prevents conflicts between States that may be caused by law enforcement officials who cross State borders without the basis of a (mutual legal assistance) treaty or permission from the affected State. As a corollary of this principle, citizens of States are protected from interferences with their fundamental rights by foreign law enforcement

officials who apply their own laws concerning investigative methods. The Internet however, easily allows law enforcement officials to gather evidence unilaterally, i.e., without permission from the affected State or a treaty basis that authorises the evidence-gathering activity, through the use of digital investigative methods. As such, tension may arise with the principle of the territorial restriction of enforcement jurisdiction. The extent to which the cross-border unilateral application of digital investigative methods is acceptable should be examined.

Aim and approach of the study

This study aims to answer the question of how the Dutch legislator can adequately regulate digital investigative methods in Dutch criminal procedural law. In this context, 'adequately regulating digital investigative methods' means that the regulation of investigative methods (1) provides the necessary instruments for law enforcement officials to gather evidence in cybercrime investigations and (2) provides the individuals involved with a minimum of protection, as required by relevant human rights treaties. In relation to the latter, the focus is on article 8 of the European Convention on Human Rights (hereinafter: ECHR), which protects the right to privacy. The approach taken in this regard is outlined below.

First, the digital investigative methods to be examined in this study are identified by explaining how evidence is obtained in cybercrime investigations. The challenges of anonymity and encryption in cybercrime investigations are also discussed, showing how up-to-date investigative methods should be used to overcome these challenges. The analysis of digital investigative methods and the challenges of anonymity and encryption takes place in chapter 2. The challenge of jurisdiction in these investigations is also introduced in chapter 2, accompanied by an explanation of how digital investigative methods can be applied across State borders and unilaterally in order to overcome this challenge.

Second, the adequacy of the pertinent regulations is tested by analysing the extent to which Dutch criminal procedural law, given the special features of digital investigative methods, requires updates to accommodate the investigative methods. In order to determine the adequacy of the Dutch legal framework in relation to human rights, Dutch regulations are tested with regard to the normative requirements that can be derived from art. 8 ECHR. These normative requirements are determined in chapter 3. In chapter 4, the desirable quality of the law that is derived from art. 8 ECHR is determined for the identified digital investigative methods. Chapters 5 to 8 then examine whether the Dutch legal framework adequately accommodates these investigative methods.

Third, the legitimacy of the cross-border unilateral application of digital investigative methods is analysed by examining issues attached to such practices. More particularly, chapter 9 examines how the cross-border uni-

lateral application of these investigative methods may interfere with State sovereignty and the legal certainty of the individuals involved.[1]

Structure of this chapter
This chapter is structured as follows. Section 1.1 provides a further characterisation of this study. Section 1.2 presents the problem statement and five research questions. In section 1.3, the restrictions of the study are specified. Section 1.4 explains the research methodologies used to answer the research questions. Finally, section 1.5 presents an overview of the structure of the study.

1.1 Characterisation of the study

The emphasis of this study, *Investigating Cybercrime*, is on the relationship between technology and the legitimacy of a criminal justice system. To ensure the legitimacy of such a system, the scope and conditions for the application of digital investigative methods must be clear. All actors involved in the criminal justice system – i.e., law enforcement officials, the individuals involved in a criminal investigation, public prosecutors, lawyers, and judges – must have clarity about both the legal basis for investigative methods and the conditions under which law enforcement officials can apply them. An accessible and foreseeable legal framework for investigative methods helps prevent arbitrary application of power by governmental authorities; it is therefore essential for protecting the rule of law. The legal framework must also comply with overarching legal norms, such as those contained in the ECHR, to provide citizens with at least a minimum level of protection against arbitrary application of governmental power. At the same time, in order to be able to correctly identify normative requirements, understanding of the technology of digital investigative methods is required. Thus, to determine whether a legal framework complies with overarching legal norms such as those contained in art. 8 ECHR, it is necessary to analyse how digital investigative methods are applied and affect fundamental rights. If they affect human rights in a different manner than non-digital 'equivalent' methods, it is examined how such differences should be accommodated in legal frameworks.

1 The term legal certainty is used to refer to the requirements of art. 8 ECHR, against which Dutch law will be tested. However, in the context of the subject matter of chapter 9, the term legal certainty should also be understood more broadly in terms of rule of law requirements. The content of legal certainty as meant in this study, will become evident in chapter 9.

The emphasis chosen has implications for the nature of this study, which may be characterised as a hybrid study involving interfaces between various fields. On the one hand, these fields are legal, with the study examining human rights law, criminal procedural law, and information and communication technology law (ICT law).[2] On the other hand, the study also draws on insights from computer science.

