Investigating cybercrime

Oerlemans, J.J.

2 Digital investigative methods

This chapter aims to answer the first research question (RQ 1): *Which investigative methods are commonly used in cybercrime investigations?* For this purpose, the technicalities of evidence-gathering activities and the challenges of cybercrime investigations are analysed. The analysis provides a basic understanding of how digital investigative methods are used in practice. The following three-step approach is taken to answer the research question.

In the first step, the object of cybercriminal investigations, namely cybercrime, is examined. The aim is to construct a basic understanding of how computers and the Internet facilitate crime. Knowledge about cybercrime is important to the understanding of how cybercrimes are investigated.

In the second step, digital leads that law enforcement officials must often follow in cybercrime investigations are examined. These digital leads are identified as (1) IP addresses and (2) online handles.[1] Subsequently, the digital investigative methods that are used to gather evidence are based on these two digital leads in cybercrime investigations.

In the third step, three challenges in cybercrime investigations are examined. These challenges are (1) anonymity, (2) encryption, and (3) jurisdiction. These three challenges have already been separately identified and briefly analysed in other literature.[2] Based on the examination of case law, the dossier research, and the conducted interviews, it became clear that these three challenges often influence the course of the investigation. Further analysis of the challenges in cybercrime investigations is required, because law enforcement authorities deal with the challenges by using novel investigative methods. The identification of digital investigative methods used in cybercrime investigations is the aim of RQ 1.

---

1 These two digital leads were chosen based on the examined literature, case law, and dossiers.

2 See most notably: Franken 2004, p. 406 in: Franken, Kaspersen & De Wild 2004. See also for a similar distinction: Europol 2015b, p. 9: *"The main investigative challenges for law enforcement are common to all areas of cybercrime: attribution, anonymisation, encryption and jurisdiction"*. Note that operational challenges to investigate cybercrime are not examined in this study. Factors such as the scarcity of the right technical expertise within police organisations to use digital investigative methods also make it difficult to effectively investigate cybercrime. See, e.g., Wall 2007, p. 160-161, Brenner 2010, p. 162-172, Koops 2010 in: Herzog-Evans 2010, p. 740-741, Struiksma, De Vey Mestdagh & Winter 2012, p. 55, Stol, Leukfeldt & Klap 2012, p. 25-27, and Stol, Leukfeldt & Domenie 2013, p. 78. The premise of this study is that law enforcement authorities have the capacity and right expertise to investigate cybercrime.

The structure of this chapter follows these three steps. Section 2.1 addresses the first step and provides a definition and brief typology of cybercrime. The section further investigates how computers and the Internet facilitate these criminal behaviours. The second step is addressed in section 2.2, which examines how law enforcement officials gather evidence based on the digital leads of IP addresses and online handles. The third step is addressed in the sections 2.3 to 2.5. The three challenges of (1) anonymity, (2) encryption, and (3) jurisdiction are separately examined in order (a) to illustrate how the challenges influence cybercrime investigations and (b) identify which investigative methods are used to overcome the challenges in cybercrime investigations. Finally, section 2.6 concludes the chapter with a summary of the findings.

2.1 Cybercrime as the object of a criminal investigation

The term 'cybercrime' is broadly accepted in literature and has been adopted by the Council of Europe in the Convention on Cybercrime (cf. Clough 2010, p. 9).[3] The term 'cybercrime' is preferred in this study over the term 'computer crime', because the prefix 'cyber' emphasises that both computers *and* the Internet are inextricably linked with the crime. Cybercrime is defined in this study as *"criminal acts committed using electronic communication networks and information systems or against such networks and systems"*.[4] Based on this definition, cybercrimes can be distinguished as:

(1) target cybercrimes: crimes in which a computer is the target of the offense; and
(2) tool cybercrimes: crimes in which a computer is used to facilitate a traditional crime.[5]

This section provides a brief typology of target cybercrimes and tool cybercrimes in subsections 2.1.1 and 2.1.2.[6] Knowledge about both types of cybercrime is required, in order to understand how computers and the Internet are used to commit such crimes and how this subsequently influences cybercrime investigations.

3 Council of Europe, Convention on Cybercrime (ETS No. 185). Adopted on 8 November 2001 in Budapest. Kaspersen (2007, p. 180-182 in: Koops 2007) noted that this convention is the most influential international treaty related to cybercrime.

4 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.

5 See also subsection 1.3.1.

6 These are generic descriptions of cybercrimes that do not necessarily correspond to the national crime depiction of the behaviours in criminal substantive law. The exact content of the crime description may have an influence on the manner it may be investigated. The examination of criminal substantive law with regard to cybercrime goes beyond the scope of this study. See, e.g., Koops 2007 and Kerr 2010 for an analysis of criminal substantive law with regard to cybercrime in the Netherlands and United States.

2.1.1 Target cybercrimes

In target cybercrimes, the computer is the target of the offence. A computer is defined as: "*any device which electronically processes data, stores data, or transfers data*".[7] This definition of a computer encompasses a wide range of different types different types of devices.

For example, the following devices may be understood as computers: (a) PCs, laptops, smartphones, and wearable computing devices (e.g., 'Google Glass'), (b) 'web servers' that deliver web content for websites, and (c) all kinds of computing devices connected to the Internet such as routers, smart meters, and even household appliances and automobiles. All these types of computers are vulnerable to crimes that may endanger the (1) confidentiality, (2) integrity, or (3) availability of computers (cf. Schermer 2010).[8]

Three examples of target cybercrimes are (A) hacking, (B) the use of malware, and (C) the use of botnets. These three crimes are briefly discussed below to illustrate what target cybercrimes entail and how the Internet facilitates these offences.

A Hacking

Hacking is perhaps the best-known example of a 'target cybercrime'. In a criminal context, the term hacking refers to the act of intentionally gaining unauthorised access to computers (cf. Kerr 2010, p. 27). Computers can be hacked in numerous ways. Hacking a computer may be as straightforward as (a) copying a login name and password by looking over the shoulder of an unwary computer user ('shoulder surfing'), (b) posing as a system administrator to trick a person into giving up his[9] login name or password (a form of 'social engineering'), or (c) buying login credentials on an online black market and subsequently using those credentials to gain access to a service. In more technically advanced attacks, hackers exploit vulnerabilities in software in order to gain access to a computer system. Hacking is often used as a vehicle to perpetrate other target cybercrimes.

---

7 This definition resembles the definition for 'automated devices' in the art. 80sexies of the Dutch Penal Code. However, this definition is broader in nature, since the criteria are not cumulative in art. 80sexies Dutch Penal Code. The Dutch Computer Crime Act III aims to expand the definition for automated devices in art. 80sexies Dutch Penal Code (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 92-94).

8 In his article, Schermer (2010) identifies crimes that can be committed with regard to computers that are part of 'ambient intelligent services'. The concept of 'ambient intelligence', which is related to the concepts of 'ubiquitous computing' and 'the Internet of Things', is not considered in this study. See for analysis of these concepts: Greenwield 2006 and Atzoria, Ierab & Morabito 2010. See Goodman 2015 for an analysis of cybercrime in relation to the Internet of Things. See Pfleeger 2003, p. 504 in: Ralston, Reilly & Hemmendinger 2003 for an analysis regarding the elements of (1) confidentiality, (2) integrity, and (3) availability.

9 For readability, 'he' and 'his' are used wherever 'he or she' and 'his or her' are meant.

The Internet facilitates hacking by allowing criminals to gain unauthorised access to computers on a global scale. In target cybercrimes, there is no physical proximity between the perpetrator and the victim of the crime (see Koops 2010, p. 740 in: Herzog Evans 2010).[10] As a result, the leads that law enforcement officials must follow are often digital in nature.

B The use of malware

In order to commit computer crimes, cybercriminals often make use of malicious software, known as 'malware'. Computers can be infected with malware in numerous ways. Malware is often distributed through (a) e-mails with a disguised infected attachment, (b) social media services that link to infected websites (suggesting access to the latest 'viral movie', for example), and (c) malicious advertisements on websites that attempt to exploit vulnerabilities on a computer system.

Malware enables cybercriminals to gain remote access to a computer and take control of the functionalities of a computer. For example, malware can be used to (a) control the user's cursor, (b) log keystrokes, (c) record video through a built-in web cam, (d) record sounds using a microphone in a computer, and (e) take screenshots of the computer screen. These functionalities of malware can be used to commit other cybercrimes.

Once the perpetrator has gained access to an infected computer, the data stored in a computer can be altered, copied, or deleted. Malware can therefore be used to (a) extort individuals by taking computer files hostage, (b) spy on individuals, (c) copy information from infected computers, and (d) direct infected computers to take certain actions. The compromised computer can also be used as a cover – a 'proxy' – to commit other crimes (cf. Clough 2010, p. 28-30).[11] Criminals continuously update malware in order to avoid security measures. These kinds of rapid innovation cycles are characteristic for cybercrime (cf. Koops 2010, p. 741 in: Herzog Evans 2010).

C The use of botnets

A botnet can be defined as a network of infected computers that is controlled by the perpetrator through a 'command-and-control' channel. Botnets can be visualised as follows.

10 Koops cites Yar 2005, p. 421 and Sandywell 2010 in: Jewkes & Yar 2010, p. 44 with regard to these two factors on how the Internet facilitates cybercrime.

11 See subsection 2.3.2 for more information about proxy services.

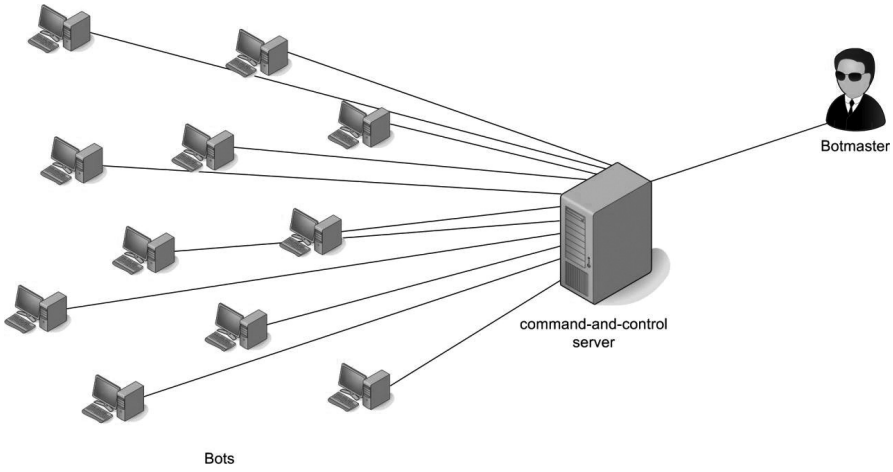

Figure 2.1: Model of a centralised botnet (see Hogben ed. 2011, p. 16).

Figure 2.1 depicts a model of a centralised botnet. It shows how all infected computers connect to one command-and-control server that is controlled by the perpetrator. In practice, the IT infrastructure of botnets is often more sophisticated in nature (see Hogben ed. 2011, p. 18-21). Criminals utilise botnets to commit other crimes, such as (a) sending large amounts of unsolicited e-mail (spam), (b) harvesting personal data (such as login names and passwords) from infected computers, (c) committing 'click fraud'[12], and (d) initiating 'denial of service attacks'[13] (see Hogben ed. 2011, p. 22-25). An organisation is required to commit these crimes and monetise the money that has been obtained by these crimes. A 'malware economy' has arisen following these target cybercrimes (see Van Eeten & Bauer 2008).

The use of botnets by criminals illustrates how computers and the Internet can facilitate crime in an automated process by remotely harvesting data obtained from infected computers (cf. Koops 2010, p. 740 in: Herzog Evans 2010). The use of botnets also illustrates how different target cybercrimes are often committed in conjunction with each other.

12 In click fraud cases, infected computers are directed to visit an advertisement. Criminals can earn money by directing infected computers to pre-selected advertisements.

13 'Denial-of-service attacks' can be characterised as an attack in which large amounts of data ('network traffic') are sent to a computer (usually a server) in order to overload that computer with traffic. As a consequence, websites or internet services facilitated by that server take more time to load and may appear unavailable.

2.1.2 Tool cybercrimes

In tool cybercrimes, computers and the Internet play an essential role, facilitating the commission of traditional crimes a number of ways. In short, criminals can take advantage of computers and the Internet to commit crimes relatively anonymously, across State borders, and even on a global scale, reaching many computer users (cf. Koops 2010, p. 740-741 in: Herzog Evans 2010).[14]

Three examples of crimes in which computers and the Internet are used as tools to commit crimes are (A) child pornography crimes[15], (B) online drug trafficking, and (C) online fraud. These three cybercrimes provide a good overview of how the Internet facilitates tool cybercrimes. They are briefly discussed below.

A Child pornography crimes

Child pornography crimes are a typical tool cybercrime. Child pornography can be defined as images or videos that depict minors engaging in sexual acts. In the past, child pornography was published in magazines and distributed by mail or bought 'under the counter' at kiosks. Since the 1990s, child pornography has predominately been distributed over the Internet (cf. Jenkins 2001).

Computers and the Internet facilitate the possession and distribution of child pornography by enabling child pornographers to access, download, upload, and distribute child pornography materials, without being in physical proximity to the victims (cf. Brenner 2010, p. 167-170). Child pornography users can distribute child pornography through a variety of internet related services, such as e-mail, chat applications, file transfer programs, and online forums (see Oerlemans 2010). The Internet facilitates perpetrators in a global reach by enabling them to target victims and collaborate with others anywhere in the world (cf. Yar 2005, p. 421).

B Online drug trafficking

Computers and the Internet can also facilitate drug trafficking. The Internet essentially provides criminals with a platform to communicate with each other and to trade in illegal goods and information (cf. Paretti 2009, p. 386, Bernaards, Monsma & Zinn 2012, p. 89-96). Specialised online trading forums allow individuals to buy and sell drugs on a global scale. Below is a screen shot of the (now defunct) drug-trading forum 'Silk Road'.

14 Koops provides an overview on twelve ways the Internet facilitates crime, building upon the work of authors such as Brenner 2002, Yar 2005, Wall 2007, and Sandywell 2010 in: Jewkes & Yar 2010.

15 The term 'child pornography crimes' refer to the possession, import, export, distribution, fabrication, and access to child pornography.

