Investigating cybercrime

Oerlemans, J.J.

10 The way forward

In chapter 2, this study identified the digital investigative methods that law enforcement authorities commonly use to gather evidence in cybercrime investigations. The normative requirements for regulating investigative methods based on art. 8 ECHR were then identified in chapter 3. Thereafter, the desirable quality of regulations for these investigative methods based on the right to privacy was determined in chapter 4. In chapters 5 to 8, the identified investigative methods were placed within the Dutch legal framework to examine whether Dutch criminal procedural law regulates them in (1) an accessible manner, (2) a foreseeable manner, and (3) a manner that meets the desired quality of the law. Finally, the cross-border unilateral application of the identified digital investigative methods and consequences thereof for the territorial sovereignty of States and legal certainty of involved individuals were examined in chapter 9.

This chapter evaluates the outcomes of the analyses conducted in previous chapters in order to provide overarching observations concerning the study's results. These observations may aid in deciding which judicial steps should be taken to amend the legal framework that regulates the investigative methods used in cybercrime investigations in the Netherlands.

This chapter is structured as follows. Section 10.1 evaluates the challenges in investigating cybercrime. Section 10.2 then examines the Dutch legal framework with regard to the identified digital investigative methods on a domestic level, while section 10.3 evaluates the (inter)national legal framework with regard to the cross-border unilateral application of the identified digital investigative methods. Finally, a summary of the chapter's findings is presented in section 10.4.

10.1 Challenges in investigating cybercrime

As explained in chapter 2, three factors make it very challenging for law enforcement authorities to successfully gather enough evidence and prosecute the perpetrator of a cybercrime, namely (1) anonymity, (2) encryption, and (3) jurisdiction.

The challenge of anonymity requires law enforcement authorities to make significant efforts to identify a computer user and gather evidence that proves that he has committed a cybercrime. As explained in chapter 2, a combination of investigative methods may provide for the means to do so. Nonetheless, the success of a criminal investigation will depend on the circumstances of the case, the measures that an individual has taken to obscure his digital traces, and the expertise that is available to law enforce-

ment authorities and the resources they are willing to devote to identifying a suspect. The analysis of case law in chapters 5 to 8 showed that individuals can only be traced based on their IP address when they do not consistently use anonymising services and techniques to hide that address. In my view, it is very possible to commit a well-planned cybercrime without leaving any usable digital leads. Hacking as an investigative method is an intrusive instrument for overcoming the challenge of anonymity, but it may provide a solution under certain circumstances.[1] Moreover, law enforcement officials can also use online undercover investigative methods to identify cybercriminals based on their online handles. It appears that Dutch law enforcement officials are more reluctant to use these investigative methods compared to their U.S. counterparts. This may be explained by the fact that undercover investigative methods are considered as privacy intrusive in the Netherlands, whereas they are not considered as privacy intrusive investigative methods in the United States. This is also reflected by the stringent regulations for undercover investigative methods in the Netherlands.

In specific circumstances, encryption can make evidence-gathering activities significantly harder for law enforcement authorities in their criminal investigations. Individuals who consistently use the right encryption techniques can pose a significant challenge to law enforcement authorities. In practice, individuals often make mistakes in their 'operational security measures' that law enforcement officials can take advantage of. In addition, a well-prepared strategy may allow law enforcement authorities to seize a computer while a suspect is still using it. Hacking as an investigative method may also provide law enforcement officials with the ability to circumvent the challenges of encryption. The use of policeware may enable then to intercept communications before they are encrypted, secure evidence, and record login names and passwords that they can later utilise to access information.