The hybrid characterisation is important for two reasons, both of which have to do with the scope. First, although it is impossible to evaluate the legitimacy of regulations without understanding the technology involved, the examination of that technology in this study can go no further than the basics. Second, given the broadness of the legal subject matter, consisting of several different legal fields, it is likewise not possible to exhaustively analyse all relevant aspects of the various legal fields involved. This study will thus not integrally examine neither the technology nor the law involved, but should be seen as an explorative overview, with the overall aim to understand the misalignments that can occur in the practice of applying digital investigative methods and the theory in the applicable legal frameworks.

Format of the study

In this regard it is important to present the format of this study. As stated earlier, the normative requirements for the regulation of digital investigative methods are derived from art. 8 ECHR. The legal framework that is tested against these normative requirements is Dutch law, which serves as an appropriate object of study for three reasons.

The first reason is that digital investigative methods are already applied in Dutch practice.[3] Unlike criminal substantive law (which is regularly updated to accommodate cybercrimes), very little has been done to rethink the criminal procedural frameworks to accommodate digital investigative

2 This study will also incorporate pertinent international law instruments.

3 See, e.g., 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, 'Onderzoek Holitna: meer dan 500 kinderpornozaken', 30 May 2012. Available at: https://www.om.nl/onderwerpen/kinderporno/@30624/onderzoek-holitna/, Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op Internet', 14 February 2014. Available at: https://www.om.nl/@32626/undercover-onderzoek/, Landelijk Parket, 'Wereldwijde actie politie en justitie tegen hackers'. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@85963/wereldwijde-actie, and Landelijke Parket, 'Anonieme, illegale marktplaatsen op internet aangepakt', 24 November 2015. Available at: https://www.om.nl/@91879/anonieme-illegale/ (last visited on 30 May 2016).

methods in the Netherlands.[4] This means that in practice, when digital investigative methods are currently applied, they are based on regulations that have been designed for offline applications. In the 1990s, the Dutch legislature already posited conceptually that the 'offline laws' are also applicable 'online'.[5] However, a conceptual statement alone does not provide clarity about the scope and the manner in which digital investigative methods are applied. Earlier research indicates that it is unclear for law enforcement officials which legal basis applies to digital investigative methods (cf. Stol, Leukfeldt & Domenie 2013, p. 79).[6] As such, Dutch law provides a useful scenario for determining whether misalignment between human rights law, domestic law, and technology exists.

The second reason is that the Netherlands is a member of the Council of Europe and as such a signatory State to the ECHR. This means that Dutch law must comply with art. 8 ECHR, which is the overarching legal framework that is tested in this study.[7] As a result, this study is also relevant for other Council of Europe members. The analysis of Dutch law in terms of compliance with art. 8 ECHR will thus provide a basis for evaluation of compliance in that sense for other Council of Europe jurisdictions.

The third reason is that the Netherlands has a civil law system with a strong commitment to the principle of legality. This means that legal certainty standards are heightened in the Netherlands, as is common in continental legal systems. In the Netherlands, the pre-trial investigative stage is particularly dominated by the 'criminal procedural legality principle' (see Kooij-

4 The implementation of the Treaty of Lanzarote of 2007 (*Trb*. 2010, 156) and the EU Directive 2013/40/EU on 'attacks against information systems' (L218/8) of 14 August 2013 (*Stb.* 2015, no. 165) last updated Dutch criminal substantive law with regard to cybercrime. Dutch criminal procedural law has not been amended to accommodate digital investigative methods between 2006 and 2015. In 2014, major revisions of Dutch criminal procedural law were proposed and published by the Dutch Ministry of Security and Justice. The ambitious project of 'Modernising Dutch criminal procedural law' aims to make the law 'technologically neutral and future-proof'. Yet, the proposals in the project only seek to amend regulations for computer searches as an investigative method. See Ölçer 2015 for an overview of the concept bill with regard to special investigative powers. In addition, in 2015, a bill for a third Computer Crime Act incorporated a proposal to accommodate hacking as an investigative method in Dutch criminal procedural law. No other digital investigative methods are regulated by these proposals.

5 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/98, 25 880, no. 1, p. 1.

6 Also note that, in a letter to the Dutch parliament in 2009, the Dutch minister of Security and Justice stated: "*There is a great need among law enforcement officials for explanation about the applicable legislation and application of (special) investigative powers on the Internet*" (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2008/09, 28 684, no. 232, p. 2-3).