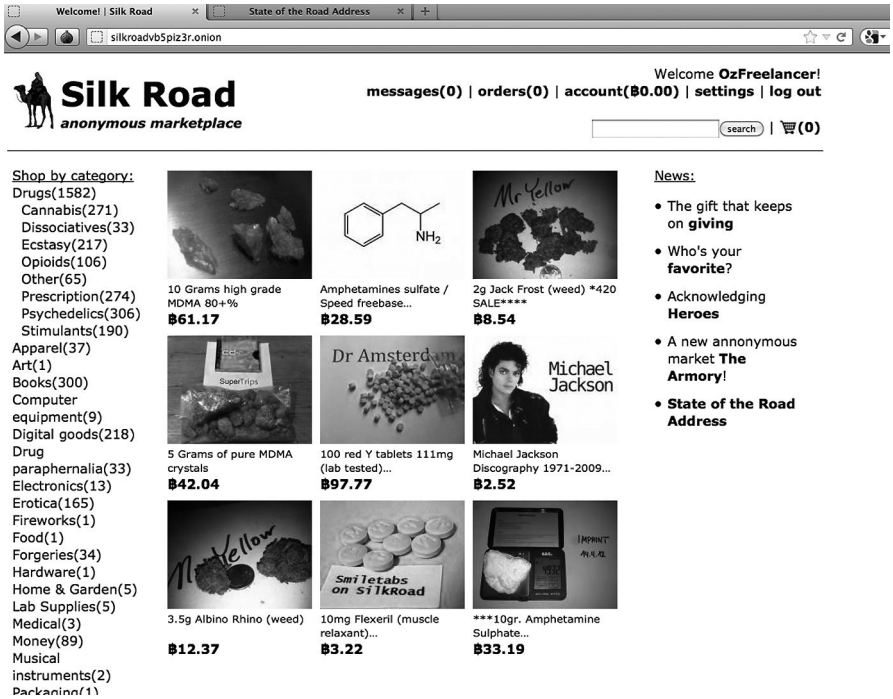

Figure 2.2: Screen shot of the Silk Road forum. Eileen Ormsby, 'The drug's in the mail', 27 April 2012, TheAge.com. Available at: https://allthingsvice.files.wordpress.com/2012/05/screen-shot-2012-04-24-at-2-02-25-am.png (last visited 30 September 2015).

Figure 2.2 illustrates how these forums bring together internet users that want to buy and sell (mostly) drugs. Silk Road was a very successful online black market that facilitated the trade in illicit goods and services, primarily drugs.[16] The U.S. prosecutor contended that during its 2,5 years in operation, Silk Road was used by several thousand drug dealers to distribute hundreds of kilos of drugs to over a 100,000 buyers. From those transactions, reportedly laundered hundreds of million ns of dollars were laundered through the forum.[17] The administrator of the forum obtained money by facilitating and withholding of a small percentage of the transactions between users of

16 The website gained popularity after an interview with the administrator of the forum, Ross Ulbricht, was published on the website Gawker (See Adrian Chen, 'The Underground Website Where You Can Buy Any Drug Imaginable', 1 June 2011, Gawker. Available at: http://gawker.com/the-underground-website-where-you-can-buy-any-drug-imag-30818160 (last visited on 30 September 2015).

17 See p. 6 of the indictment of the United States against Ross Ulbricht. Available at: https://www.justice.gov/sites/default/files/usao-sdny/legacy/2015/03/25/US%20v.%20Ross%20Ulbricht%20Indictment.pdf (last visited on 30 September 2015).

the forum.[18] The increase of online black markets specialising in drug trafficking in the last five years, illustrates how the Internet provides a global platform for criminals to distribute illegal goods and services (cf. UNODC 2014, p. 18 and Europol 2015a, p. 31).[19] An important factor may also be that the Internet can provide (a degree of) anonymity when individuals make use of specialised services. This aspect is further examined in section 2.3.

C Online fraud

Clough (2010, p. 372-373) submits that online fraud is *"undoubtedly one of the most common forms of cybercrime"*. He argues that (1) the scale of potential victims, (2) the anonymity that the Internet provides to the perpetrators, and (3) the ease of communication are factors that facilitate fraudulent online scams. Indeed, most people are familiar with scams sent by e-mail with fraudulent investment opportunities or scams that aim to trick people into transferring funds. Online fraud is a rather broad category of tool cybercrimes, whilst it is often also closely linked to target cybercrimes.

An example that illustrates how online fraud is committed and how this tool cybercrime is intertwined with the commission of target cybercrimes follows hereinafter. In an online fraud scheme in which criminals use 'banking malware', criminals often send an innocent looking e-mail to victims that lure them into clicking on a link.[20] That link then directs the victim to a website that automatically downloads so-called banking malware on the computer system of the victim, insofar the victim's computer is vulnerable to the attack. When the victim attempts to electronically transfer funds from his online banking website, the banking malware turns into action and

18 See Pammy Olson, 'The man behind Silk Road – the internet's biggest market for illegal drugs', *The Guardian*, 10 November 2013. Available at: http://www.theguardian.com/technology/2013/nov/10/silk-road-internet-market-illegal-drugs-ross-ulbricht (last visited on 20 November 2015). After the arrest of the forum administrator, Ross Ulbricht, his laptop was seized. His laptop contained 144,336 bitcoins, a virtual currency worth more than 28 million dollars at the time. See the press release of the U.S. Department of Justice, 'Manhattan U.S. Attorney Announces Forfeiture Of $28 Million Worth Of Bitcoins Belonging To Silk Road', 16 January 2014. Available at: http://www.justice.gov/usao/nys/pressreleases/January14/SilkRoadForfeiture.php (last visited 30 September 2015.

19 See also Patrick Howell O'Neill, 'Dark Net markets offer more drugs than ever before', *The Daily Dot*, 15 May 2015. Available at: http://www.dailydot.com/crime/dark-net-census-growth-37-percent/ (last visited on 3 August 2015). For a recent example of online drug trading forums originating in the Netherlands, see: *ANP*, 'OM wil tot zeven jaar cel voor Internetdealers', *Nu.nl*, 23 September 2014. Available at: http://www.nu.nl/Internet/3885624/wil-zeven-jaar-cel-Internetdealers.html (last visited on 17 April 2015) and J.J. Oerlemans, 'Veroordelingen voor drugshandel via online marktplaatsen', *Computerrecht* 2015, no. 3, p. 170, relating to the cases of Rb. Midden-Nederland, 9 October 2014, ECLI:NL:RBMNE:2014:4790 and ECLI:NL:RBMNE:2014:4792.

20 See, e.g., Rb. Rotterdam, 20 July 2016, ECLI:NL:RBROT:2016:5814, *Computerrecht* 2016/175, m.nt. J.J. Oerlemans. Note that many more attack methods are available to criminals.

instead transfers money to a different recipient (cf. Sandee 2015).[21] Hence, online fraud (a tool cybercrime) has taken place with the aid of hacking and malware (a target cybercrime).

Note that the criminals who create malware or hack computers to steal information are not necessarily the same people who monetise the information. Furthermore, the process of hacking and monetising the stolen data is highly organised. Criminals often have different professional roles assigned to them in order to deal with the different economic and technical aspects of the crimes.[22] Cross-border online crime groups are often fluid and temporal in nature. In other words, the Internet also permits perpetrators to loosely organise themselves in order to (a) divide labour and (b) share skills, knowledge, and tools to commit crimes (cf. Koops 2010, p. 740 in: Herzog Evans 2010).[23]

2.2 Digital leads

The illustration of target cybercrimes and tool cybercrimes in section 2.1 has shown that cybercrimes can be committed on a large (global) scale, across State borders, reaching many computer users. The investigation of target cybercrime and tool cybercrimes have in common that – at the start of the investigation – there are no physical leads available. The examined literature, case law, and dossiers show that the only leads that are often available in cybercrime investigations are (1) IP addresses and (2) online handles.

An *Internet Protocol address* is a numerical address that is assigned to a computer, which is part of a computer network and makes use of the Internet Protocol to communicate. Internet access providers also assign an IP address to the network device that computers use to access the Internet. For example, the (public) IP address assigned to the network device that this author's working station is connected to at Leiden University is '132.229.159.109'. IP addresses usually consist of four sets of numbers between 0 and 255.[24] As a digital lead, IP addresses often do not specifically identify the device that an individual utilises, but they do provide law enforcement officials with a clue about the particular network that a person uses for his internet connection. Law enforcement officials can attempt to

21 Sandee describes in his report how the popular type of banking malware, called ZeuS, infected computers and siphoned money of the online bank accounts of its victims. The report also describes the sophisticated organisation behind the malware.

22 See, e.g., Hogben ed. 2011, p. 21, Soudijn & Zegers 2012, p. 114-115 and Sandee 2015.

23 See for further analysis, e.g., Brenner 2002, p. 45-47, Choo 2008, p. 276, McCusker 2006, p. 267, Paretti 2009, p. 398, Soudijn & Zegers 2012, p. 114-115 and Europol 2015a.

24 This is only true insofar the IP address uses the IP protocol version 4 (IPv4). Steadily, IP addresses with IP protocol version 6 (IPv6) replace IPv4. The transition from IPv4 to IPv6 will impact digital investigations (cf. Bernaards, Monsma & Zinn 2012, p. 135-136). An analysis of the manner in which the transition to IPv6 impacts cybercrime investigations is beyond the scope of this study.

identify a computer user by requesting or ordering the disclosure of data from the organisation or person that has information about the devices and computer users within a network. The investigation process based on IP addresses as a digital lead is further explained in subsection 2.2.1.

An *online handle is* a name an individual uses to interact with other individuals on the Internet. An online handle may be the real name of an individual. On the Internet, it is also common to use pseudonyms, called 'nicknames', as online handles when communicating with other people. Nicknames are often used on online discussion forums or chat channels. Online handles can also consist of the first part of an e-mail address and profile names on social media services. Online handles are a digital lead for three reasons. They (1) can allow law enforcement officials to gather publicly available information about an internet user, (2) can direct law enforcement officials to an online service provider that may hold information about an internet user, and (3) can enable law enforcement officials to interact (undercover) with the individual. The investigative process based on online handles in cybercrime investigations is further explained in subsection 2.2.2.

This section (section 2.2) thus examines the two digital leads that law enforcement officials follow in cybercrime investigations and the investigative methods that law enforcement officials subsequently use to gather evidence. Creating a clear understanding of the actual – technical – acts involved therein will create a basis for the analysis of digital investigative methods (with their accompanying legal frameworks), which will be analysed in the following chapters.

2.2.1 Tracing back an IP address to a computer user

As explained in the introduction of this section, public IP addresses do not specifically identify the device that an individual utilises. However, they do provide law enforcement officials with a clue about the particular network that a person uses for his internet connection. Figure 2.3 illustrates how computers in a residence are connected to the Internet by a network connection device, such as a router.[25]

25 A router 'routes' traffic by cable or WiFi to a connected computer.

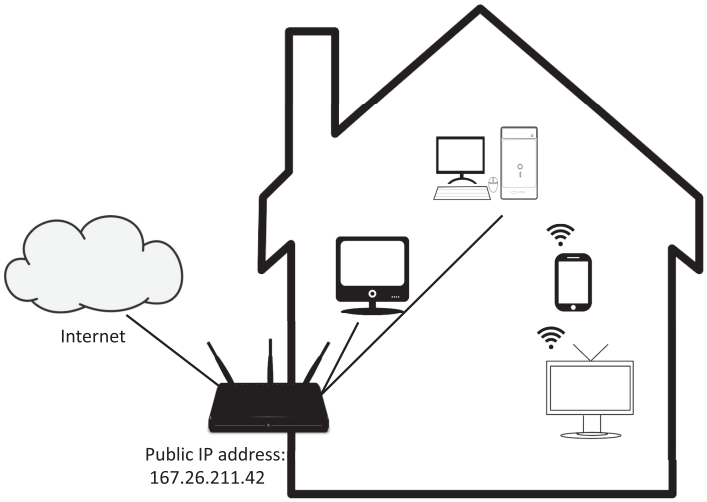

Figure 2.3: Simplified model of a residential internet connection.

Tracing back a computer user on the basis of an IP address as a digital lead can take place as follows. Imagine that in a criminal investigation related to a hacking case, an IP address is available because detection systems logged a suspect IP address at the time the hacking incident occurred. As illustrated above, the logged IP address could be the 'public IP address' of a router, distributing a broadband internet connection to the devices that members of a household utilise to access the Internet. Using publicly available services, law enforcement officials can often find the organisation to which that specific IP address is assigned.[26] In the event that an internet access provider allocates the IP address to a subscriber, law enforcement officials can send a *data production order* to an internet access provider to identify the customer. A data production order requires the custodian of data to deliver or make data available to law enforcement authorities within a specified period. Internet access providers usually retain logs of the IP addresses assigned to customers for billing and security purposes. As a result, internet access providers are often able to provide the identity of the subscriber that has been assigned a specific IP address to law enforcement authorities.

Using the name and address information that belong to a subscriber, law enforcement agents may be able to locate the suspect.[27] To establish a link between (1) the crime, (2) the IP address, and (3) the suspect, the application of additional investigative methods – such as performing a digital forensic analysis of a router distributing the internet connection and interviewing

26 Visit, for example, http://whois.domaintools.com and type in '132.229.159.109' to trace the IP address to the company or institution that allocated it. The query will unsurprisingly return contact data from Leiden University (last visited 19 January 2014). However, the information is often not up-to-date or accurate.

27 See for a more extensive analysis Clayton 2004, p. 17-25.

members of the household – may be required. Information that is available on seized computers can also provide law enforcement authorities with further evidence of a crime.

The above example represents an ideal situation for law enforcement officials, i.e., when an IP address is allocated by an internet access provider and directly relates to the residential internet connection that a suspect uses. However, even in that ideal situation, law enforcement officials still need to take several steps (and have to invest considerable time and energy in the process) to prove that the suspect used the identified computer when the crime was committed. Nevertheless, the digital lead in the form of an IP address will often be an indispensable starting point.

2.2.2 Online handles

As explained in the introduction of section 2.2, online handles can enable law enforcement officials to identify an internet user in three different manners.[28] Online handles can (1) allow law enforcement officials to *gather publicly available information* about an internet user, (2) can direct law enforcement officials to an online service provider and information about internet users with *data production orders*, and (3) can enable law enforcement officials to interact with the individual that makes use of a particular online handle by using *online undercover investigative methods*. These three investigative activities of law enforcement officials are described below.

A Gathering publicly available online information

Online handles provide law enforcement officials with a lead to collect information about an individual that is publicly available on the Internet. Publicly available information can be defined as information that anyone can lawfully obtain (a) upon request, (b) through purchase, or (c) observation (cf. Eijkman & Weggemans 2012, p. 287).[29] The term 'publicly available information' is derived from article 32(a) of the Convention of Cybercrime and includes information provided by a third party that is only available after registration or payment.[30]

---

28 Note that the use of nicknames by criminals is common, as they will be inclined to hide their real identities (cf. Fabers 2010, p. 131-132). Cybercriminals often know each other only by nickname and may have never even met in real life (cf. Choo 2008, p. 277). Interviews with law enforcement officials and the dossier research conducted in the course of this research indeed showed that cybercrime suspects in those cases always use nicknames.

29 Eijkman &Weggemans refer to the National Open Source Enterprise, Intelligence Community Directive 301 of July 2006 for this definition.

30 Note how the Europol Decision of 2009 stipulates *"(...) Europol may directly retrieve and process data, including personal data, from publicly available sources, such as media and public data and commercial intelligence providers* (...)". See art. 25(4) of the Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/271/JHA), L 121/51.

An online handle may in itself provide the information required to identify a suspect. It may also be the beginning of a 'digital trail' that may be followed as individuals use the Internet. Such trails may include information about individuals who are of interest to a criminal investigation that is posted by *other* internet users.