Jurisdiction is the greatest challenge in cybercrime investigations. The fact that a suspect resides in the territory of a State that the investigating State does not have an extradition treaty with may prove to be an insurmountable obstacle for successfully prosecuting a cybercrime. A lack of priority in relation to executing legal assistance requests or a lack of competent law enforcement officials to gather digital evidence may also hamper evidence-gathering activities in cybercrime investigations. The ability to gather evidence by applying certain investigative methods unilaterally across State borders (see chapter 9) may provide law enforcement authorities the means to gather evidence on foreign territory. However, it will not necessarily enable them to successfully prosecute a foreign individual. Furthermore, as explained in chapter 9, many forms of cross-border digital evidence gathering activities still require permission of the affected State or a legal basis in a treaty in order to take place on a legitimate basis.

1 Policeware to relay back identifying information concerning the computer and network that used by the suspect is particularly interesting. See subsection 2.4.3.

Taken together, the challenges of anonymity, encryption, and jurisdiction can make cybercrime investigations and the successful prosecution of cybercriminals very challenging. As a consequence, law enforcement officials have propagated a strategy to 'disrupt' cybercrime.[2] For example, Europol's Cybercrime Centre has been actively disrupting cybercrime by dismantling botnets that criminals have used to commit cybercrime in recent years.[3] These operations are part of a strategy in which law enforcement authorities 'move from prosecution to the disruption of cybercrime'.[4] However, during these operations law enforcement authorities utilise far-reaching special investigative powers that are created for *gathering evidence* in criminal investigations in order to prosecute individuals for cybercrime. It is questionable that this goal is reached in these disruption operations. For instance, the above-mentioned dismantling of botnets often does not result in the successful prosecution of cybercriminals.

It is important to keep in mind that the powers created for law enforcement authorities in criminal procedural law are not meant to maintain public order by frustrating criminals in their operations (cf. Corstens & Borgers 2014, p. 26). Instead, these powers are intended to enable law enforcement officials to gather evidence in criminal investigations and determine whether a person is guilty or innocent of a crime, after which he is punished as deemed appropriate. When a society believes that new powers to disrupt or halt crime online should be granted to law enforcement authorities, a debate should take place and these powers should be restricted appropriately by law.

In the meantime, efforts must still be made to successfully prosecute cybercriminals. Criminal law has an important role to play in (1) providing just outcomes for perpetrators and victims of cybercrime; (2) achieving deterrence, rehabilitation, and societal reintegration aims in relation to con-

2 See Huisman et al. 2016, p. 67-68. See also, e.g., Jacobs (2012, p. 2764) and Prins (2012, p. 52), who described the practice as an effective strategy to combat cybercrime.

3 See the following Europol press releases about disrupting botnets (without mentions of arresting suspects), 'Notorious botnets infecting 2 million computers disrupted', 5 December 2013. Available at: https://www.europol.europa.eu/content/notorious-botnet-infecting-2-million-computers-disrupted, 'Global action targeting Skylock malware', 10 July 2014. Available at: https://www.europol.europa.eu/content/global-action-targeting-shylock-malware, and 'Botnet taken down through international law enforcement cooperation', 25 February 2015. Available at: https://www.europol.europa.eu/content/botnet-taken-down-through-international-law-enforcement-cooperation (last visited on 18 May 2015).

4 John Leyden, 'Cuffing darknet-dwelling cyberscum is tricky. We'll "disrupt" crimes instead, warns top cop', *The Register*, 29 April 2014. Available at: http://www.channelregister.co.uk/2014/04/29/europol_boss_calls_for_push_to_disrupt_cybercrime/ (last visited on 18 May 2015). See also Europol 2015b, p. 12: *"While targeting high profile, high value targets such as malware developers may be beneficial, the disruptive effect of targeting either shared criminal infrastructure or the less ubiquitous actors who provide key support services, such as bulletproof hosting, may have more significant impact across a greater division of the cybercrime community and represent a more pragmatic approach for law enforcement."*

victed offenders; and (3) creating deterrence for potential perpetrators (cf. UNODC 2013, p. 170).