7 For the regulation of criminal procedural investigative methods, emphasis is often placed on art. 8 ECHR in the Netherlands. See, e.g., *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 9-13, *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2003/04, 29 441, no. 3 (explanatory memorandum General Act on Data Production Orders), p. 4-6 and *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 56-59.

mans & Mevis 2013, p. 3). Art. 1 of the Dutch Code of Criminal Procedure (hereinafter DCCP) articulates this principle as follows: *"criminal procedure is only carried out in the manner provided by law"*.[8] Essentially, in the context of criminal investigations, this principle dictates that the evidence-gathering activities of law enforcement officials must be regulated in the DCCP.[9] The promotion of legal certainty is the central objective of the criminal procedural legality principle (cf. Corstens & Borgers 2014, p. 19).[10] The criminal procedural legality principle brings with it that for intrusive investigative methods, Dutch law requires a legal basis in clear and detailed (statutory) regulations. As such, within other Council of Europe member state jurisdictions, the Netherlands provides a good model for study. The reason is that ECHR standards are 'minimum' standards, which are applicable in 47 different jurisdictions. Differences between the legal systems of member states can bring with them that variation exists in the manner in which ECHR standards are applied domestically. As long as domestic application does not fall short of the minimum standards of the ECHR, the treaty allows for divergence. In terms of the principle of legality in criminal procedural law, divergence may exist in terms of the manner in which criminal procedure is regulated. So, in some Council of Europe member states' legal systems, domestic requirements for legal bases for investigative methods may not be as strict as those in others. With its heightened domestic requirements in terms of the principle of legality, Dutch law will thus require analysis of pertinent ECHR normative requirements in 'full force'.

The 'IRT affair'

It is relevant in this respect to mention earlier experiences in the Netherlands with regards to the regulation of new investigative methods. In the beginning of the 1990s, Dutch police forces cooperated in 'Interregional Detective Teams' (in Dutch, *Interregionale Recherche Teams*, or IRT) to combat serious organised crime. Inspired by U.S. law enforcement officials who used deep-cover operations to investigate (in particular) drug-related crimes, Dutch law enforcement officials made extensive use of paid informants and under-

8 Here, 'law' means statutory laws established by acts of the House of Representatives and reviewed by the Dutch Senate. Thus, in the Netherlands, the legislature decides which criminal procedure regulations apply. The underlying idea is that the creation of criminal procedural law cannot be left to judges, not even implicitly, as a result of ambiguous procedures for investigative methods that leave too much room for interpretation by judges (see Corstens & Borgers 2014, p. 19).

9 Procedures with regard to administrative or technical aspects of investigative methods can be regulated outside criminal procedural law. See also the letter regarding the contours of the project, 'Modernising Criminal Procedural Law', of 30 September 2015, p. 10-11. 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 23 March 2016).

10 For a more extensive analysis regarding the backgrounds of the legality principle in criminal procedural law, see Simmelink 1987 and Groenhuijsen & Knigge 2004, p. 11-16.

cover agents to acquire information about criminal organisations.[11] Selected law enforcement officials and a few public prosecutors authorised the (un) controlled delivery of drugs transports in order to build up credibility and maintain the cover of undercover agents. Therewith, drugs were allowed to reach the market.[12] The use of paid informants and authorised drug transports was poorly reported by the law enforcement officials and in part kept undisclosed during ensuing trials.[13]

Ultimately, the use of new investigative methods became public and led to unrest within the Dutch society. The event was dubbed the 'IRT affair', named after the teams that applied the controversial investigative methods. An inquiry was subsequently conducted by the parliamentary inquiry commission Van Traa, which delivered an extensive report on the use of special investigative methods by Dutch law enforcement officials and made recommendations for new regulations. In part, these recommendations eventually led to the Special Investigative Powers Act, which was adopted in 1999.[14] The act reinforced the rule that investigative methods that interfere with the rights and freedoms of individuals in more than a minor way or threaten the integrity of a criminal investigation must be regulated in detail in the DCCP.[15]

Lesson learned?

The history of the legislative reforms regarding undercover investigative methods should evoke the continued consciousness Dutch legislature. In particular, new investigative methods may again require amendments to legislation. The explanatory memorandum of the Special Investigative Powers Act explicitly notes that the Dutch legislature is charged with the task of amending or creating new legislation when:

---

11 See for an extensive analysis, see Nadelmann 1993, Nadelmann 1995, in: Fijnaut & Marx 1995, Fijnaut and Marx 1995 in: Fijnaut & Marx 1995.

12 See for extensive description about the investigative methods used: *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1995/96, 24 072, no. 10-11 (Van Traa Report), p. 72-164.

13 In addition, the majority of the public prosecutors and the minister of justice were not sufficiently informed about these interregional detective teams' investigative methods. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1995/96, 24 072, no. 11 (Van Traa Report), p. 427-428.

14 *Stb.* 1999, 245, 27 May 1999 (entered into force on the 1 February 2000).