In this study, the gathering of publicly available online information as an investigative method is further distinguished as: (A1) the manual gathering of online information, (A2) the automated gathering of publicly available online information, and (A3) the observation of the online behaviours of an individual. These types of gathering publicly available online information as an investigative method are examined below.

A.1 Manual gathering of online information

Law enforcement officials can manually gather publicly available online information. In its most elementary form, the investigative method consists of a law enforcement official looking for information about a person on the Internet by typing in key words on an internet search engine, such as Google. Information that is publicly available online can be gathered from a wide variety of sources, including: (a) websites open to the general public, (b) social media websites, (c) online phone directories, (d) discussion forums and blogs, (e) news articles, and (f) commercial or scientific reports (cf. Carter 2009, p. 285).

A.2 Automated gathering of publicly available online information

Information that is publicly available on the Internet can also be collected using automated data collection systems. Law enforcement authorities have an interest in making large amounts of online data available to them and making use of the available data as efficiently as possible.[31] Against that background, software has been developed for this purpose that essentially 'vacuums' relevant information from publicly available sources on the Internet and pre-emptively stores that information in police systems. That way, the information can be made accessible to law enforcement officials later in time. For instance, so-called 'crawler' and 'spider' software automatically look for relevant information on the Internet based on certain parameters, such as certain search terms or images (cf. Lodder et al. 2014, p. 70). 'Scraper' software can also automatically download the online data onto computer systems. Automated data collection systems can find information on the Internet more efficiently and provide information to law enforcement officials more effectively.

31 For instance, the Dutch iColumbo system reportedly aims to provide *"an 'intelligent, automated, "near" real-time Internet monitoring service' for governmental investigators"*. See 'Deelprojectvoorstel, Ontwikkeling Real Time Analyse Framework voor het iRN Open Internet Monitor Network', 'iColumbo'. Available at http://www.nctv.nl/Images/deel-projectvoorstel-ontwikkeling-icolumbo-alternatief_tcm126-444133.pdf (last visited on 23 December 2015).

Koops (2013, p. 655) highlights that automated data collection systems may include advanced options, such as: *"plug-ins that enhance the search and analysis capacities of Internet searches, for example, through entity recognition, image-to-image conversion, and automated translation"*. Commercial services that automatically collect and analyse publicly available online information are also available to law enforcement authorities. For example, the Dutch company 'Obi4Wan' collects information from more than four hundred thousand internet sources every day in order to provide 'online monitoring' solutions.[32] Law enforcement can also obtain a quick overview of a suspect's social media network by using tools that map out an individual's friends on social media profiles. Internet monitoring systems can also harvest relevant information for extended periods of time, enabling law enforcement officials to create a timeline of an individual's online behaviours or online communications. Once the information is harvested, individuals can no longer delete online posts or alter information to prevent others from acquiring the information. All publicly available information that a suspect or other individuals post online is theoretically available to law enforcement officials in a criminal investigation.

A.3 Observing online behaviours of individuals

Law enforcement officials may also observe the behaviours of individuals on publicly accessible places online based on an online handle. For instance, law enforcement officials can take detailed notes about public posts that an individual makes on online services such as social media services, online forums, and chat services.

Similar to visual surveillance in the physical world, this investigative method allows law enforcement officials to learn more about the individual involved in the criminal investigation by observing his online behaviours. The observation of an individual's online behaviours can be regarded as the digital equivalent of the investigative method of 'visual observation' in the physical world.

The difference between the manual gathering of publicly available online information and the observation of online behaviours is that the manual gathering regards *information that has already been published* by individuals, and the observation of online behaviours concerns *new information that is being generated by individuals*.[33]

32 See http://www.obi4wan.com/online/social-media-monitoring/ (last visited on 19 September 2015). Although the service is mainly advertised to be useful for 'reputation management', the service also ensures that relevant information that has been posted online is available for further analysis. According to their website, Obi4Wan counts the Dutch national police as one of their clients.

33 See for a similar distinction CTIVD 2014, p. 9 and p. 42.

B Data production orders

Online handles can also provide a lead to an online service provider that stores information about an individual that may be of interest to law enforcement authorities. For instance, an online handle that consists of an e-mail address that ends with '@gmail.com' is obviously from the popular webmail service offered by Google, Gmail. In that event, law enforcement authorities may be able to obtain data of a specific account holder at Gmail with a data production order issued to Google. As explained in subsection 2.2.1, a data production order requires the custodian of data to deliver or make data available to law enforcement authorities within a specified period.

Many different types of structured and unstructured data (e.g., account information, traffic data, and stored documents) are stored and processed by third parties. This study focuses on data production orders that are issued to online service providers, since these providers often provide important evidence in cybercrime investigations. Data production orders that are issued to online service providers can be divided into the following four categories: (1) subscriber data, (2) traffic data, (3) other data, and (4) content data. The categorisation is largely based on the distinctions made with regards to production orders in the Convention on Cybercrime.[34] The four categories of data production orders are further examined below.

The first category, subscriber data, relates to subscriber data from online service providers. The category of subscriber data entails the following data: (a) the type of communication service used, the technical provisions taken, and the period of service, (b) a subscriber's name, postal or geographical address, telephone number, billing and payment information, and (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.[35] Subscriber data can thus be used to identify a suspect based on such information.

The second category, traffic data, consists of data that is generated by a computer system as part of the chain of communication. Traffic data can reveal the following information about a communication: origin, destination, route, time, date, size, duration, and type of underlying service.[36] Law enforcement officials can obtain valuable evidence by analysing network traffic data (cf. Oerlemans 2012, p. 31).[37] Traffic data may enable law enforcement officials to learn about (a) the device that a suspect uses, (b) the internet services that a suspect is using at a specific time, and (c) the suspect's device's location data.

---

34 Council of Europe, Convention on Cybercrime (ETS No. 185). Adopted on 8 November 2001 in Budapest. See art. 16-18 of the Convention on Cybercrime.

35 Art. 18(3) Convention on Cybercrime.

36 Art. 1(d) Convention on Cybercrime.

37 See also the analysis of Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited on 18 August 2015).

The third category, other data, is not identified in the Convention on Cybercrime. The category of 'other data' is data that is not subscriber data, traffic data, or content data (which will be described below). For example, other data can consist of individuals' profile information that may depict information such as the date of birth, relationship status, sexual orientation, and political views, which may be available at social media providers. Profile information can aid law enforcement officials in gathering more information about the background and network of individuals surrounding an individual.

The fourth category, content data, is named but not explicitly defined in the Convention on Cybercrime. Content data is 'data with regard to the meaning or message conveyed by the communication, other than traffic data'.[38] This category of data consists of private messages that can be sent using online service providers. Arguably, the category also entails stored documents that are available from online storage providers. Law enforcement officials can gather content data from online service providers with data production orders. This data may provide them with evidence about the crime that is under investigation, but can also enable them to learn about a suspect and his surroundings, which can influence the use of other investigative methods (see Odinot et al. 2012, p. 91-94).

C Online undercover investigative methods

An online handle can provide law enforcement officials with an opportunity to interact with the individuals involved in a criminal investigation. When a suspect or an individual that has valuable information for law enforcement authorities is active on a social media service, law enforcement officials can interact with that individual on the Internet. For instance, law enforcement officials can add themselves to a suspect's network by introducing themselves as 'friends' of the suspect. These activities can be identified as *online undercover investigative methods*.

The distinguishing feature of undercover investigative methods, as compared to other investigative methods, is that law enforcement officials *interact* with other individuals – using a fake identity – in order to gather evidence in a criminal investigation (cf. Marx 1988, p. 11-13 and Kruisbergen & De Jong 2010, p. 239). In this context, a fake identity means that they do not reveal that they are law enforcement officials. In undercover investigations, suspects are both unaware of the purpose and the identity of the undercover agents (cf. Joh 2009, p. 161). Although this study focuses on evidence-gathering activities by law enforcement officials, it is important to point out that civilians can be recruited by law enforcement authorities to act as informants and to collect information about suspects in criminal investigations. In an online context, this provides law enforcement officials with the opportunity to request an informant's login credentials and to use

38 Explanatory memorandum Convention on Cybercrime, par. 209.

his online account to gain access to otherwise private information.[39] For example, with access to the online account of an informant, law enforcement officials can view content that is only accessible to members of an online forum. Informants can also be instructed to interact with other individuals and to log those communications for law enforcement officials.

Online undercover investigative methods that are applied by law enforcement officials can be distinguished in the following investigative methods, which are commonly used in cybercrime investigations: (1) online pseudo-purchases, (2) online undercover interactions, and (3) online infiltration operations.[40]

The first undercover investigative method, performing an online pseudo-purchase, can best be described as a scenario in which an undercover law enforcement official poses as a potential buyer of an illegal good in order to gather evidence of a crime. For example, law enforcement officials can buy drugs from a drug dealer to gather evidence in a criminal investigation. In a similar way, law enforcement officials can, for instance, buy stolen data and weapons from vendors in online forums in order to collect evidence in a cybercrime investigation.[41]

The second undercover investigative method, performing online undercover interactions with individuals, can take place on many online services, such as chat services, private messaging services, social media services, online discussion forums, and online black markets.[42] With the right knowledge of internet subcultures, law enforcement officials can interact and build relationships with individuals under a credible, fake identity in order to gather evidence in criminal investigations (cf. Siemerink 2000b, p. 145 and Petrashek 2010, p. 1528).

---

39 Problems may arise when law enforcement officials make use of an individual's existing personal information, such as a profile photo of a social media service or a name of an individual, without consent. See, e.g., the following quote in a news article covering a high-profile case in which the DEA used personal information of suspect for investigation purposes: "*After her cellphone was confiscated when she was arrested, a DEA agent named Timothy Sinnigen used the photos on her phone, including images of Arquiett in her skivvies and Arquiett with her son and niece, to create a profile page in her name so he could contact people he suspected of being involved with drugs*" (Kate Knibbs, 'DEA Used a Woman's Private Photos to Catfish Drug Dealers on Facebook', *Gizmodo*, 20 January 2015. Available at: http://gizmodo.com/doj-will-pay-134k-for-catfishing-drug-dealers-with-wom-1680743269). The woman involved successfully sued the U.S. Justice Department and settled for 134,000 dollars.

40 This distinction is used in Dutch criminal procedural law and has been identified in the examined case files.

41 See, e.g., Arrondissementsparket Amsterdam, 'Pseudokoop wapen met bitcoins door politie en OM', 17 January 2014. Available at: https://www.om.nl/vaste-onderdelen/zoeken/@32570/pseudokoop-wapen/ (last visited on 17 March 2016).

42 See, e.g., Landelijk Parket, 'Undercover onderzoek naar illegale marktplaatsen op Internet', 14 February 2014. Available at: https://www.om.nl/@32626/undercover-onderzoek/ (last visited on 17 March 2016).

The third undercover method distinguished in this study is performing an online infiltration operation. Infiltration operations are similar to undercover interactions with individuals. However, infiltration operations are characterised by the fact that undercover agents are authorised (to a certain extent) to participate in a criminal organisation in order to maintain cover and to gain a targeted individual's trust in a criminal investigation (cf. Joh 2009, p. 166). In infiltration operations, law enforcement officials can *participate* in a criminal organisation in order to gather evidence in a criminal investigation and to gain access to the upper echelons of a criminal organisation (cf. Joh 2009, p. 167). These operations can also take place, for instance, through participation in a criminal organisation that is active on an online black market.

The following case is illustrative of a successful infiltration operation of an online black market. In 2006, the FBI conducted an innovative undercover operation on the online forum 'DarkMarket'.[43] DarkMarket was an online black market in which participants specialised in trading stolen credit cards. Access to the market was only provided through an introduction of another forum member. To infiltrate the forum, an FBI agent was provided a cover by the non-profit private organisation Spamhaus, which combats spam and other cybercrimes. With the cover of the made-up criminal 'Pavel Kaminski', reported by Spamhaus as a notorious Eastern European cybercriminal, access was granted by other forum members to the DarkMarket forum. Using the nickname of 'Master Splyntr', the undercover FBI agent was able to climb to the highest levels of the organisation behind the forum. The undercover agent identified other forum members by interacting with them online. The FBI agent also secretly sent network traffic from the forum to a computer of the FBI that logged the IP addresses associated with all the forum's registered members. Ultimately, the FBI arrested fifty-eight individuals and proclaimed it had prevented seventy million dollars in damage.[44] The FBI concluded that: "*what's worked for us in taking down spy rings and entire mob families over the years -embedding an undercover agent deep within a criminal organization – worked beautifully in taking down Dark Market*".[45] Even after a decade, this online undercover operation is still exemplary for its successful use of the investigative method of infiltration on the Internet.

43 The summary of the DarkMarket investigation is based on the books from Misha Glenny, *DarkMarket: CyberThieves, CyberCops and You*, London: Bodley Head 2011 and Kevin Poulson, *Kingpin. How one hacker took over the billion-dollar cybercrime underground*, New York: Crown Publishers 2011.

44 See the FBI press release "Dark Market' Takedown Exclusive Cyber Club for Crooks Exposed', 20 October 2008. Available at: http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 (last visited on 22 July 2015). The FBI was probably able to prevent damages by informing credit card companies of stolen credit card credentials.

45 See the FBI press release "Dark Market' Takedown Exclusive Cyber Club for Crooks Exposed', 20 October 2008. Available at: http://www.fbi.gov/news/stories/2008/october/darkmarket_102008 (last visited on 22 July 2015).

2.3 The challenge of anonymity

In section 2.2, it was explained how the digital leads of an IP address and an online handle can enable law enforcement officials to gather evidence in a cybercrime investigations. However, cybercrime investigations are seldom as straightforward as explained above. There are three common challenges that law enforcement officials encounter in cybercrime investigations.[46] As mentioned in the introduction of this chapter, these are (1) anonymity, (2) encryption, and (3) jurisdiction.

In this section, the challenge of *anonymity* in cybercrime investigations is further examined. First, the common techniques that cybercriminals use to increase their anonymity by obscuring their IP address are examined in subsections 2.3.1 and 2.3.2. Second, it is explained in subsection 2.3.3 which digital investigative methods law enforcement officials can use to overcome the challenge of anonymity.

2.3.1 Different internet access points

When an individual uses different internet access points (as opposed to typical, household internet connections), it requires (significantly) more effort on the part of law enforcement officials to trace back an IP address.[47] For example, individuals can make use of (a) a WiFi connection of another person, (b) a computer at a cybercafé, and (c) publicly available internet connections (called 'hotspots') at airports, restaurants, or hotels, in order to access the Internet (cf. Bernaards, Monsma & Zinn 2012, p. 61, UNODC 2012, p. 58-60). Law enforcement officials who follow the digital lead of an IP address allocated to these access points will not be directed to the residence or workplace of the suspect, which makes it more difficult to identify a computer user. The example provided below illustrates such a situation.