10.2 Updating the domestic legal framework

The analyses in chapters 5 to 8 have shown that the Dutch legislature has failed to create legislation that meets all three normative requirements of (1) accessibility, (2) foreseeability, and (3) an adequate quality of the law regarding the regulation of the identified digital investigative methods that are commonly used in cybercrime investigations.

This is a striking observation, seeing as the Dutch legislature is tasked with amending the legal framework when technological developments significantly influence the investigative methods that are used in criminal investigations.[5] Dutch law enforcement authorities have already been applying the identified investigative methods for years. However, the regulations for these investigative methods are either (1) non-existent or (2) ambiguous in their scope and the manner in which they are executed by law enforcement authorities.[6] That is a worrisome conclusion, given that the right to privacy – and ultimately the rule of law – aim to protect individuals from the arbitrary application of power by governmental authorities. The analysis has also shown that the quality of the law should be improved, though not necessarily (only) in criminal procedural law, with regard to all of the identified investigative methods in order to adequately regulate digital investigative methods.

The task ahead

The Dutch legislature has not amended the DCCP to better accommodate digital investigative methods since 2006.[7] Initiatives have recently been taken to update the legal framework, but both the Computer Crime Act III and the project 'Modernising Criminal Procedural Law' fail to take all regulations that are required for digital investigative methods into consideration.

The Computer Crime Act III correctly identifies the challenges that law enforcement authorities encounter in criminal investigations.[8] However, the belief that a new investigative power that would enable law enforcement authorities to hack computers – even abroad – is *the solution* for effectively combatting cybercrime by prosecuting individuals is naive. The Dutch legislature is currently overemphasising a single investigative method for gath-

5 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1996/97, 25 403, no. 3 (explanatory memorandum Special Investigative Powers Act), p. 12.

6 See also section 8.5.

7 Cf. *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8.

8 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8-16.

ering evidence more effectively in cybercrime investigations; other relevant investigative methods also merit its attention. This study has shown that hacking is not the only investigative method that law enforcement authorities use to overcome the challenges of anonymity, encryption, and jurisdiction to gather evidence in cybercrime investigations. The gathering of publicly available online information, the issuing of data production orders to online service providers, and the application of online undercover investigative methods are also important investigative methods that overcome these challenges and help law enforcement officials to gather digital evidence in cybercrime investigations.

The Dutch Ministry of Security and Justice plans to modernise Dutch criminal procedural law and make the DCCP 'technology independent' and 'future proof'.[9] In 2014, it even created a special YouTube video to inform Dutch citizens about how technology has changed society, using illustrations related to computers, cloud computing, and social media services.[10] However, after meticulously reviewing the modernisation plans, the only digital investigative method the legislator definitively seeks to update is computer searches.[11]

A *full review* of Dutch criminal procedural law is instead required to accordingly accommodate all investigative methods that relate to the digital evidence-gathering activities of law enforcement authorities. We cannot deny the digitalisation of investigative activities. The Dutch legislature should provide both the necessary instruments for law enforcement authorities to effectively execute their tasks *and* provide the citizens involved with adequate procedural safeguards to protect their rights and freedoms. This means that a broader review should be conducted than has been performed in this study. It is emphasised here that this study has only examined the accessibility, foreseeability, and desired procedural safeguards for the regulation of digital investigative methods in Dutch criminal procedural law. The requirements for regulating investigative methods were derived from art. 8 ECHR. A full review should also take the normative requirements that can be derived from other ECHR rights into consideration.[12] In addition, it is likely that organisational measures must be taken to enable Dutch law

9 See Rijksoverheid.nl, 'Contourennota Wetboek van Strafvordering in consultatie', 3 February 2015. Available at: https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/nieuws/2015/02/03/contourennota-wetboek-van-strafvordering-in-consultatie (last visited on 30 December 2015).

10 Available at: https://www.rijksoverheid.nl/onderwerpen/modernisering-wetboek-van-strafvordering/inhoud/eenvoudigere-procedures-strafvordering (last visited on 30 December 2015).