15 This standard was first set in the landmark case of Zwolsman in 1995, in which the Dutch Supreme Court decided that searching the trash bags of citizens was not a privacy-infringing investigative method to the extent that it required detailed regulations in the Dutch Criminal Procedural Code (HR 19 December 1995, ECLI:NL:HR:1995:ZD0328, *NJ* 1996, 249 m nt. Schalken). This standard was later affirmed with regard to other investigative methods by the Dutch legislature in *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum to the Special Investigative Powers Act), p. 110 and 115 and the Dutch Supreme Court (see, e.g., HR 20 January 2009, ECLI:NL:HR:2009:BF5603, *NJ* 2009, 225, m.nt. Borgers, HR 13 November 2012, ECLI:NL:HR:2012:BW9338, *NJ* 2013, 413, m.nt. Borgers and and HR 1 July 2014, ECLI:NL:HR:2014:1562, *NJ* 2015/115, m.nt. P.H.P.H.M.C. van Kempen).

"developments in crime – that often find their origin in technological developments – require the application of new investigative methods that interfere with the right to privacy of involved citizens in more than a minor way".[16]

With the development of digital investigative methods, the task of critically reviewing the adequacy of existing frameworks and, if necessary, adopting new legislation has become one of utmost importance.[17] These digital investigative methods have as of yet not been clearly defined by law. The digital investigative methods are applied in a covert manner, which makes them particularly sensitive in terms of art. 8 ECHR and similar to the investigative methods which were eventually regulated in the Special Investigative Powers Act in 1999. The implications of their technological functions must be examined to understand their relationship with the law.

1.2 Problem statement and research questions

The Dutch legal framework must provide law enforcement officials with the instruments they need to obtain evidence when investigating crimes in today's networked world. At the same time, it must adequately protect citizens' fundamental rights and freedoms. The problem statement (PS) is formulated as follows.

PS: *To what extent does Dutch criminal procedural law adequately regulate the investigative methods used in (cross-border unilateral) cybercrime investigations?*

Five research questions are formulated to answer the problem statement.

The first research question aims to identify the investigative methods that are commonly used in cybercrime investigations. It is formulated as follows.

RQ 1: *Which investigative methods are commonly used in cybercrime investigations?*

16 *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 12 (all texts from parliamentary proceedings are translated by the author).

17 See also the Council of Europe Recommendation Rec(2005)10 to member states on "special investigation techniques" in relation to serious crimes including acts of terrorism, adopted by the Committee of Ministers on 20 April 2005: *"Considering that special investigation techniques are numerous, varied and constantly evolving and their common characteristics are their cover nature and the fact that their application could interfere with fundamental rights and freedoms"* (also adopted by the Draft Recommendation on "special investigation techniques" in relation to serious crimes including acts of terrorism, consolidated by the SIT Drafting group at its second meeting (Rome, 13-14 June 2016)).

In order to identify the relevant investigative methods, an analysis is conducted to ascertain (1) which digital leads law enforcement officials typically follow, (2) which investigative methods law enforcement officials subsequently utilise to gather evidence based on these digital leads, and (3) which investigative methods are used to overcome the challenges of anonymity and encryption in cybercrime investigations.

The second research question aims to determine the requirements that art. 8 ECHR imposes on the domestic legal frameworks of contracting States to regulate investigative methods *generally*. It is important to note that art. 8 ECHR and the accompanying case law of the European Court of Human Rights (hereinafter: ECtHR) with regard to this provision are not specifically developed for application in a digital context. Although in recent case law, the ECtHR has started to develop its thinking about the relationship between the treaty and the digital world, case law in this regard is sparse. Chapter 3 discusses requirements as they apply generally. The manner in which this general framework should apply to the digital context is discussed in the ensuing chapters (particularly chapter 4). The second research question is formulated as follows.

RQ 2: *Which normative requirements can be derived from art. 8 ECHR for the regulation of investigative methods?*

The third research question aims to determine what requirements exist for the regulation of the identified digital investigative methods. Depending on the gravity of the privacy interference, the ECtHR may require detailed regulations and specific procedural safeguards. Contracting States to the ECHR, including the Netherlands, must implement these requirements in their domestic legal frameworks. The requirements for digital investigative methods are determined by positioning the identified digital investigative methods in the existing general framework in art. 8 ECHR. This will be done by analysing the gravity of the privacy interferences involved in the application of the digital investigative methods (in light of their technological functions) and on that basis, determining what type of regulations is desired. The third research question is formulated as follows.

RQ 3: *Which quality of law is desirable for the identified digital investigative methods?*

The fourth research question aims to determine how the Dutch criminal procedural law that regulates the identified digital investigative methods can be improved by taking the identified normative requirements of art. 8 ECHR into consideration. The Dutch legal framework is considered adequate when the normative requirements from art. 8 ECHR are met. The fourth research question is formulated as follows.

RQ 4: *How can the legal framework in Dutch criminal procedural law be improved to adequately regulate the identified investigative methods?*

The issue here is whether the basis that is currently used in practice for applying digital investigative methods is adequate, given the technical and legal implications of these methods. The research field for RQ 4, i.e., the application of digital investigative methods, is rather wide. To answer the research question, the following four investigative methods are examined (each in a separate chapter). [In passing, it is noted that here the answer to RQ 1 is anticipated upon.]