In 2009, a Dutch minor announced on the online forum '4chan.org' that he would kill his classmates in his Dutch high school.[48] The police likely obtained an IP address from logging information of the post available at 4chan. The IP address was tracked down to a Dutch internet access provider. The subscriber information belonging to the subscription for internet access was subsequently obtained from the provider by use of a data production order. In this case, the suspect used the WiFi connection of his neighbour, thereby leading the law enforcement officials to the residence of his unsuspecting neighbour and her boyfriend, instead of to the suspect's residence. When the law enforcement officials arrived at the suspect's neighbours' house, the neighbours stated that they shared the login credentials

46 These challenges are identified based on literature, the examination of case law, the conducted dossier research, and the conducted interviews.

47 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 11.

48 See Rb. Den Haag, 2 April 2010, ECLI:NL:RBSGR:2010:BM1481.

of their router with a young man living next door to their apartment. This statement provided a new lead to the law enforcement officials and caused them to perform a second search, this time at the residence of the suspect. Eventually, a statement of the suspect himself and a temporary file on his computer containing the actual threat provided the essential evidence for his conviction.[49]

This example illustrates how straightforward it is for cybercriminals to direct law enforcement officials into following the wrong lead. In this case, law enforcement officials were able to identify the suspect. However, this may not have been possible if the suspect had hacked a different WiFi-router to access the Internet that belonged to individuals with no relation to the suspect.[50] As explained above, many other manners exist to access the Internet from a different internet connection. It will depend on the consistency with which an individual makes use of this anonymisation method, the techniques that are used, and the amount of logging information that is available at these internet access points whether an individual can be identified by law enforcement officials.

2.3.2 Anonymising services

There are many anonymising services available on the Internet that make it harder for law enforcement officials to track down suspects based on their IP address (cf. UNODC 2013, p. 143).

The following three services are briefly discussed to illustrate how anonymising services challenge law enforcement officials in gathering evidence: (A) proxy services, (B) VPN services, and (C) Tor.[51]

A Proxy services

Proxy services are services that send network traffic through an intermediary computer; such computers are called 'proxy servers'. A proxy server functions as a gateway. Proxy services strip away the originating IP address. The public IP address of the network connection that a suspect uses is changed to the proxy server's address (cf. Hagy 2007, p. 51-52).[52]

---

49 See Rb. Den Haag, 2 April 2010, ECLI:NL:RBSGR:2010:BM1481, Hof Den Haag, 9 March 2011, ECLI:NL:GHSGR:2011:BP7080 and HR 26 March 2013 ECLI:NL:HR:2013:BY9718.

50 The term 'war driving' is used when referring to the activity of searching for wireless networks to use by using WiFi-enabled equipment such as a laptop from a car (see, e.g., Bryant et al. 2008, p. 113).

51 It is important to note that these three anonymising services are not the only services that provide a degree of anonymity online. For example, Freenet is publicly available software that enables users to anonymously share files and visit websites (see Clarke et al. 2001, and Clarke et al. 2010). In addition, anonymity networks that are still in development – in particular the Invisible Internet Project ('I2P') – may prove to be popular in the near future (cf. Ciancaglini et al. 2013, p. 18).

52 These can be commercially available proxy services, but hacked computers can also act as a gateway for the network traffic of criminals (see Bernaards, Monsma & Zinn 2012, p. 61).

B Virtual Private Network Services

Virtual Private Network services (VPN services) are services that route traffic through an intermediary server, thereby changing the originating (public) IP address of an internet user. In addition to proxy services, VPN services encrypt the internet traffic in transit.[53] The workings of proxy services and VPN services for the situation in which an individual makes use of (broadband) internet connection at this home is illustrated in Figure 2.4.

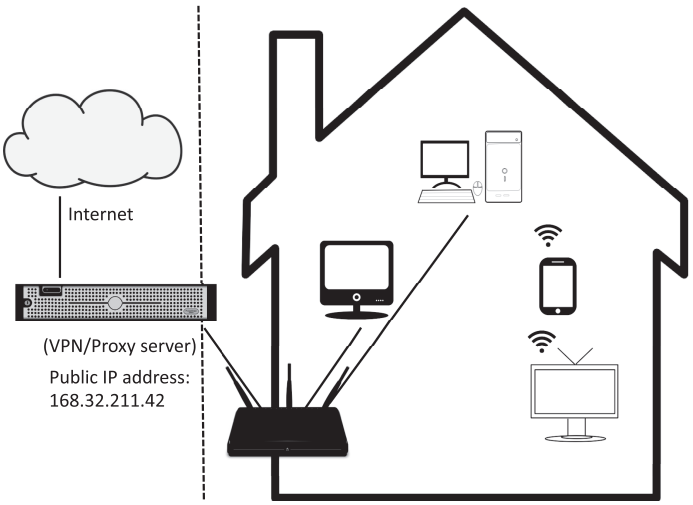

Figure 2.4: Simplified model of an individual that uses of a server of a proxy service or VPN service to access the Internet.

Figure 2.4 illustrates how proxy services and VPN services route traffic through an intermediary server and change the originating (public) IP address of a household internet connection of an internet user to the IP address of a proxy-service provider's server or a VPN-service provider.[54] Proxy-service providers and VPN-service providers provide more anonymity to internet users, because it requires more effort from law enforcement officials to trace an IP address back to the computer user. In essence, intermediary computers are an additional link in the chain.[55]

Law enforcement officials may be still able to trace internet users, depending on the logging information and subscriber data that is available

53 Subsection 2.4.1 under A explains what 'encryption in transit' entails.

54 It depicts a simplified model, because individuals can make use of multiple proxy services or VPN services. Furthermore, individuals can connect to the anonymising services from different places.

55 Internet users can even send network traffic from one proxy to another proxy server or VPN server to create additional links in the chain, e.g., creating a series of obstacles in a criminal investigation. However, the technique may delay network traffic and can create several points of weakness in the ICT infrastructure (cf. Van den Eshof et al. 2002, p. 34-35).

at the anonymity service. Law enforcement officials must examine the log files of the intermediary server of an anonymising service (cf. Casey 2011, p. 693). A logged IP address of a customer may then provide a lead to the originating IP address. Alternatively, law enforcement officials may be able to obtain subscriber data or payment data with data production orders issued to the service, which can be used to directly identify the proxy- or VPN user.

C Tor

Tor is a system designed to anonymise network traffic.[56] The Tor system performs two essential tasks. It *encrypts* network traffic, and it *routes* traffic through relays on its network. Internet traffic goes 'one hop at a time' through relays.[57] Each relay only knows which relay sent the data to it (the last sender) and the next relay through which the data will be routed (first addressee). No individual relay knows the complete path that the network traffic has taken. The Tor system makes sure that traffic analysis techniques cannot establish a link to the connection's source and destination.[58] Using this 'onion routing' technique, Tor makes it possible to use the Internet without revealing the originating public IP address.[59] Note that the Tor system is used by a wide variety of individuals, including (a) people who live in oppressive regimes or activists who are in danger of being prosecuted for their ideas or beliefs, (b) people who want to use the Internet in relative anonymity, and even (c) law enforcement officials who want to use the Internet relatively anonymously.[60] However, the system is also misused by criminals who can (relatively) anonymously trade illegal goods, offer illegal services, and exchange or distribute child pornography (cf. Bernaards, Monsma & Zinn 2012, p. 62, Europol 2015c, p. 19, and Moore & Rid 2016, p. 21).[61]

The workings of the Tor system is illustrated in Figure 2.5.

---

56 Tor is an abbreviation for 'The Onion Routing'.

57 Tor relays are also referred to as 'routers' or 'nodes'.

58 This description of Tor is derived from the article 'What is Tor' from the website of the Electronic Frontier Foundation. Available at: https://www.eff.org/torchallenge/what-is-tor.html (last visited on 6 February 2015) and 'Tor: overview' from the website of the Tor project. Available at: https://www.torproject.org/about/overview.html.en (last visited on 6 February 2015). See Dingledine, Mathewson & Syverson 2004 for a description about the technical workings of Tor.

59 However, some researchers suggest Tor users can be deanonymised. See, e.g., Chakravarty et al. 2014. See also Larry Hardesty, 'Shoring up Tor. Researchers mount successful attacks against popular anonymity network – and show how to prevent them', 28 June 2015. Available at: https://news.mit.edu/2015/tor-vulnerability-0729 (last visited on 27 August 2015).

60 Note that, at the same time, network traffic from Tor can also stand out from regular internet traffic.

61 In the Netherlands, the use of Tor and Tor hidden services by child pornographers became apparent to the public during the prosecution of Robert M. in 2011. See Rb. Amsterdam 23 July 2012, ECLI:NL:RBAMS:2012:BX2325, par 4.4.5 and the press release of the Public Prosecution Service on 31 August 2011, 'Kinderporno op anonieme, diep verborgen websites'. Available at: http://www.om.nl/onderwerpen/verkeer/@156657/kinderporno-anonieme/ (last visited on 1 February 2013).

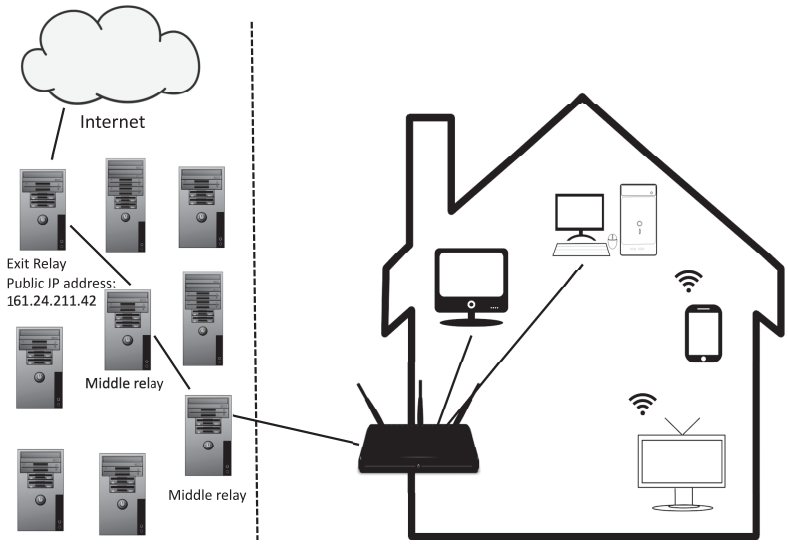

Figure 2.5: Simplified model of how Tor works.

Figure 2.5 illustrates how the Tor system anonymises network traffic by routing internet traffic from one relay to another. Internet traffic that is sent through the Tor system generally passes three relays before it reaches its destination.[62] The first two relays are 'middle relays' that receive traffic and pass it along to another relay. An 'exit relay' is the final relay through which Tor traffic passes before it reaches its destination. Because Tor traffic exits through the exit relay, the IP address of the exit relay is interpreted by others as the source of the traffic.[63] Tor is straightforward to use because it is integrated in a special web browser, which can be downloaded from the website of the Tor project.[64]

Apart from providing the means to hide the originating IP address, the Tor system also allows individuals to access 'hidden services' on the Internet. Hidden services are websites or online services that are only accessible to computers that make use of the Tor system. Tor users can set up a server to publish content on a website, use chat services, and use mail services that are only available to other Tor users.[65] The combination of those websites and services that are publicly accessible and that also hide the IP addresses

62 See https://blog.torproject.org/blog/lifecycle-of-a-new-relay (last visited on 2 February 2015: *"Tor clients generally make three-hop circuits (that is, paths that go through three relays)"*.

63 See 'What is Tor' from the website of the Electronic Frontier Foundation. Available at: https://www.eff.org/torchallenge/what-is-tor.html (last visited on 6 February 2015).

64 See https://www.torproject.org/about/overview.html (last visited on 2 February 2015).

65 See https://www.torproject.org/docs/tor-hidden-service.html.en (last visited on 9 October 2013).

of the servers that run them are referred to as the 'Dark Web'.[66] Since the exact location of these servers is not visible, law enforcement officials cannot use data production orders to gather data from an online service provider. For that reason, at the start of the investigation, other investigative methods must be used to gather evidence.

2.3.3 Overcoming the challenges of anonymity

Law enforcement officials can overcome the challenges of anonymity when investigating cybercrime by using a variety of investigative methods. One such combination of methods is discussed below by detailing the digital investigative methods used in the *Silk Road* investigation. In subsection 2.2.2, it was explained how law enforcement officials can (1) gather personal information about individuals from the Internet, (2) make use of data production orders to gather evidence, and (3) interact with individuals on the Internet using an online handle as a digital lead. Even when individuals make use of anonymising services, an online handle may still provide a powerful lead for law enforcement officials to gather evidence. In addition, law enforcement officials can also gain remote access to computer by use of hacking techniques (called 'hacking as an investigative method' in this study) in order to ascertain the location of the computer.

The *Silk Road* investigation provides a good example of how a combination of investigative methods can enable law enforcement officials to deal with the challenge of anonymity in cybercrime investigations. As explained in subsection 2.1.2, Silk Road was a successful online black market that facilitated the trade in illicit goods and services, primarily drugs. Importantly, Silk Road was a hidden service only accessible through Tor. The webserver of Silk Road and its administrator were therefore difficult to locate for law enforcement officials. The forum administrator used the nickname 'Dread Pirate Roberts' and taunted law enforcement officials by giving interviews to journalists about his successful (and illegal) website.[67] However, the FBI was able to trace 'Dread Pirate Roberts' using the following seven investigative methods:

(1) gathering publicly available online information based on an online handle (i.e., "rossulbricht@gmail.com" that was obtained from an advertisement for Silk Road that Ross Ulbricht (who was identified as Dread Pirate Roberts) posted years before Silk Road became a success);

66 Andy Greenberg, 'Hacker Lexicon: What Is the Dark Web?', *Wired*, 19 November 2014. Available at: http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/ (last visited on 25 November 2014).

67 See Andy Greenberg, 'An Interview with A Digital Drug Lord: The Silk Road's Dread Pirate Roberts', *Forbes*.com, 13 August 2013. Available at: http://www.forbes.com/sites/andygreenberg/2013/08/14/an-interview-with-a-digital-drug-lord-the-silk-roads-dread-pirate-roberts-qa/ (last visited on 20 November 2015).

(2) issuing data production orders to the following online service providers: Google, WordPress, PayPal, and an online forum;
(3) performing online undercover interactions with Ross Ulbricht on TorChat;
(4) performing pseudo-purchases of drugs on Silk Road;
(5) using identified drug dealers on Silk Road as informants in order to learn more about the website's administrator;
(6) gaining remote access to the server by use of hacking techniques[68]; and
(7) seizing the web server in a data centre[69] after a successful mutual legal assistance request to Iceland and search for evidence stored on the seized webserver of Silk Road.[70]

Eventually, U.S. law enforcement officials traced the suspect Ross Ulbricht to the city of San Francisco. By observing the behaviours of Ross Ulbricht in the physical world and by analysing corresponding activities on the Silk Road's server, the investigators were able to match the times at which Ross Ulbricht turned on his computer and logged onto Silk Road as an administrator.[71] On 1 October 2013, the FBI arrested Ross Ulbricht and seized his laptop in a library in San Francisco.[72] His laptop and the seized Silk Road servers contained the necessary evidence to prosecute Ross Ulbricht for drug trafficking and money laundering. On 5 February 2015, he was found

68 See Andy Greenberg, 'Ross Ulbricht Calls For New Trial, Alleging Feds Hacked Tor', *Wired*, 9 March 2015. Available at: http://www.wired.com/2015/03/ross-ulbricht-calls-new-trial-alleging-feds-hacked-tor/ (last visited on 30 September 2015). U.S. law enforcement authorities never acknowledged they hacked Silk Road's server.