11 See subsection 8.4.1. See also J.J. Oerlemans, 'Modernisering Strafvordering geldt niet voor de opsporing', *Computerrecht* 2016, no. 1, p. 1.

12 It should be noted that Ölçer (2008, p. 26) and Hirsch Ballin (2012, p. 42-62) both emphasise in their dissertations how heavily the ECtHR weighs the right to a fair trial as provided in art. 6 ECtHR when deciding on the legitimacy to use an investigative method in light of the ECHR. See also Groenhuijsen & Knigge 2002, p. 323-326 for a list of reasons why investigative methods may require detailed regulations in criminal procedural law.

enforcement authorities to utilise all possibilities for gathering digital evidence in criminal investigations in practical terms (cf. Huisman et al. 2016, p. 58).

Transparency and foreseeability

It is reiterated here that the events in the 1990s that led to the IRT affair were partially caused by the secretive use of undercover investigative methods in criminal investigations. In 1997, the special Van Traa inquiry commission eventually concluded that many of the undercover investigative methods that were being used in practice needed to be more strictly regulated and that more transparency was required in relation to the application of undercover investigative methods by the IRT teams.

Parallels can be drawn between the IRT affair from the 1990s and the current practice of digital evidence-gathering activities.[13] This study has shown that the legal basis for conducting digital investigative methods in Dutch criminal procedural law is currently often unclear. An adequate legal basis is often lacking for the identified digital investigative methods when taking into account their intrusiveness based on the right to privacy in art. 8 ECHR. However, I agree with Schermer that the regulation of digital investigative methods is not presently under a normative crisis, since the required legal framework basis is in part already there. After the IRT affair, the basis of the legal framework was created by the Act on Special Investigative Powers. Nevertheless, for the automated gathering of publicly available online information and hacking as an investigative method, new regulations should be created by the Dutch legislature. To adequately regulate the other types of gathering publicly available online information, more clarity should be provided about their scope and manner they are applied in guidelines that are created by the Public Prosecution Service. Furthermore, to adequately regulate the issuing data production orders to online service providers and online undercover operations, substantial amendments to the DCCP are required. Given the today's fast-paced technological environment in which digital investigative methods are applied in, the Dutch legislature must continually monitor whether Dutch criminal procedural law provides for a foreseeable legal framework that is also of sufficient quality in terms of protection for the individuals involved.

To monitor the application of (digital) investigative methods by Dutch law enforcement authorities, I concur with Buruma's recent suggestion to create a 'Supervisory Commission for the Dutch Police' (Buruma 2016, p. 1541). This supervisory commission could be mandated to control and evaluate the evidence-gathering activities of Dutch law enforcement authorities and to share its findings with both the Dutch Parliament and the public

13 See also B.W. Schermer, 'Digitale IRT-affaire of nieuwe opsporing?', 14 March 2012. Available at: http://webwereld.nl/security/59972-digitale-irt-affaire-of-nieuwe-opsporing-opinie (last visited on 4 May 2016).

(through published reports).[14] It could also identify needs for new regulations for investigative methods from both law enforcement and fundamental rights perspectives.

10.3 International legal framework

In chapter 2, this study showed that mutual legal assistance as a mechanism for obtaining evidence on foreign territory does not provide an adequate response to the global problem of cybercrime. I am not alone in this observation. For instance, Koops and Goodwin (2014, p. 41) state that: *"There seems to be considerable agreement, both with practitioners and with academic cyber-investigation experts, that classic mutual legal assistance is inadequate"*. An extensive report of the United Nations Office on Drugs and Crime (UNODC) on cybercrime also concluded that: *"analysis of formal and informal cooperation mechanisms is unable to find that the current global cooperation situation is sufficient"* (UNODC 2013, p. 208).