(RQ 4a) Gathering publicly available online information (chapter 5)
(RQ 4b) Issuing data production orders to online service providers (chapter 6)
(RQ 4c) Applying online undercover investigative methods (chapter 7)
(RQ 4d) Performing hacking as an investigative method (chapter 8)

The fifth research question is related to the international dimension of cybercrime investigations, which becomes apparent in two situations. First, when the suspect involved in a criminal investigation resides on foreign territory. Second, when evidence (often stored on computers) is located on foreign territory. In these situations, the law enforcement officials who investigate cybercrime commonly have to gather evidence on foreign territory.

Mutual legal assistance is the formal method for obtaining evidence that is located abroad. However, the Internet allows law enforcement officials to utilise certain investigative methods across borders, without the need to physically enter another State. Nonetheless, this unilateral application of investigative methods produces extraterritorial effects on foreign territory and may be questioned on the basis of the territorial limitation of enforcement power, as an established principle in international law. The fifth research question is formulated as follows.

RQ 5: *To what extent is it desirable and legitimate that the identified investigative methods are applied unilaterally across State borders?*

The fifth research question is answered by taking into account (1) the possible infringement of the effected State's territorial sovereignty and (2) the legal certainty of the individuals involved. States have different perspectives on the extent to which investigative methods can be applied across State borders. To illustrate these different perspectives and the implications thereof, a legal comparison between the Netherlands and the United States is conducted.[18]

18 See subsection 1.4.2 for the research methodology of the conducted comparative legal research.

1.3 Restrictions of the research

This research is restricted by focusing on evidence-gathering activities that are conducted by law enforcement officials in cybercrime investigations. The evidence-gathering activities are examined in their relation with the right to privacy as articulated in art. 8 ECHR. The focus gives rise to three restrictions, which are further discussed below.

1.3.1 Restriction to cybercrime investigations

This study focuses on digital investigative methods that are used in criminal investigations that involve cybercrime. Cybercrime is defined as *"criminal acts committed using electronic communication networks and information systems or against such networks and systems"*.[19] Cybercrime is often distinguished as:

(1) target cybercrimes: crimes in which the computer is the target of the offense.
(2) tool cybercrimes: crimes in which the computer is used to facilitate a traditional crime.
(3) crimes in which the use of the computer is an incidental aspect of the commission of the crime, but significant to law enforcement because computers contain traces of evidence of a crime.[20]

Criminal investigations with regard to crimes in which digital evidence only plays a significant role are not considered as cybercrime investigations in this study. Digital evidence is nowadays involved in almost all criminal investigations (cf. Brenner 2010, p. 37). Cybercrime investigations that involve target cybercrimes and tool cybercrimes are more interesting for this research, since investigating these crimes often requires law enforcement officials to follow specific digital leads across State borders, which creates an interesting dynamic to the investigation of these crimes. In addition, the challenges that are often present in these cybercrime investigations require law enforcement officials to use novel digital investigative methods that are of interest to this study.[21]

19 See Communication of 22 May 2007 from the European Commission, 'Towards a General Policy on the Fight against Cybercrime', COM(2007)267 final, p. 2.

20 See Charney 1994, p. 489. Cf. Brenner 2010, p. 39-47. The categorisation closely resembles the categorisation originally made by Parker back in 1976 (Parker 1976, p. 17-22).

21 The search of a place and subsequent seizure of computers and (internet) wiretapping are also investigative methods that are commonly used in cybercrime investigations. However, these investigative methods have a solid basis in Dutch criminal procedural law and are not considered as novel digital investigative methods that require specific analysis.

1.3.2 Restriction to evidence-gathering activities by law enforcement officials

The focus is on the evidence-gathering activities in criminal investigations with regard to cybercrime that are carried out by law enforcement officials. Many of the investigative methods that law enforcement officials use to gather evidence are regulated in the DCCP. The regulation of investigative methods in other legal frameworks are not examined.

The restriction to evidence-gathering activities by law enforcement officials also means that investigative activities in the context of cyberterrorism, cyberespionage, and cyberwar are not examined. Other governmental authorities than law enforcement authorities investigative cyberespionage, as well as 'cyberattacks' that rise to the level of terrorism or war. Those activities are regulated by different legal frameworks. This study only focuses on criminal procedural law. More particularly, only the regulations of investigative methods that can be used by law enforcement officials in 'regular criminal investigations', which start when a reasonable suspicion of a crime exists, are analysed. These investigative methods may be regulated as 'investigative powers' or 'special investigative powers' in Titles IV and IVA of the DCCP. The investigative powers and special investigative powers that can be used in criminal investigations when (1) a reasonable suspicion is present that crimes are being planned or committed in an organised crime context (Title V) and (2) indications are available that terrorist crimes are being planned (Title VB), are not examined in this study. Special investigative powers that can be applied with the aid of civilians (regulated in Title VA and VC) are also excluded from this study. Finally, the regulations for the use of datamining techniques to analyse data in 'explorative investigations' (in Dutch: verkennend onderzoek) in art. 126gg DCCP is not examined.[22]