69 The data centre also reportedly kept system logs for six months, which showed all the other computers that had recently communicated with the web server.

70 This can deduced from the court documents involving the Silk Road case and the following articles: Nate Anderson and Cyrus Farivar, 'How the feds took down the Dread Pirate Roberts', *Ars Technica*, 3 October 2013. Available at: http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts/, Kim Zetter, 'How the Feds Took Down the Silk Road Drug Wonderland', *Wired*, 18 November 2015. Available at: http://www.wired.com/2013/11/silk-road/, Andy Greenberg, 'Undercover Agent Reveals How He Helped the FBI Trap Silk Road's Ross Ulbricht', *Wired*, 14 January 2015. Available at: http://www.wired.com/2015/01/silk-road-trial-undercover-dhs-fbi-trap-ross-ulbricht/, and Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 May 2015. Available at: http://www.wired.com/2015/05/silk-road-untold-story/ (last visited on 30 September 2015).

71 Ibid.

72 Note that the arrest was orchestrated in such a way that law enforcement authorities were able to keep the laptop logged into the Silk Road server, while the Silk Road server was secured as evidence in Iceland.

guilty of drug trafficking and money laundering.[73] In May 2015, he was sentenced to life in prison.[74]

The investigative methods used to deal with the challenge of anonymity are for a large part the same as the investigative methods used to gather evidence based on the digital leads of a suspect's online handle(s). Additionally, U.S. law enforcement authorities may have hacked the Silk Road server, which IP address was obscured by the use of Tor, in order to overcome the challenge of anonymity and determine its location.[75] This made it possible to seize the server and subsequently secure its contents in a data centre in Iceland by use of mutual legal assistance.

The Silk Road investigation illustrates how much effort it takes for law enforcement officials to track down suspects who make use of anonymising services. At the same time, the Silk Road investigation illustrates how many individuals find it difficult to consistently use anonymising services and protect their identities. Law enforcement officials use those mistakes to collect the required information to successfully gather evidence and identify suspects. In addition, the use of hacking as an investigative method can be a powerful technique to identify suspects by determining the location and contents of their computer.

2.4 The challenges of encryption

In section 2.2, it was explained that IP addresses and online handles are often the only digital leads at the start of a cybercrime investigation. As explained in section 2.3, the use of different internet access points and anonymising services further challenge law enforcement officials during the first stage of an investigation. Once the communication network which a suspect used or the suspect himself is identified, law enforcement officials commonly face another challenge in cybercrime investigations: the use of *encryption*. The term 'encryption' refers to the process of converting data from its original form ('plain text') into an indecipherable or scrambled form ('cipher text') using a mathematical algorithm.[76] Encryption scrambles data in cipher text,

73 See the press release of the U.S. Department of Justice, 'Ross Ulbricht, The Creator and Owner Of The "Silk Road" Website, Found Guilty In Manhattan Federal Court On All Counts', 5 February 2015. Beschikbaar op: http://www.justice.gov/usao/nys/pressreleases/February15/UlbrichtRossVerdictPR.php (last visited on 30 September 2015).

74 See Sam Thielman, 'Silk Road operator Ross Ulbricht sentenced to life in prison', *The Guardian*, 29 May 2015. Available at: http://www.theguardian.com/technology/2015/may/29/silk-road-ross-ulbricht-sentenced (last visited on 30 September 2015).

75 See Andy Greenberg, 'Ross Ulbricht Calls For New Trial, Alleging Feds Hacked Tor', *Wired*, 9 March 2015. Available at: http://www.wired.com/2015/03/ross-ulbricht-calls-new-trial-alleging-feds-hacked-tor/ (last visited on 30 September 2015). U.S. law enforcement authorities never acknowledged they hacked Silk Road's server.

76 For purposes of this study, the exact workings of the technologies used for encryption are not relevant and are therefore not analysed in detail. See, e.g., Schneier 2007, for a technical explanation of the workings of encryption.

making it impossible for law enforcement officials to read the contents of data without the key that decrypts data back into plain text.

The use of encryption challenges law enforcement officials in cybercrime investigations in two situations: (1) during the analysis of data in transit that is encrypted (*encryption in transit*) and (2) when law enforcement officials stumble upon encrypted data on computers during a computer search (*encryption in storage*).[77] A 'computer search' is understood in this study as an investigative method in which law enforcement officials search a place in order to seize documents stored on computers for evidence-gathering purposes.

This section examines the technical challenges of encryption. It also identifies the investigative methods that law enforcement officials use to deal with this challenge. The challenges of encryption in transit and encryption in storage are further examined in subsections 2.4.1 and 2.4.2. The digital investigative methods used to overcome the technical challenges of encryption are examined in subsection 2.4.3.

2.4.1 Encryption in transit

Law enforcement authorities in both the Netherlands and the United States warn that their ability to read the contents of intercepted communications is declining. In general, (internet) wiretaps work as follows. Internet wiretaps intercept all incoming and outgoing internet traffic of a network access device, such as ingoing and outgoing internet traffic from a broadband internet router or ingoing and outgoing internet traffic generated by a smartphone.[78]

As a result of encryption in transit, law enforcement officials are often not able to interpret encrypted network traffic that is generated by parties other than internet access providers.[79] This means that the contents of network traffic, such as private messages that are sent over social media services or apps, cannot be read by law enforcement officials (cf. Bellovin et al. 2014a, p. 12). For instance, in 2014, the popular messaging service WhatsApp implemented 'end-to-end encryption'. Subsequently, law enforcement officials were no longer able to read intercepted information from WhatsApp.

---

77 Authors such as Wiemans (2004, p. 168-169), Byrant et al. (2008, p. 98), and Koops (2012, p. 16) previously made the distinction between encryption in transit and encryption in storage.

78 See Odinot et al. 2012 and Oerlemans 2012 for a more extensive analysis. With regard to wiretapping internet traffic from a smartphones, it is likely that a more unique identifying number is used, such as an IMEI-number or a mobile telephone number.

79 Internet access providers have to decrypt data that these 'public telecommunication service- or network providers' encrypt themselves. Many online service providers are not considered as 'public telecommunication service- or network providers' or reside on foreign territory, outside the reach of law enforcement authorities (see Oerlemans 2012, p. 26).

There is not even a decryption key available at WhatsApp that may be obtained by a legal order, because the keys are stored at the end users' computers.[80] Apple's popular iMessage service reportedly also enables end-to-end encryption and hinders the wiretapping efforts of law enforcement authorities.[81]

Law enforcement authorities view their declining ability to intercept electronic communications in plain text as a major obstacle, because wiretaps have historically provided law enforcement officials with useful evidence in criminal investigations. Stated differently, law enforcement authorities argue that they are '*going dark*', because their practical ability to intercept electronic communications is declining.[82] Below, (A) developments in the use of encryption in transit and (B) other developments that make internet wiretapping less effective are examined.

A Developments in the use of encryption of data in transit

Three developments regarding the use of encryption of data in transit can be distinguished. They challenge law enforcement officials in criminal investigations in particular and are mentioned below.

The first development is the increase of default encryption implemented by popular online communication service providers. For example, Microsoft's webmail Hotmail (now Outlook mail), all services provided by Google, the microblog service Twitter, and the social media service Facebook are all encrypted by default.[83] Intercepted communications from these

80 See Ellen Nakashima, 'WhatsApp, most popular instant-messaging platform, to encrypt data for millions', *The Washington Post*, 19 November 2014. Available at: http://www.washingtonpost.com/world/national-security/whatsapp-worlds-most-popular-instant-messaging-platform-to-encrypt-data-for-millions/2014/11/18/b8475b2e-6ee0-11e4-ad12-3734c461eab6_story.html (last visited 27 November 2014).

81 Dan Goodin, 'Apple's iMessage crypto stymies federal eavesdropping of drug suspect', *Ars Technica*, 4 April 2013. Available at: http://arstechnica.com/tech-policy/2013/04/apples-imessage-crypto-stymies-federal-eavesdropping-of-drug-suspect/ (last visited 29 December 2014). However, see also the (partly technical) analysis of Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited 18 August 2015). Weaver points out that, for example, traffic data is still available for analysis by law enforcement authorities. See subsection 2.2.2 under B with regard to the term 'traffic data'.

82 See the Statement of Valerie Caproni: "*In the ever-changing world of modern communication technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications*". See also Ellen Nakashima, 'Proliferation of new online communications services poses hurdles for law enforcement', *The Washington Post*, 25 July 2014. Available at: http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html (last visited 25 July 2014).

83 Interestingly, the switch to encrypted traffic by these services (except Gmail, because Google's webmail service applied encryption by default before) occurred in only two years' time between 2011 and 2013.

online services are likely no longer readable for law enforcement officials when an internet wiretap is used to gather evidence (unless the results of the communications are publicly accessible on the Internet) (cf. Swire 2012, p. 202-203).

The second development regards the increased use of anonymising services that encrypt network data by default. Internet traffic that is routed through VPNs and Tor is encrypted by default, making the data unreadable for law enforcement officials without the keys to decrypt the data (cf. Koops et al. 2005, p. 61, and Bernaards, Monsma & Zinn 2012, p. 62).[84] In 2015, Europol stated: *"the use of simple proxies and VPNs has continued to increase in the past 12 months and is now the norm amongst cybercriminals"* (Europol 2015b, p. 51). Europol also noted that *"the adoption of Tor as an anonymising solution has seen the greatest growth in the past 12 months, with half of EU Member States noting an increase in its use of obfuscation of criminal activity"* (Europol 2015b, p. 51).

The third development regards the increased use of a manual encryption of electronic communications by individuals. Internet users can manually encrypt specific electronic communication services by using programs such as 'Pretty Good Privacy' (PGP) to encrypt the contents of e-mail messages (cf. Singleton 2008, p. 294-295).[85] Europol noted an increase of the use of encrypted messages with PGP by cybercriminals in 2015 (Europol 2015b, p. 50).

B Other developments in internet wiretapping

It is important to point out that the use of encryption techniques is only one of four reasons why the practical ability of law enforcement officials to intercept electronic communications is declining. The other three reasons for the limited usefulness of internet wiretapping as an investigative method are: (1) legal and geographical limits, (2) the fragmented use of internet connections, and (3) the amount of traffic and diversity in Internet protocols. The other three reasons are briefly considered below.

(1) Wiretapping is legally and geographically limited to the investigating State's territory. Law enforcement authorities can only enforce wiretapping obligations on communication service providers that reside within the investigating State's territory. Law enforcement officials typically wiretap all traffic that is generated by a broadband internet connection from an internet access provider or network traffic generated by smartphones (see Smits 2006, p. 77 and Oerlemans 2012, p. 22). There is no connection available to wiretap when an individual

84 See also the *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9.

85 However, there are news articles that suggest that Dutch law enforcement authorities (with the aid of the National Forensic Institute) are able to decrypt encrypted messages by PGP on certain mobile telephones. See, e.g., Jan Meeus, 'De crimineel sms't, de politie kijkt mee', *NRC Handelsblad*, 20 June 2016.

does not make use of a telecommunication provider within the investigating States territory. For instance, internet wiretapping by Dutch law enforcement authorities can only take place within the territorial borders of the Netherlands. American online service providers cannot be forced to wiretap information for Dutch law enforcement authorities.

(2) When using an internet wiretap, only network traffic from a broadband internet connection or network traffic generated by smartphones can be intercepted. This means that in many cases only part of the network traffic that an individual makes use of during the day is intercepted. The reason is that people also often use WiFi connections and 'hotspots' with WiFi connections offered by restaurants, public transportation companies, and hotels to access the Internet (cf. Koops et al. 2005, p. 61). As a result, law enforcement authorities will often obtain only a fragmented picture of the electronic communications of a targeted individual within a specific time frame (cf. Koops et al. 2005, p. 63, Oerlemans 2012, p. 30-31 and Bellovin et al. 2013, p. 63-64).[86]

(3) The amount and variety of information that is intercepted in a wiretap has strongly increased over the last decade. For law enforcement officials, it is a challenge to interpret the large amounts of internet network traffic generated by many different applications, which often use different communications protocols (cf. Koops et al. 2005, p. 60, Diffie & Landau 2007, p. 55, and Odinot et al. 2012, p. 158).

Considering the above-mentioned developments in internet wiretapping, it is unsurprising that a Dutch evaluation report on wiretapping explicitly states that Dutch law enforcement officials experience the limits imposed by encryption of data in transit as a major challenge in criminal investigations (see Odinot et al. 2012, p. 129).

However, instead of arguing that law enforcement officials are losing wiretapping as an important instrument in criminal investigations, one can also argue that technology provides law enforcement officials with more powerful means of gathering evidence in criminal investigations than in the pre-internet era (cf. Swire and Ahmad 2012). For example, Swire and Ahmad argue that law enforcement are currently experiencing 'a golden age of surveillance' due to (1) the amount of information that is publicly available online, (2) the ability to intercept traffic data (including location data) despite the challenge of encryption in transit, and (3) the ability to acquire data with data production orders from online service providers (cf. Swire and Ahmad 2012, p. 463-474).

86 The Dutch legislator explicitly mentions the wide variety in internet connections as a challenge to fully intercept electronic communications of an individual (see *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 11).

The changes in the investigative powers of law enforcement authorities caused by technological developments indeed seem to lead to a new balance of power. However, when taking together the technological developments that have taken place in the past five years, news articles regarding the use of anonymising techniques and encryption techniques by criminals, the available literature on the topic, and conducted interviews with experts, it appears that the power of law enforcement authorities to intercept communications has declined considerably. This development has a large impact on criminal investigations conducted by Dutch law enforcement authorities. Dutch law enforcement authorities heavily rely on wiretapping as an investigative method in criminal investigations involving serious crime (see Odinot et al. 2012, p. 104-105). Law enforcement authorities must therefore seek alternatives for obtaining the evidence required to successfully prosecute cybercrimes.

2.4.2 Encryption in storage

Law enforcement authorities also view the encryption of data in storage as a growing challenge in criminal investigations.[87] The use of encryption to protect data in storage changes readable (plain text) data on a computer into cipher text. The use of encryption in storage makes the information unreadable for law enforcement officials when the decryption key is unavailable.