As a result of this failure of the mutual legal assistance model for cybercrime investigations, the international legal regime needs to be amended in relation to digital evidence-gathering activities. Current mutual legal assistance treaties seem to ignore the fact that law enforcement officials already gather digital evidence unilaterally across State borders. Treaty authors appear to think only in terms of a world in which law enforcement officials have to physically cross borders to gather evidence. All States should start including the concept of digital evidence-gathering activities in their bi- and multilateral mutual legal assistance treaties. They should also make efforts to reach agreements with other States concerning the conditions under which cross-border unilateral digital evidence-gathering activities are acceptable.

Chapter 9 illustrated the manner in which digital investigative methods are today being applied unilaterally across State borders in a territorially partitioned legal world. The cross-border unilateral application of investigative methods on foreign territory should be allowed insofar as the investigative methods do not interfere with the territorial sovereignty of the involved States and legal certainty in an unacceptable manner. The problem is that States have different perspectives on (1) the severity of the infringements of

14 These reports can also include statistics regarding the use of special investigative powers in the Netherlands. In 2012, the former Dutch State Secretary of the Ministry of Security and Justice refused to publish statistics regarding data production orders, stating such information could harm criminal investigations and even citing national security grounds (*Aanhangsel Handelingen* II 2011/12, no. 2011Z23302 (Answer to Parliamentary questions of the El Fassed about online privacy). The argument that these statistics harm law enforcement investigations or national security was poorly motivated. See J.J. Oerlemans, 'Our government should provide statistics about online data collection', *Leiden Law Blog* 2012. Available at http://leidenlawblog.nl/articles/our-government-should-provide-statistics-about-online-data-collection (last visited on 25 November 2014).

their territorial sovereignty that occur when investigative methods are used on their territory by foreign law enforcement authorities and (2) the gravity of the privacy interferences that take place for the individuals involved in these cross-border unilateral cybercrime investigations. This was illustrated in chapter 9 through a legal comparison between the Netherlands and United States with regard to the identified investigative methods.

The danger is that a situation will arise in which law enforcement authorities from all over the world engage in cross-border unilateral evidence-gathering activities that are regulated by their own domestic laws. An unrestricted cross-border unilateral application of investigative methods is undesirable, because it may result in diplomatic tensions between States or other political repercussions and a practice that is not foreseeable to the individuals involved. A key aspect of both the right to privacy and the rule of law is that individuals can foresee the conditions under which law enforcement authorities can use governmental power to prevent and investigate crimes and in doing so interfere in their private lives.

The task ahead

The way forward is to harmonise criminal procedural laws and elaborate the conditions under which States can apply certain digital investigative methods unilaterally across State borders. States should engage in negotiations with each other to attempt to agree on the terms under which foreign law enforcement authorities can remotely gather evidence on foreign territory unilaterally, i.e., without consent or mutual legal assistance from local law enforcement authorities. This will require the development of a common understanding concerning the circumstances under which law enforcement authorities may conduct cross-border unilateral evidence-gathering activities (cf. UNODC 2013, p. 223). I prefer that the minimum safeguards derived from art. 8 ECHR are set as a standard. States must yield part of their territorial sovereignty to combat cybercrime more effectively while simultaneously providing a degree of legal certainty and protection for their citizens by agreeing to the conditions under which cross-border digital evidence activities can take place. However, this is easier said than done.

Previous initiatives to create a global cybercrime convention with an international cybercrime court have not taken root.[15] States are apparently unwilling to give up part of their territorial sovereignty to regulate how evidence can be collected on their territory in an online context (cf. Brenner 2010, p. 173). It is more realistic to aim for States agreeing on the conditions under which other States can collect evidence using network searches

15 See, e.g., Chief Judge Stein Schjølberg, 'Report of the Chairman of HLEG to ITU Secretary-General Dr. Hamadoun I. Touré', *ITU Global Cybersecurity Agenda (GCA)*, High-Level Experts Group (HLEG) 2008, p. 6-9. Available at: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (last visited on 25 February 2015). See also Stein Schjølberg and Solange Ghernaouti-Helie, 'A Global Treaty on Cybersecurity and Cybercrime', 2nd ed., 2011.