Governments can also take other measures to deal with the challenges that are arise in cybercrime investigations, such as a decryption order to deal

22 See with regard to use of datamining techniques by law enforcement authorities, e.g., Sietsma 2006 and Brinkhoff 2016. Digital investigations can certainly be a part of investigations under Title V and VB, and differences in the distinct bases for application may be pertinent to the assessment of the adequacy of the specific regulations in different titles. However, given the nature of this study as a non-exhaustive exploration of the relationship between digital investigative methods and the law, the focus will be on the 'standard' application of the methods on the basis of a 'classical' reasonable suspicion of guilt in the sense of art. 27 DCCP. It may be added here that as part of the current modernisation project of the DCCP, the Dutch Ministry of Security and Justice has proposed amendments to redesign the structure of special investigative powers in Dutch criminal procedural law so that the special investigative powers are not regulated three times, but once in the DCCP. The three distinct bases for application will remain however and be regulated in the general provisions of the DCCP. See the discussion document regarding the general provisions for pre-trial investigations (6 June 2014), p. 27-29. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (last visited 15 November 2015).

with the challenges of encryption.[23] The focus on evidence-gathering activities also brings with that these measures are not examined.

This author is aware that, in practice, policing is not performed by law enforcement officials alone.[24] For instance, private IT security firms, security departments from companies, and online service providers also fight cybercrime. Tensions may arise regarding an individual's right to privacy when these individuals are under investigation by a private organisation. However, criminal procedural law consists of a legal framework that only regulates investigative methods that are used by law enforcement officials.[25] Questions concerning the use of investigative methods by private parties in an online context thus fall outside the scope of this study's problem statement.

1.3.3 Restriction to art. 8 ECHR

This study investigates requirements based on art. 8 ECHR for regulating digital investigative methods in the domestic legal frameworks of States. However, when regulating investigative methods within a domestic legal framework, other fundamental rights – such as the right to a fair trial as specified in art. 6 ECHR – are also important (cf. Ölçer 2008, p. 527-530 and Hirsch Ballin 2012, p. 42-62). Accompanying requirements to ensure a legitimate criminal justice system based on art. 6 ECHR are thus not examined. These requirements include respecting rights such as the privilege against self-incrimination, the prohibition of entrapment, and notifying individuals involved in criminal investigations of the use of investigative methods. The mechanisms that ensure the disclosure of information in the course of crimi-

23 Current (October 2016) debates about measures (1) that require companies to hand over a 'golden key' or 'backdoor' to law enforcement authorities to enable law enforcement officials to acquire decrypted data and (2) enable law enforcement authorities to issue a decryption order to suspects in order to force them to hand over an encryption key to law enforcement authorities under the threat of a prison sentence are not dealt with in this study, since these measures do not concern investigative methods. See, e.g., Bruce Schneier, 'iPhone Encryption and the Return of the Crypto Wars', *Schneier on Security* (blog), 6 October 2014. Available at: https://www.schneier.com/blog/archives/2014/10/iphone_encrypti_1.html and Matt Burgess, 'Tim Cook: Apple won't weaken encryption to meet FBI demands', *Wired,* 12 February 2016. Available at: http://www.wired.co.uk/news/archive/2016-02/17/tim-cook-apple-encryption-iphone-san-bernardino and Kieren McGarthy, 'French, German ministers demand new encryption backdoor law', *The Register*, 24 August 2016. Available at: http://www.theregister.co.uk/2016/08/24/french_german_ministers_call_for_new_encryption_backdoor_law/ (last visited on 10 October 2016).

24 For analysis of the trend in public-private policing, see Garland 2001 and Ericson & Haggerty 1997.

25 See also Fijnaut in: Groenhuijsen & Knigge 2002, p. 689-749, Nuis et al. 2004, and the discussion document regarding the general provisions for pre-trial investigations (6 June 2014), p. 37-38. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (last visited on 11 February 2016).

nal prosecution and the mechanisms that ensure transparency in the use of investigative methods by law enforcement officials in criminal investigations, are also not examined.

It is arguable that regulations for investigative methods are only effective when law enforcement officials respect them. In criminal procedural law, remedies can be provided to suspects for procedural defects that are caused by law enforcement officials. Remedies aim to show law enforcement authorities that investigations do not benefit from disregarding the regulations for investigative methods and that authorities must take procedural regulations seriously. This interest is balanced against the public interest not to leave criminal behaviours unpunished (cf. Keulen & Knigge 2010, p. 523-524).[26] In the Netherlands, trial judges can apply a remedy for procedural defaults with regard to the application of investigative methods.[27] The question whether these Dutch regulations for remedies find the right balance is not considered in this study, since it is related not only to art. 8 ECHR but rather to art. 6 ECHR.