Whether law enforcement officials are capable of decrypting data depends on many different factors. For example, the strength of the password used to protect the key is a factor. Depending on the circumstances of the case and encryption techniques that are utilised, law enforcement officials may be able to recover sufficiently incriminating evidence from unencrypted areas of storage media (cf. Casey et al. 2011, p. 129). Law enforcement officials may also be able to exploit the sloppiness of an individual who uses encryption to protect his data (see Koops 2012b, p. 23-24). A telling example of this is the Russian espionage case of Anna Chapman and Mikhail Semenko in the United States. In this case, the FBI managed to overcome the challenge of encryption in storage by recovering pieces of paper containing the necessary passphrases to decrypt the data (see Casey et al. 2011, p. 131). A different strategy is to prevent individuals from turning on an encryption measure. Law enforcement officials will meticulously plan seizures of computers ahead of time in order to seize a suspect's computer while it is still running, thereby giving the suspect no chance to turn on an

87 See, e.g., Faber et al. 2010, p. 118 and p. 300, Brenner 2011, p. 82, Koops et al. 2012, p. 21 and 44-46, and Mevis, Verbaan & Salverda 2016, p. 58. See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 8.

encryption feature (Casey 2011, p. 131).[88] Of course, law enforcement officials can also request that a suspect voluntarily give up his password to decrypt information.

Despite these workarounds to handling the challenge of encryption in storage, it is clear that encryption poses a challenge in cybercrime investigations. Europol stated in 2015 that: *"More than three-quarters of cybercrime investigations in the EU encountered the use of some form of encryption to protect data and/or frustrate forensic analysis of seized media"* (Europol 2015b, p. 50).[89] Two reasons why encryption in storage has become a major challenge in cybercrime investigations are that encryption techniques have become easy to use and that encryption is a standard feature in many computers and operation systems.

In particular, the use of (A) full disk encryption and (B) the encryption of files stored in the cloud pose significant challenges for law enforcement officials in criminal investigations. These encryption techniques are further examined below.

A Full disk encryption

Full disk encryption is a security measure in which a storage medium, such as hard disc, in a computer is fully encrypted. Implementing full disk encryption as a security measure is not difficult. Freely available encryption software, such as TrueCrypt, can fully encrypt a storage medium. Full disk encryption is also offered as a standard security option on computers (cf. Chatterjee 2011, p. 276). For law enforcement authorities, it is reportedly not possible to 'break' modern encryption within a reasonable timeframe (cf. Europol 2015b, p. 69).

In 2014, the director of the FBI first publicly declared how standard encryption measures on iPhones and Android phones also hamper law enforcement officials.[90] Apple and Google reportedly encrypt their phones "*so thoroughly (...) that the company is unable to unlock iPhones or iPads for*

88 For example, in the Silk Road case, the FBI meticulously planned the arrest of Ross Ulbricht to make sure his computer remained turned on after seizure to prevent encryption and perform live forensics. See Joshuah Bearman, 'Silk Road: The Untold Story', *Wired*, 23 May 2015. Available at: http://www.wired.com/2015/05/silk-road-untold-story/ (last visited 30 September 2015).

89 Mevis, Verbaan & Salverda (2016, p. 58) state that over half of the respondents in their interviews indicate that encryption in storage 'regularly' imposes a challenge in their criminal investigations (with regard to all types of crimes in the Netherlands).

90 Technically, the standard encryption measures on iPhones work differently than full disk encryption. However, they are comparable and the security measure poses law enforcement authorities the same problem.

police".[91] The standard device encryption on modern iPhones is an ongoing problem for law enforcement authorities at the time of writing (October 2016).[92] Full disk encryption on a computer and standard device encryption may therefore leave law enforcement authorities unable to analyse data on a seized computer if they do not obtain the encryption key in order to decrypt the data on the computer (cf. Casey et al. 2011).[93]

B Encryption of files stored in the cloud

Cloud computing enables people to log in to a web portal and make use of electronic communication services and online storage services.[94] Law enforcement officials seeking information that is made available through these web portals cannot obtain the information by seizing a computer and analysing the information stored on it. Instead, the information is sent back and forth by the online service providers and is processed on the servers in data centres of online service providers. Law enforcement officials can possibly intercept the data in transit. However, as already stated above, the challenge of encryption in transit makes it impossible under certain circumstances for law enforcement officials to read the contents of network traffic.[95]

---

91 Craig Timberg and Greg Miller, 'FBI blasts Apple, Google for locking police out of phones', The Washington Post, 25 September 2014. Available at: http://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html (last visited on 25 September 2014). However, note that the user must utilise a strong password and not the 4-digit passcode as a security measure. It is straightforward to crack a 4-digit passcode. See the analysis of Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited 18 August 2015).

92 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 (last visited on 18 April 2016).

93 In certain circumstances and on certain computers, law enforcement officials can perform 'live forensics'. In the process of live forensics, volatile information is captured from physical memory on a computer system (cf. Adelstein 2006, p. 64). That volatile information may include an encryption key, which can be used to decrypt the data stored on a computer system. Therefore, live forensics may be a solution for full disk encryption or partial encryption of disks (cf. Casey 2011 et al. p. 132, Bryant et al. 2008, p. 105-110, and Koops et al. 2012b, p. 46).

94 Cloud computing has been defined as *"a model for enabling convenient on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"* (Mell & Grance 2009). This is the definition used by the U.S. National Institute of Standards and Technology (NIST). For this study only cloud computing techniques relating to Software as a Service (SaaS) are considered. SaaS is software provided by a third party provider running on a cloud infrastructure. Available on demand and accessible from various devices through an interface, such as a web browser or App. Examples of SaaS are web based email services, online word processing tools and web content delivery services.

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

The manual encryption in storage of files 'in the cloud' appears to be a major challenge for law enforcement authorities. In this case, a user encrypts files before uploading them to the servers of cloud providers (cf. Colarusso 2011, p. 92-93). These files are unreadable by law enforcement officials, even when they collect the files from third party providers through data production orders.

2.4.3 Overcoming the challenges of encryption

The challenges of encryption in transit and encryption in storage make it more difficult for law enforcement officials to read the content of intercepted network traffic and analyse data after the seizure of a computer.

However, law enforcement officials can use digital investigative methods to overcome these challenges and gather evidence. The investigative methods of (A) data production orders that are issued to online service providers and (B) hacking as an investigative method, can be used to overcome the challenges of encryption in transit and encryption in storage. These digital investigative methods are further examined below.

A Data production orders issued to online service providers

As explained in subsection 2.2.2 under B, data production orders enable law enforcement officials to obtain data from online service providers. Thus, companies that provide online storage services can also be forced to hand over decrypted data to law enforcement officials when they are issued with a data production order. Online service providers are often able to decrypt data themselves (1) for advertisement purposes, (2) in case a customer forgets his password, and (3) for security purposes and for law enforcement purposes (cf. Soghoian 2010, p. 52 and 70-71).[96]

Therefore, even though an individual may have enabled full disk encryption on a computer, law enforcement officials may be able to collect a copy of that data from an online service provider. For example, if an iPhone is encrypted and law enforcement seeks to obtain information stored on it, they may be able to obtain the information by issuing a data production order to Apple in order to collect a backup copy of the contents of an

96 For example, Apple can decrypt information from their customers and law enforcement authorities. See Apple iCloud's Terms and Conditions: *"You acknowledge and agree that Apple may, without liability to you, access, use, preserve and/or disclose your Account information and Content to law enforcement authorities, government officials, and/or a third party, as Apple believes is reasonably necessary or appropriate, if legally required to do so or if Apple has a good faith belief that such access, use, disclosure, or preservation is reasonably necessary to: (a) comply with legal process or request; (b)* (...) *or (d) protect the rights, property or safety of Apple, its users, a third party, or the public as required or permitted by law."* Available at http://www.apple.com/legal/icloud/en/terms.html (last visited 20 October 2016).

iPhone.[97] Swire predicts that the challenges of encryption will drive law enforcement authorities to issue more data production orders to online service providers (cf. Swire 2012).[98]

B Performing hacking as an investigative method

Law enforcement officials can also gain remote access to computers to overcome the challenges of encryption in transit and encryption in storage. In this study, the investigative activity in which law enforcement officials can gain remote access to computers is called 'performing hacking as an investigative method'. Hacking as an investigative method can be best described as an umbrella term, which encompasses different investigative methods that have in common that law enforcement officials remotely obtain access to a computer system (cf. Oerlemans 2011, p. 891).

Hacking is distinguished in this study as an investigative method which appears in the following three forms: (B.1) network searches, (B.2) remote searches, and (B.3) the use of policeware (cf. Oerlemans 2011 and Conings & Oerlemans 2013). These three types of hacking are further examined below.

B.1 Network searches

A network search is an investigative method that takes place during a search at a particular place (in the physical world). During a network search, law enforcement officials gain remote access to an interconnected computer that is connected to a computer that has been previously seized (for instance, during a search of a residence). As part of a network search, law enforcement officials can then examine an external hard drive or media player that is part of the same (internal) network.

A network search can enable law enforcement officials to deal with the challenge of encryption in storage by accessing remotely stored information through an interconnecting computer. A network search is considered as a type of hacking as an investigative method, because law enforcement officials can gain remote access to a computer system (of which the suspect is not necessarily aware). For instance, remotely stored information may be accessible through an online account that can be accessed with obtained log-

97 Law enforcement officials may be able to obtain data that is backed-up by Apple's iCloud service. See C. Foresman, 'Apple holds the master decryption key when it comes to iCloud security, privacy', *Ars Technica* 2012. Available at: http://arstechnica.com/apple/2012/04/apple-holds-the-master-key-when-it-comes-to-icloud-security-privacy/. See also Nicolas Weaver in the article of Paul Rosenzweig, 'iPhones, the FBI, and Going Dark', 4 August 2015. Available at: https://www.lawfareblog.com/iphones-fbi-and-going-dark (last visited 18 August 2015).

98 However, note that, law enforcement officials may not be able to acquire the data within an acceptable time frame due to unacceptable delays in mutual legal assistance procedures (cf. NIST 2014, p. 7). See also *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 9. See section 2.5 for further analysis with regard to the challenge of jurisdiction cybercrime investigations.

in credentials.[99] Using a network search, law enforcement officials can gain access to online accounts of individuals through a running seized computer (cf. Conings & Oerlemans 2013).[100] The prevalence of 'apps' on smartphones with accompanying login credentials make it possible for law enforcement officials to use those credentials and collect evidence that can be accessed through programs located on a seized computer that is connected to the Internet.

B.2 Remote searches

The investigative method of a remote search refers to an evidence-gathering activity in which law enforcement officials remotely access a computer and search the data that is stored on it (cf. Brenner 2012).

Remote searches may enable law enforcement officials to deal with the challenge of encryption in storage in criminal investigations. By using the proper investigative method, law enforcement officials can gain remote access to a computer that a suspect uses. After remote access is obtained, law enforcement officials can take screen shots of the computer, write down a report of the evidence-gathering activities, or even copy relevant data for evidence-gathering purposes (cf. Oerlemans 2011, p. 892). In this manner, law enforcement officials can avoid seizing a computer during a search and can analyse a computer before the data stored on a computer is encrypted.

B.3 The use of policeware

Law enforcement officials can overcome the challenge of encryption in transit by intercepting communications of an individual 'at the source', i.e., the computer itself, before encryption in transit is enabled for communications (cf. Abate 2011, p. 124).[101] This can be made possible by using 'computer monitoring software', which is called 'policeware' in this study.[102] To use policeware, law enforcement officials must remotely gain access to a computer and install the software. The software may enable law enforcement officials to log the suspect's keystrokes. Thereafter, the officials can remotely

99 Law enforcement officials can obtain login credentials from programs at the seized computer or from cookies to access certain web services. Login credentials can also be obtained through informants or voluntarily provided by a suspect.

100 See also the discussion document regarding the search and seizure of devices (6 June 2014), p. 52-53. Available at: https://www.rijksoverheid.nl/documenten/publicaties/2014/06/06/herziening-van-het-wetboek-van-strafvordering (last visited February 2016). The Dutch legislator indicates that Dutch law enforcement officials can log in to a server of Gmail or Dropbox to access e-mails and documents stored 'in the cloud'.

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

102 Jacobs (2012) first used the term 'policeware' in literature.

turn on the computer's microphone.[103] Subsequently, the recorded data is sent to law enforcement officials. The use of policeware enables law enforcement officials to intercept communications in criminal investigations.[104]

Law enforcement officials can also overcome the challenge of encryption in storage using policeware. With the ability to intercept keystrokes of a computer user, law enforcement officials can collect individuals' passwords and login credentials (cf. Fox 2007, p. 828). Passwords that are logged by a keylogging functionality of policeware can be used to decrypt a hard disc or files of an individual (cf. Oerlemans 2011, p. 905-907). Policeware can also create a 'back door' to computers for law enforcement authorities to remotely access a computer. As noted above (under B.2), law enforcement officials can then look at the computer screen through the eyes of a suspect by taking screenshots. After remote access has been obtained to a computer of a suspect, law enforcement officials can copy data that they deem relevant to an investigation. For this reason, the use of policeware can take place prior and in conjunction with the investigative method of a remote search.

Finally, it should be noted here that policeware can also be used to overcome the challenge of anonymity in cybercrime investigations. Once law enforcement officials gained remote access to a computer and installed the software, the software can be directed to send law enforcement officials the originating (public) IP address of the computer and other identification information.[105] The FBI reportedly makes use of policeware with specifically these functionalities.[106] In the last decade, the use of policeware enabled

103 Commercially available software for law enforcement authorities reportedly have these capabilities. See, e.g., Morgan Marquis-Boire, 'From Bahrain With Love: FinFisher's Spy Kit Exposed?', *Citizen Lab*, 25 July 2012. Available at: https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (last visited on 10 July 2014), Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, 'Mapping Hacking Team's "Untraceable" Spyware', *Citizen Lab*, 17 February 2014.

104 Commercial policeware vendors reportedly advertise this kind of software with the following description: "*A stealth, spyware-based system for attacking, infecting and monitoring computers and smartphones. Full intelligence on target users even for encrypted communications (Skype, PGP, secure web mail, etc.)*" (Bill Marczak, Claudio Guarnieri, Morgan Marquis-Boire, and John Scott-Railton, 'Mapping Hacking Team's "Untraceable" Spyware', *Citizen Lab*, 17 February 2014 with reference to http://wikileaks.org/spyfiles/files/0/31_200810-ISS-PRG-HACKINGTEAM.pdf (last visited on 10 July 2014).

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

106 Reportedly, software is available that provides U.S. law enforcement with the following information: (a) the IP address of the computer, (b) MAC address, (c) a list of open TCP and UDP ports, (d) a list of running programs, (e) operation system information, (f) default internet browser and version, (g) registered user of the operation system, (h) currently logged in user, and (i) last visited URL. See Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 July 2007. Available at: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware (last visited on 30 December 2014). The information is obtained through data access requests to U.S. governmental agencies.

them to identify individuals that made anonymous bomb threats through webmail in the United States.[107]

2.5 The challenge of jurisdiction

From section 2.2 to section 2.4, it has been explained how law enforcement officials can gather evidence in cybercrime investigations, even when the technical challenges of anonymity and encryption arise. However, even though law enforcement officials may be technically able to gather the evidence in a cybercrime investigation, they can still face legal challenges. In this section, the legal challenge of jurisdiction is further examined. It also identifies the approach that law enforcement officials use to overcome this challenge in cybercrime investigations.