and data production orders on foreign territory within the Convention on Cybercrime, since negotiations are already under way for these investigative methods (cf. Koops & Goodwin 2014, p. 83). It may also be possible to create a mutual legal assistance treaty between the EU and the United States for cross-border unilateral data production orders that are issued to online service providers.[16] The Netherlands can also pursue the further harmonisation of criminal procedural powers on the EU level. Unfortunately, the harmonisation of any criminal procedural powers between EU Member States has been ignored in the most recent EU initiative on combating cybercrime.[17]

In the meantime, the Netherlands and other States should create a policy for cross-border unilateral digital evidence-gathering activities and be aware of the consequences that these investigative activities may have on both State sovereignty and the rights and freedoms of the individuals involved. Chapter 9 presented suggestions that should be considered as a first step towards developing a policy for cross-border unilateral cybercrime investigations. The details of the desirable procedures and treaty provisions must be subjected to further scientific study.

10.4 Chapter conclusion

This chapter evaluated the outcomes of the analyses in the previous chapters to provide overarching observations concerning the study's results. These observations may aid in deciding how we move forward in amending the domestic and international legal frameworks that regulate the digital investigative methods used in cybercrime investigations.

Section 10.1 emphasised how the challenges of (1) anonymity, (2) encryption, and (3) jurisdiction make it difficult for law enforcement officials to gather evidence in cybercrime investigations. The examined digital investigative methods may provide a solid overview of the instruments that law enforcement authorities can use to overcome these challenges in cybercrime investigations. It was pointed out that the special investigative powers that are created to provide instruments for gathering evidence and prosecuting cybercriminals cannot be solely be used to 'disrupt' cybercrime.

In section 10.2 it was argued that Dutch criminal procedural law requires a general overhaul if it is to adequately regulate the use of digital inves-

16 See the press release of the Council of the European Union on 9 June 2016, 'Fight against criminal activities in cyberspace: Council agrees on practical measures and next steps', in which the council concludes that action is required *"in the area of improving cooperation with service providers, through the development of a common framework (e.g. use of aligned forms and tools) with them to request specific categories of data"*. Available at: http://www.consilium.europa.eu/en/press/press-releases/2016/06/09-criminal-activities-cyberspace/ (last visited on 8 June 2016).

17 See the EU Directive 2013/40/EU about 'attacks against information systems' (2013/40/EU (L218/8) of 14 August 2013. See also subsection 2.5.2.

tigative methods. The Dutch legislature's current efforts to update criminal procedural law are insufficient. This study has shown that, in addition to hacking as an investigative power and the seizure of computers, the (1) gathering of publicly available online information, (2) undercover investigative methods, and (3) data production orders also require the attention of the Dutch legislature. A full review of Dutch criminal procedural law to accommodate digital investigative methods should also take the requirements of fundamental rights beyond art. 8 ECHR into consideration. A parallel was also drawn between the events that led to the Dutch IRT affair and the current practice of digital evidence-gathering activities. I have argued that the Dutch legislature and Public Prosecution Service should create legislation where needed and provide more clarity regarding the legal basis in criminal procedural law that is used to apply digital investigative methods.

In section 10.3, the international legal framework for the cross-border unilateral application of the identified investigative methods was evaluated. I argued that harmonisation in the cross-border unilateral application of the identified investigative methods is desirable. However, beyond the existing provisions in the Convention on Cybercrime, the results of the efforts to harmonise digital investigative methods have so far been disappointing. To both combat cybercrime effectively *and* protect the rights and freedoms of the individuals involved, States have to accept that cross-border unilateral digital evidence-gathering activities occur and need to be regulated on an international level. In the meantime, States should create their own policies for cross-border unilateral digital evidence-gathering activities and be aware of the consequences that these investigative activities may have on both State sovereignty and the rights and freedoms of the individuals involved.