The *regulation* of the investigative methods themselves is placed at the forefront of this study. It means that, although all aspects of art. 8 ECHR will be examined, the core of that provision as it pertains to the requirements of regulations is the primary focus in this study.

1.4 Research methodology

Four methodologies are used to answer the research questions: (1) desk research, (2) comparative legal research, (3) fieldwork, and (4) analysis. These methodologies are briefly discussed below.

1.4.1 Desk research

As applied in this study, desk research consists of scrutinising available scientific literature concerning the following five topics: (a) cybercrime, (b) the application of investigative methods in cybercrime investigations, (c) the relationship between the right to privacy and investigative methods, (d) the regulation of investigative methods in Dutch criminal procedural law, and

26 See for further reading, e.g., Embregts 2003, Van Woensel 2004, Keulen & Knigge 2010 and Borgers 2012.

27 In the Netherlands, the following remedies can be applied: (1) the determination a procedural defect has occurred (without imposing further sanctions), (2) the reduction of the imposed sentence, (3) the exclusion of evidence, and (4) the barring further prosecution of the suspect. The first remedy is created in case law (see, most notably, HR 30 March 2004, ECLI:NL:HR:2004:AM2533, par 3.6.1). The last three remedies are codified in art. 359a(1) DCCP. To decide which sanction is most appropriate, a trial judge must take into account the (1) interests served by the rule that is not observed, (2) the damage resulting from the noncompliance, and (3) the seriousness of the noncompliance for the suspect (art. 359a(2) DCCP).

(e) the territorial limits of enforcement jurisdiction. Desk research is thus applied in order to answer all five research questions.

In addition, desk research is applied to analyse Dutch regulations, legislative history, and jurisprudence regarding the identified digital investigative methods. Finally, news articles are examined and cited where they may shed light on the application of investigative methods in cybercrime investigations.

1.4.2 Comparative legal research

Comparative legal research is conducted in relation to the legal systems of the Netherlands and the United States.[28] This research method is used in order to examine the two countries' approaches to both the regulation of digital investigative methods and the principle of the territorial limitation of enforcement jurisdiction. Comparative legal research is primarily used for answering the fifth research question. Choosing the United States for study is part of the research methodology. The United States is chosen for this legal comparison for three reasons.

(1) The U.S. federal law enforcement agencies are frontrunners in the investigation and prosecution of cybercrime. The U.S. Federal Bureau of Investigation (FBI), the U.S. Secret Service, the U.S. Drug Enforcement Agency (DEA), and the U.S. Immigration and Customs Enforcement (ICE) have been particularly active in pursuing more 'high-tech' criminals, even when those suspects live outside the territorial borders of the United States.[29] The experience of U.S. law enforcement agencies can thus provide interesting insights, both in terms of practice and legal regulation.

(2) Knowledge about U.S. federal regulations may be important for Dutch law enforcement agencies and citizens, as many Dutch citizens make use of U.S. online services, such as Facebook, Gmail, Twitter, and LinkedIn. Therefore, Dutch law enforcement officials may be required to gather data on U.S. territory. Knowledge about U.S. law may assist them in gathering evidence on U.S. territory.

---

28 I was a visiting scholar of George Washington University from 5 September to 25 November 2011. This visit enabled me to study materials available in the United States and to speak with experts on digital investigations from the law enforcement and academic community.

29 The FBI is the largest federal organisation in the U.S. that handles computer crimes. Other federal agencies focus on specific crimes. The U.S. Secret Service particularly deals with financial fraud, such as the illegal online trade of credit card data. The DEA focuses on the illegal drug trade, and ICE conducts criminal investigations with regard to child abuse offences.

(3) The United States has a different approach toward the territorial limitation of enforcement jurisdiction than States in continental Europe, including the Netherlands. Past criminal investigations on money-laundering offences and drug-related offences have shown that U.S. law enforcement authorities are willing to intrude on the territory of sovereign States and override local legal norms in the pursuit of suspected criminals abroad (cf. Nadelmann 1993, p. 472-473). The different approaches of the Netherlands and the United States, as they pertain to the territorial limitation of enforcement jurisdiction, deserve further examination within the context of the cross-border unilateral application of digital investigative methods.

The Netherlands and the United States have rather different legal systems. The Netherlands has a civil law system; the United States has a common law system. Most notably, U.S. criminal procedural law is not bound by a criminal procedural legality principle as it is in the Netherlands. Instead, as in other common law States, the decisions of the Supreme Court of the United States are particularly important to U.S. criminal procedural law (cf. LaFave et al. 2009b, p. 3). There is thus not necessarily a broad set of statutory laws available to regulate investigative methods in the United States. In contrast, intrusive investigative methods in the Netherlands are regulated in detail within criminal procedural statutory law.