This section examines the legal challenge of jurisdiction. The examination is started by providing a brief description of the concept of enforcement jurisdiction in subsection 2.5.1. Then, the mechanism of mutual legal assistance to obtain evidence located on foreign territory is examined in subsection 2.5.2. Subsequently, the limits of mutual legal assistance as a mechanism for extraterritorial evidence-gathering activities in cybercrime investigations are addressed in subsection 2.5.3. Finally, the way law enforcement officials overcome the challenge of jurisdiction is examined in subsection 2.5.4.

2.5.1 Enforcement jurisdiction

The term 'jurisdiction' describes the limits of the legal competence of a State or a different regulatory authority to make, apply, and enforce rules of conduct upon persons (see Lowe 2006, p. 335 in: Evans 2006). In European criminal law, the 'jurisdiction' of a State is split into (1) the capacity to make and apply law (*jurisdiction to prescribe*) and (2) the capacity to ensure compliance with such laws through executive, administrative, police or other non-judicial action (*jurisdiction to enforce)*.[108] This study focuses on the jurisdiction to enforce.

---

107 See, e.g., Kevin Poulsen, 'FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats', *Wired*, 18 July 2007. Available at: http://archive.wired.com/politics/law/news/2007/07/fbi_spyware and Kevin Poulson, 'Documents: FBI Spyware Has Been Snaring Extortionists, Hackers for Years', *Wired*, 16 April 2009. Available at: http://www.wired.com/2009/04/fbi-spyware-pro/ (last visited on 30 December 2014).

108 See, e.g., Mann 1984, O'Keefe 2004, p. 737-738, Lowe in: Evans (ed.) 2003, p. 329, and Shaw 2008, p, 645-646. In U.S. criminal law, a third category of 'adjudicative jurisdiction' is distinguished, which refers to a sovereign's authority to have its courts determine whether a particular law was violated (see Restatement (Third) of Foreign Relations Laws of the United States par 401(a)-(c) (1987)). However in practice, courts decide whether a person is guilty of criminal behaviour by applying its national criminal laws and thus prescriptive jurisdiction and adjudicative jurisdiction collapse into one (cf. Akehurst 1974, p. 179, O'Keefe 2004, p. 737-738, and Kohl 2007, p. 16).

The jurisdiction to enforce is territorially limited. The common view is that States can investigate crimes on their territory on their own terms, as part as the execution of their sovereign rights. This strict territorial limitation of the jurisdiction to enforce has been explicitly made clear by the Permanent Court of Justice in 1927.[109] In the landmark case of *Lotus v. Turkey*, the Permanent Court of Justice stated that:

"The first and foremost restriction imposed by international law upon a State is that – failing existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention".[110]

Thus, law enforcement officials cannot mount an investigation on foreign territory without ad hoc permission or a treaty.[111] Crawford (2012, p. 479) aptly describes the territorial restriction of enforcement jurisdiction as follows:

"Persons may not be arrested, a summons may not be served, police or tax investigations may not be mounted, order for production of documents may not be executed, except under the terms of a treaty or other consent given."

When law enforcement officials unilaterally gather evidence on foreign territory without the permission of the affected State and without a treaty basis that authorises the evidence-gathering activity, their behaviour infringes upon the following three principles of international law: (1) sovereignty, (2) equality of States, and (3) the principle of non-intervention (cf. Shaw 2008, p. 645). These three principles are briefly discussed below.

(1) *Sovereignty*. Sovereignty refers to a State's privilege to exercising power over its territory (cf. Stigall 2012, p. 328).[112] As part of its territorial sovereignty, States regulate the use of governmental power in relation to investigative methods that are utilised over individuals on their own territory.[113] The manner in which a State regulates the evidence-gathering activities of law enforcement officials within its territorial borders falls within the exercise of its sovereign rights (cf. UNODC 2013, p. 184). Therefore, when foreign law enforcement authorities wield their power over citizens of another State, it infringes on the sovereignty of the State in which those citizens live.

109 PCIJ, SS Lotus (France v. Turkey), 1927, *PCIJ Reports*, Series A, No. 10.
110 PCIJ, SS Lotus (France v. Turkey), 1927, *PCIJ Reports*, Series A, No. 10, p. 18-19.
111 See also, e.g., Reijntjes, Mos & Sjöcrona, p. 257 in: Van Sliedregt, Sjöcrona & Orie 2008.
112 Referring to Cassese 2005, p. 49.
113 However, note that fundamental human rights and international treaties restrict the exercise State power over individuals on its territory (cf. Gill 2013, p. 221 in: Ziolkowlski 2013).

(2) *Equality of States*. The principle of the legal equality of States implies that, formally speaking, all members of the international community are on the same footing (see Cassese 2005, p. 52). Whatever their size or power, States have a duty to not intervene in the internal affairs of other States.
(3) *Principle of non-intervention.* The duty not to intervene in the internal affairs of other States is called the principle of non-intervention (cf. Shaw 2008, p. 212).[114] Together with the principle of sovereign equality, the principle of non-intervention is designed to ensure that each State respects the fundamental prerogatives of other members of the community (cf. Cassese 2005, p. 53).

These three principles are considered as the 'cornerstones of international law' (cf. Ryngaert 2007, p. 40). Ultimately, these principles are essential to maintaining a reasonably stable system of competing States (cf. Shaw 2008, p. 213). As Shaw explains: *"setting limits on the powers of States vis-à-vis other states contributes to some extent to a degree of stability within the legal order"* (Shaw 2008, p. 213). States that gather evidence on the territory of another State, without permission or consent derived from a treaty, can enter into conflict. The reason is that these extraterritorial evidence-gathering activities can be perceived as an infringement of the territorial sovereignty of the other State. The extraterritorial enforcement of jurisdiction is therefore only possible with permission of the affected State or based on a treaty (see Mann 1964, p. 44-49).

As a consequence of the territorial sovereignty of a State, States have (a) local criminal laws that specify which behaviours are considered as 'cybercrimes', (b) local authorities who investigate cybercrimes under local laws that stipulate the scope of the instruments that can be used to investigate crime, and (c) local authorities that prosecute cybercrime in local courts.

In cybercrime investigations, law enforcement officials are often required to gather evidence on foreign territory and prosecute foreign individuals (cf. UNODC 2013, p. 119). Therefore, it should be observed that the investigation and prosecution of cybercrime take place *locally* and are limited by the physical borders of a State, whereas cybercrimes themselves are often *cross-border* in nature (cf. Brenner & Schwerha IV 2002, p. 395).

Of course, States have developed a mechanism to collect evidence on foreign territory without infringing on the territorial sovereignty of the State in which the evidence is located. That mechanism is known as mutual legal assistance and is further analysed in the subsection below.

114 The principle of non-intervention in international law is also reflected in the U.N. General Assembly's Declaration on Principles of International Law Concerning Friendly Relations and Cooperation, which states: *"No State or group of States has the right to intervene, directly or indirectly, for any reason whatever, in the internal or external affairs of any other State"* (general assembly of 24 October 1970, 25th session, A/RES/25/2625) (cf. Stigall 2012, p. 336). See also art. 2(7) of the Charter of the United Nations.

2.5.2 Mutual legal assistance

Mutual legal assistance is the formal procedure by which states request and obtain evidence on foreign territory.[115] States can agree on the conditions under which evidence can be gathered on their territory upon request by local law enforcement authorities or even unilaterally by foreign law enforcement officials under supervision of local law enforcement authorities. The conditions in which mutual legal assistance is provided to other law enforcement authorities can be agreed upon in treaties.

Below, the Convention on Cybercrime (under A) and the Treaty of Lisbon (under B) are briefly examined in order to illustrate how mutual legal assistance mechanisms work in the context of cybercrime investigations.

A Convention on Cybercrime

The Convention on Cybercrime is the most important multilateral treaty in cross-border cybercrime investigations.[116] The convention is particularly important for the following three reasons.

(1) *Harmonisation of criminal substantive law with regard to cybercrime*. Harmonisation of criminal substantive law facilitates mutual legal assistance, because States will criminalise harmful behaviours in a similar manner. In that case, it is easier for States to agree on mutual legal assistance to gather evidence from other States and to extradite individuals.

(2) *The obligation to regulate certain investigative powers in a domestic legal framework*. The regulation of investigative powers is important, because they provide the practical tools for law enforcement authorities to investigate cybercrimes.

115 Notably, mutual legal assistance also entails (1) the exchange of information ('intelligence') between law enforcement authorities, (2) the transfer of criminal proceedings, and (3) the extradition of suspects. This study focuses on the evidence-gathering activities in criminal investigation by law enforcement authorities using investigative methods in cybercrime investigations. As a consequence, informal cooperation between law enforcement authorities is also not considered. Law enforcement officials in the Netherlands do not have the authority to gather evidence with investigative methods and exchange evidence with their foreign counterparts without permission of the formal authority (usually a public prosecutor), even when law enforcement authorities have the authority to gather evidence themselves. Although some authors question whether public prosecutors are able to practically supervise the exchange of evidence under informal constellations between law enforcement authorities, it is clear that – in theory -only a model of formal mutual legal assistance for evidence gathering on foreign territory applies in the Netherlands (see Reijntjes, Mos & Sjöcrona, p. 263 in: Van Sliedregt, Sjöcrona & Orie 2008 and Vander Beken 1999, p. 341). See more generally with regard to police cooperation, the exchange of intelligence, and the international criminal law framework, e.g., Bassiouni 2008, p. 19-21.

116 See for an extensive analysis of the Convention on Cybercrime, e.g., Kaspersen, p. 156-172 and 175-180 in: Koops 2007 and Oerlemans 2016, in: Verrest and Paridaens 2016.

(3) *The creation of a system for swift international cooperation*. The Convention on Cybercrime obliges member states to create a contact point to ensure the provision of immediate mutual legal assistance for cybercrime investigations.[117] The contact point must be available twenty-four hours a day, seven days a week. The contact point ensures that the assigned law enforcement authority within a member state is able to coordinate mutual legal assistance proceedings with other law enforcement authorities. The idea is to make mutual legal assistance procedures in cybercrime investigations more efficient.

However, two States that are crucial to cybercrime investigations, Russia and China, did not ratify the Convention on Cybercrime. Therefore, these States (1) may have regulated cybercrimes in a completely different manner, (2) have not necessarily implemented the mentioned investigative powers in their domestic legal frameworks, and (3) do not have a contact point that is obliged to cooperate with foreign law enforcement authorities that ratified the convention. This may frustrate international cybercrime investigations.

In addition to the Convention on Cybercrime, many other multilateral treaties aim to harmonise criminal substantive laws with regard to cybercrimes.[118] However, those other treaties do not harmonise investigative methods for evidence-gathering purposes.[119] So far, efforts to provide for a global (UN) treaty to harmonise cybercrimes and provide for a more effective mechanism to gather evidence in criminal investigations involving cybercrime have failed.[120] Apparently, the majority of States are unwilling to give up part of their territorial sovereignty to regulate the ways in which evidence can be collected in cybercrime cases.

117 See art. 35 of the Convention on Cybercrime.

118 See UNODC 2013, p. 63-76 for an overview of treaties with regard to cybercrime. Five regional or international clusters that developed treaties can be identified which are the (1) Council of Europe or the European Union, (2) the Commonwealth of Independent States or the Shanghai Cooperation Organization, (3) intergovernmental African organizations, (4) the League of Arab States, and (5) the United Nations (UNODC 2013, p. 63).

119 See extensively, e.g., UNODC 2013, p. 63-71.

120 See 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 25 February 2015). See also Stein Schjølberg and Solange Ghernaouti-Helie, 'A Global Treaty on Cybersecurity and Cybercrime', 2nd ed., 2011.

B Treaty of Lisbon

The Treaty of Lisbon is of great significance to evidence-gathering activities within the European Union.[121] Since the ratification of the Treaty of Lisbon in 2007, the legislative authorities of the European Union are authorised to impose binding rules on evidence-gathering activities in criminal matters (cf. Summers et al. 2014, p. 46).[122]

However, at this time (October 2016), there is (1) no EU law enforcement authority, (2) no EU prosecution authority, and (3) no EU court with jurisdiction to try individuals who violate EU criminal law (cf. Summers et al. 2014, p. 272). Currently, there are 28 different national criminal procedural codes in the European Union that regulate evidence-gathering activities by law enforcement officials in criminal investigations in their own manner.[123] As a result, in international criminal investigations, the criminal procedural laws of the individual member states dictate how evidence must be obtained from each territory, unless specific treaty provisions apply. Not surprisingly, strict formalities and lengthy mutual legal assistance procedures often plague cooperation between States in the EU (cf. Cryer et al. 2010, p. 88).

The EU instrument of 'mutual recognition' aims to change the traditional principle that the local laws of the 'requested State' stipulate under which conditions evidence is gathered ('*locus regit actum*'). Mutual recognition means that States within the EU must recognise each other's judicial systems and must immediately execute mutual legal assistance requests under the criminal procedural laws of the issuing (EU Member) State with a minimum of formality and exceptions (cf. Bantekas 2007). Most notably, the 'European Investigation Order' is a mutual legal assistance instrument that ensures that an 'issuing State' can collect evidence with co-operation of the 'executing State' under the formalities and procedures expressly indicated

121 Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon on 13 December 2007, entered into force on 1 December 2009, OJ C306.

122 Criminal law and criminal procedural law can be harmonised upon the basis of art. 82 of the Treaty on the Functioning of the European Union (TFEU). The EU has the explicit competence to harmonise computer crime between Member States in art. 83(1) TFEU (see Summers et al. 2014, p. 233). However, note that a legal procedure was created in art. 83(3) TFEU called the 'emergency break procedure', which allows member states to protest against legislation that would affect fundamental aspects of their criminal justice system (see for a more extensive analysis, e.g., Klip 2012, p. 36 and Summers et al. 2014, p. 46-78). The United Kingdom, Ireland and Denmark made reservations to the applicable EU treaties on mutual legal assistance in criminal investigations and do not take part in all treaties (see Mitsilegas 2009, p. 53-56).

123 Following the referendum in the United Kingdom on 24 June 2016, a majority of the British people voted to leave the EU. It is possible the United Kingdom will soon leave the EU. See also Jennifer Rankin, Jon Henley, Philip Oltermann, and Helena Smith, 'EU leaders call for UK to leave as soon as possible', *The Guardian*, 24 June 2016. Available at: http://www.theguardian.com/politics/2016/jun/24/europe-plunged-crisis-britain-votes-leave-eu-european-union (last visited on 26 June 2016).

by the issuing State.[124] Overall, the European Investigation Order has the potential for a more efficient means to gather evidence in criminal investigations.[125]

However, even when the European Investigation Order is used, local law enforcement officials within a particular State gather the evidence.[126] Thus, the law enforcement officials of the investigating State still depend on the cooperation of law enforcement officials in the requested State. Currently, there is no broader vision in the European Union to fight crime under harmonised criminal procedural rules (cf. Klip 2012, p. 473). Summers et al. (2014, p. 283) observe: *"there is a clear and overt resistance among Member States to further communitarisation"*.[127] This becomes apparent in the manner the EU seeks to combat cybercrime. The EU Directive 2013/40/EU concerning 'attacks against information systems' harmonised criminal substantive law in relation to target cybercrimes and established mandatory minimum penalties for these crimes.[128] However, the directive does not harmonise criminal procedural law, which may facilitate evidence-gathering activities in cybercrime investigations. Harmonisation of criminal procedural law within the EU to combat cybercrime is also not expected in the near future.

---

124 See the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal Matters, (OJ L 130/1). The European Investigation Orders also applies to 'computer related offences' (see Appendix D of the Directive). Not all cross-border evidence-gathering activities fall under the Directive. Recital 24 notes that additional rules are necessary for (a) the temporary transfer of persons held in custody, (b) hearing by video or telephone conference, (c) obtaining of information related to bank accounts or banking transactions, (d) controlled deliveries, and (e) covert investigations. The European Investigation Order also does not apply to the investigative methods of wiretapping and the data production orders issued to electronic communication service providers (cf. Van Daele 2012, p. 219-220). Moreover, there are grounds for States to refuse the European Investigation Order. The most important exceptions are stipulated in art. 9(2), art. 9(5) and art. 11 of Directive 2014/41/EU.

125 At the same time, the European Investigation Order is strongly criticised by legal scholars. See for, example, Ruggeri (in: Ruggeri 2014, p. 3) who argues that there is no proper balance between the efficiency of prosecution and the protection of human rights of the individuals involved. See also: Raad voor de Rechtspraak, 'Wetsvoorstel Europees onderzoeksbevel biedt onvoldoende bescherming', 5 November 2015. Available at: https://www.rechtspraak.nl/Organisatie/Raad-Voor-De-Rechtspraak/Nieuws/Pages/Wetsvoorstel-Europees-onderzoeksbevel-biedt-onvoldoende-bescherming.aspx (last visited 9 November 2015).

126 Note that even when law enforcement authorities of the issuing State are present on the territory of the other State, the authorities: *"shall be bound by the law of the executing State during the execution of the EIO. They shall not have any law enforcement powers in the territory of the executing State, unless the execution of such powers in the territory of the executing State is in accordance with the law of the executing State and to the extent agreed between the issuing authority and the executing authority."* (art. 9(5)).

127 Referring to Mitsilegas 2009.

128 See EU Directive 2013/40/EU about 'attacks against information systems' (2013/40/EU (L218/8) of 14 August 2013. The Directive also forces member states to respond to mutual legal assistance requests within eight hours and to indicate whether the request will be answered and the form and estimated time of the answer. See for a more extensive analysis of EU criminal law and cybercrime, e.g., Summers et al. 2014, p. 231-254.

2.5.3 Limits of mutual legal assistance

Mutual legal assistance, as a mechanism to obtain evidence on foreign territory, has two important limitations. The first limitation is that mutual legal assistance is only available insofar States are able to agree upon the conditions for extraterritorial evidence gathering. Law enforcement officials are completely dependent on the willingness of local law enforcement authorities to cooperate when no treaty can be negotiated. The second limitation is that mutual legal assistance procedures can be burdensome for law enforcement authorities, especially in cybercrime investigations (cf. Prins 2012, p. 49). In other words, mutual legal assistance procedures can take too much time for law enforcement officials.

Mutual legal assistance procedures can become significantly more burdensome when suspects make use of anonymising services to change the visible IP address. This enhanced jurisdictional challenge is illustrated in Figure 2.6.

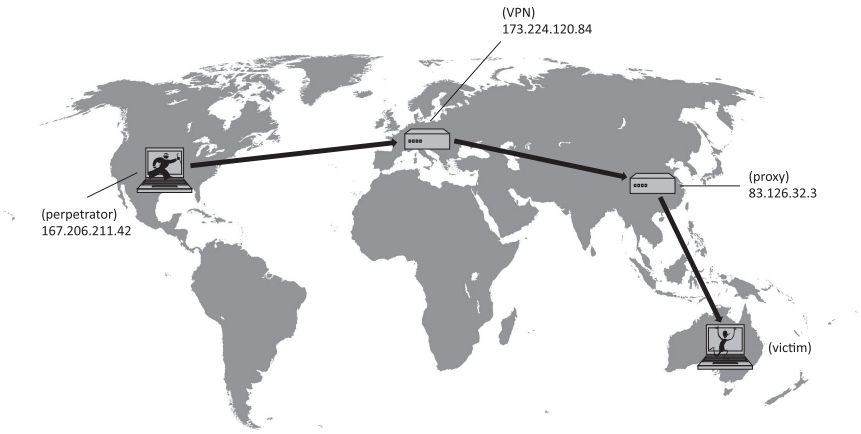

Figure 2.6: Illustration of the global nature of cybercrime and the jurisdiction challenge in cybercrime investigations.

Figure 2.6 illustrates a criminal in the United States using a VPN server in Germany and a proxy server in China to obscure his IP address and commit a crime in Australia. In that case, law enforcement officials in Australia have to use mutual legal assistance procedures to collect evidence from a proxy-service providers and VPN-service providers in order to follow up on the digital lead of an IP address. Following Figure 2.6, in order trace back the suspect, law enforcement officials require subscriber data from (1) a proxy provider in China, (2) a VPN provider in Germany, and (3) an internet access provider in the United States. Thus, evidence must be obtained from online service providers in each successive jurisdiction through which the communication passes (cf. Sussmann 1999, p. 468). As explained in subsection 2.3.2, a proxy service and VPN service may provide an additional link in the chain

to trace back the address of an internet user. Tracing back the originating IP address of a computer therefore requires a considerable amount of time.

To conclude, gathering of evidence in cross-border cybercrime investigations through the mutual legal assistance model can be burdensome (even between Member States of the European Union). When cybercriminals make use of anonymising services, it can be even more difficult to obtain evidence by use of mutual legal assistance procedures. In situations where the requested state is unwilling or unable to afford mutual legal assistance, law enforcement officials are left empty handed (cf. Stigall 2013, p. 23). To be direct: current mutual legal assistance mechanisms seem to be unable to meet the investigative and prosecutorial challenges of cybercrime investigations (cf. UNODC 2013, p. 214 and Koops & Goodwin 2014, p. 41).[129]

2.5.4 Overcoming the challenge of jurisdiction

Law enforcement officials can overcome the challenge of jurisdiction in cybercrime investigation by gathering evidence across State borders. The Internet can facilitate evidence-gathering activities that may take place on foreign territory, while investigators are still within the territorial borders of the investigating State (cf. Siemerink 2000c, p. 240). Thus, digital investigative methods can be applied within the territorial borders of the investigating State and produce effects outside the investigating State territorial borders at the same time. For instance, law enforcement officials can chat with an individual on foreign territory to gather evidence in a domestic criminal investigation.

Practically, no mutual legal assistance is required to gather the evidence. Therefore, cross-border unilateral evidence-gathering activities that are facilitated by the Internet can be regarded as a manner of overcoming the challenge of jurisdiction in cybercrime investigations. Law enforcement officials may be inclined to succumb to unilateral action when there are no mutual legal assistance treaties in place or the data cannot be acquired within a reasonable time frame (cf. NIST 2014, p. 7). The following Dutch case is illustrative for this situation. In 2008, a Dutch public prosecutor instructed a law enforcement official to log in to a Hotmail account, using login credentials that were provided by an informant.[130] The public prosecutor was of the opinion that it would take too much time to obtain the documents from Microsoft (offering the webmail service 'Hotmail').[131] In the view of the public prosecutor, the circumstances of the case required immediate action, because law enforcement officials expected to find the details about a large delivery of cocaine in the port of Rotterdam in the Netherlands in

129 See also See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 2015/16, 34 372, no. 3 (explanatory memorandum Computer Crime Act III), p. 49.

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

131 The webmail service 'Hotmail' has been recently rebranded by Microsoft as 'Outlook mail'.

the Hotmail account. After the law enforcement officials gained access to the incriminating e-mails in the Hotmail account, the information in those e-mails indeed led to the seizure of cocaine stored in a ship in the port of Rotterdam.[132]

However, theoretically, law enforcement officials can infringe on the territorial sovereignty of a State when their investigative activities produce extraterritorial effects. As extensively explained in subsection 2.5.1, extraterritorial investigations of law enforcement officials without permission or consent derived from a treaty basis with the affected State are not allowed by international law.

New regime in international law?

To solve this problem, one option is to create a completely new legal regime in international law in order to allow the application of extraterritorial investigative techniques by use of digital investigative methods. In the early 1990s, certain legal scholars submitted that "cyberspace" is a distinct "place", which is not subject to the traditional notions in law.[133] In addition, more recently, legal scholars suggested that a new legal regime in international law should be applicable to cyberspace. Inspired by the special legal regime for outer space or the high seas, some scholars suggested that a similar legal regime should apply to cyberspace.[134] Other scholars suggested that cyberspace should be viewed as a 'global commons' that should be regulated by global treaties.[135]

These suggestions for an alternative legal regime in international law for cyberspace have not taken root (cf. Pirker 2013, p. 195 in: Ziolkowski 2013 and Koops & Goodwin 2014, p. 67). States have consistently applied their territorially based rules to behaviours of individuals that are facilitated by the Internet, refusing to treat the Internet as a 'separate place' with different rules (cf. Kohl 2007, p. 11, Pirker 2013, p. 194 in: Ziolkowski 2013 and Koops & Goodwin 2014, p. 21). In other words, the legal world is still very much

132 See the facts of the case described in Rb. Rotterdam, 26 March 2010, ECLI:NL:RBROT:2010:BM2520. Interestingly, there are no other published judgements available in the Netherlands, which indicate that law enforcement authorities gained remote access to the contents of webmail services. Perhaps this case turned up the surface, because the public prosecutor in question specifically requested the judge to decide whether the investigative method was a legitimate investigative power.

133 See most notably, Johnson and Post, whom argued that the Internet undermined the feasibility – and legitimacy – of laws based on geographical boundaries (Johnson & Post 1996, p. 1378). This notion has been nicely described by John Perry Barlow in the first paragraph of his 'Declaration of Cyberspace', written on 8 February 1996: "*Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.*" Available at https://projects.eff.org/~barlow/Declaration-Final.html (last visited 1 March 2015).

134 See, e.g., Franzese 2009, Stahl 2011 and Hildebrandt 2013.

135 See, e.g., Lukasik 2000. See Koops & Goodwin (2014, p. 67-77) for an overview and analysis of alternative legal regimes of international law for 'cyberspace'.

divided into territorial borders of sovereign States (see, e.g., Van Staden & Vollaard 2002, p. 183 in: Kreijen et al. 2002 and Stigall 2013, p. 9).

To conclude, investigative activities that take place on the Internet are subjected to the normal rules of international law on the exercise of jurisdiction (cf. Pirker 2013, p. 196 in: Ziolkowski 2013). Thus, the investigative activities of law enforcement officials in cybercrime investigations are restricted by the territorial limitation of enforcement power. At the same time, this study holds a realistic view of the application of investigative methods to cybercrime investigations. States continue to apply their rules to behaviours that take place on the Internet, but this does not negate the fact that the Internet is a borderless medium that does not take territorial borders into account.

Disparity of the legally divided world and online investigations

Currently, there is a disparity between the *theory* of a world that is legally divided by the territorial borders of sovereign States and the *reality* of an interconnected world in which law enforcement officials can virtually cross State borders.[136] In 1998, the Dutch legislature observed that the possibility of cross-border unilateral online investigations may be in conflict with the territorial sovereignty of other States.[137] According to the Dutch legislature, further research was required into how to deal with this legal issue.[138] However, very little research has been performed with regard to the question of the applicability and desirable territorial limits of these online investigations.[139]

The cross-border unilateral application of digital investigative methods and the tension that this approach poses to the principle of the territorial limitation of enforcement jurisdiction is further examined in chapter 9.

2.6 Chapter conclusion

The aim of this chapter is to determine which digital investigative methods are commonly used in cybercrime investigations (RQ 1). To answer RQ 1, a three-step approach was taken. In step one, the object of the criminal investigation, cybercrime, was examined. In step two, the two digital leads that law enforcement officials often follow in cybercrime investigations and the

136 See also Koops & Goodwin 2014, p. 78 who observe: *"In our research, we are struck by the lack of understanding with cyber-investigation experts of basic principles and developments of international law as well as by the lack of understanding with international law experts of basic principles and developments of cyber-investigation"*.

137 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1997/98, 25 880, no. 1, p. 81

138 See *Kamerstukken II* (Parliamentary Proceedings Second Chamber) 1999/2000, 25 880, no. 10, p. 24.

139 With the notable exceptions of the article of Siemerink in 2000(c) and the report of Koops & Goodwin in 2014.

accompanying evidence-gathering activities were examined. In step three, the three challenges in cybercrime investigations and the digital investigative methods used to overcome these challenges were analysed.

Step one was addressed in section 2.1 by providing a typology of cybercrime. Three examples of target cybercrimes and three examples of tool cybercrimes were provided to illustrate how computers and the Internet facilitate cybercrime. This knowledge was required to understand how the type of crime, in this case *cybercrime*, influences criminal investigations. In brief, the analysis has shown that criminals can take advantage of computers and the Internet to commit crimes relatively anonymously across State borders. They can also reach many computer users as potential victims.

Step two was addressed in section 2.2 by explaining the investigative activities that law enforcement officials take based on the two digital leads of (1) IP addresses and (2) online handles. The analysis showed that law enforcement officials use the following digital investigative methods to gather evidence based on these two leads: (a) gathering publicly available online information, (b) issuing data production orders to online service providers, and (c) applying online undercover investigative methods.

Step three was addressed in three parts in the sections 2.3 to 2.5. Three challenges in cybercrime investigations were identified as (1) anonymity, (2) encryption, and (3) jurisdiction. The analysis showed that the technical challenge of anonymity can be overcome by using the same investigative methods as those based on the digital leads from online handles. The analysis with regard to the technical challenges of encryption showed that law enforcement officials can overcome this challenge by using (a) data production orders that are issued to online service providers and (b) hacking as an investigative method. The analysis with regard to legal challenge of jurisdiction has shown that mutual legal assistance – a mechanism for gathering evidence that is located on foreign territory – is often too burdensome for cybercrime investigations. Practically speaking, law enforcement officials can also gather evidence unilaterally across State borders. In that case, law enforcement officials of the investigating State gather evidence that may be located on foreign territory. These evidence-gathering activities are in tension with the principle of the territorial limitation of enforcement jurisdiction.

These three steps lead to the conclusion that the following digital investigative methods are commonly used – and applied across State borders – in cybercrime investigations:

(1) gathering of publicly available online information;
(2) issuing data production orders to online service providers;
(3) applying online undercover investigative methods; and
(4) performing hacking as an investigative method.