Due to the global nature of cybercrime and the similar challenges faced by law enforcements authorities in both States, a functionalist approach is appropriate for this legal comparison (cf. Gordely in: Monateri 2012). The starting point of the legal comparison is thus the equivalent function of the regulations and concepts. This approach is used with the aim of determining how the selected investigative methods are regulated in both the Netherlands and the United States and to examine each State's approach to the principle of the territorial limitation of enforcement jurisdiction.

1.4.3 Fieldwork

Fieldwork is necessary for gaining a better understanding of both cybercrime and the investigative methods utilised in cybercrime investigations. The fieldwork conducted for this study aims to fill knowledge gaps about the application and regulation of investigative methods in cybercrime investigations as well as to validate the findings of the desk research. The results of the fieldwork are therefore used to inform the findings for all five research questions. The fieldwork consists of (1) semi-structured interviews and (2) an analysis of police reports in criminal trial dossiers (i.e., dossier research).

Semi-structured interviews were conducted with 14 individuals with expertise in digital investigations. A combination of experts in a variety of fields were chosen. They have (a) expertise on technical aspects of digital investigative methods, (b) law enforcement experience in cybercrime investigations, or (c) knowledge of the theoretical background of the legal basis

for investigative methods. Thus, respondents in the relevant fields – technical, legal, and law enforcement – were chosen. Appendix A provides an overview of the individuals who were interviewed.

The dossier research consists of reviewing 10 case files at the High-Tech Crime and Telecommunications Department of the Dutch Public Prosecution Service. These case files were selected because they contain police reports that describe the application of digital investigative methods. The reports are analysed to determine which legal provisions law enforcement officials base the use of digital investigative methods on. In addition, the dossier research aims to establish what obstacles often arise in cybercrime investigations and how law enforcement officials handle these challenges by applying certain investigative methods. Prior permission to analyse the dossiers was obtained from the Research and Documentation Centre of the Dutch Ministry of Security and Justice. No permission was given to this researcher to copy any materials from the examined dossiers. Moreover, prior authorisation from the coordinating public prosecutor has been required for any references made to the examined case files.

1.4.4 Analysis

The results of different research methodologies are triangulated in order to answer the research questions. Triangulation means that the findings of the (1) desk research, (2) comparative legal research, and (3) fieldwork are compared to validate their results. This approach is suitable for the hybrid approach applied, which aims to provide an overview of legal frameworks and identify the misalignments that can occur in the practice of applying digital investigative methods within these frameworks. The results of the analysis provide important input for improving the relevant legal frameworks.

1.5 Structure of the thesis

An overview of the structure of this thesis follows.

Chapter 1 has introduced the subject of the thesis and formulated both the problem statement and research questions. The restrictions imposed on the scope of the research scope were also discussed, as were the research methodologies. Finally, this chapter presents the structure of the thesis.

Chapter 2 answers RQ 1 by explaining how evidence is gathered in cybercrime investigations. It examines how computers and the Internet facilitate crime and subsequently influence criminal investigations with regard to cybercrimes. In addition, the challenges of cybercrime investigations and their influences on the use of investigative methods are examined. The chapter also identifies the investigative methods that are commonly used in cybercrime investigations.

Chapter 3 answers RQ 2 by examining the normative requirements that can be derived from art. 8 ECHR for the regulation of investigative methods.

Chapter 4 answers RQ 3 by determining the gravity of the privacy interference that is caused by applying the identified digital investigative methods. Depending on the gravity of the privacy interference, a framework is proposed for requirements for the regulation of digital investigative methods.

Chapter 5 answers RQ 4a by investigating whether the gathering of publicly available online information is adequately regulated within Dutch criminal procedural law.

Chapter 6 answers RQ 4b by examining whether the issuing of data production orders to online service providers is adequately regulated by Dutch criminal procedural law.

Chapter 7 answers RQ 4c by testing whether the domestic legal framework for applying online undercover investigative methods is adequately regulated by Dutch criminal procedural law.

Chapter 8 answers RQ 4d by investigating whether the applicable regulations for performing hacking as an investigative method is adequately regulated by Dutch criminal procedural law.

Chapter 9 examines the international dimension of the application of digital investigative methods in cybercrime investigations. The extent to which evidence-gathering activities can be applied unilaterally across State borders is examined for each of the selected investigative methods. The analysis thus provides an answer to RQ 5.

Chapter 10 evaluates the previous chapters. Both the domestic and international legal frameworks are assessed to determine the steps that can be taken forward to legitimately and successfully investigate cybercrime.

Chapter 11 answers the problem statement. It presents the findings of this study and provides recommendations for improving the regulation of the investigative methods that are utilised in cybercrime investigations.