The Black Box Of Botnet Mitigation

-

Studying the Relationship between European Union Legislation and Botnet Mitigation Efforts

J.A. van Berlo

ANR 100325

Bachelor Thesis Liberal Arts and Sciences (Major: Law in Europe)

Tilburg University, Netherlands

Supervisor: Dr. C.M.K.C. Cuijpers

Date: 05-06-2019

I would like to thank those around me for being patient when necessary. I would like to thank them even more for getting impatient, after that.

Abstract

Botnets are an enormous and ever-growing threat to the security of our cyberspace. This thesis maps the European Union legislation relevant to botnet mitigation, focusing especially on that legislation pertaining to privacy and data protection. It will also examine how European Union legislation criminalizes behavior related to the propagation and detection of botnets. It will also examine in which ways the legislation regulates botnet mitigation efforts of private parties, as well as private parties collaborating with law enforcement authorities. Subsequently it will assess how the legislation discussed facilitates or obstructs common botnet mitigation efforts. It will also discuss the risks to certain fundamental rights (such as privacy and the right to data protection) which are posed by a lack of accountability found in current botnet mitigation efforts.

Table of Contents

"Die Geschichte der Menschheit ist die Summe menschlicher Entscheidungen. Wir entscheiden normativ, was wir wollen. Das wird so bleiben."

- **Thomas Ramge, 'Mensch und Maschine' (2018)[1]**

Chapter 1: Research Question and Outline

In this first chapter I will introduce the central research question of this thesis and its sub-questions, as well establish the general outline of the thesis. Before I can do so however, some general concepts and their pertinence to the research question will have to be introduced.

1.1 The Problem of Botnets

Botnets are one of the most persistent and costly threats currently faced by our internet economy. The OECD uses the following definition of a botnet:

'Botnets are networks of compromised computers ("bots", i.e. robots) connected through the Internet which are used for malicious purposes. These machines have been infected through a variety of techniques generally involving the installation of malicious software (known as malware) that enable the orchestrator of the botnet ("bot master") to control them remotely.'
- (OECD, 2012), p.7

Because the malware on these computers operates very sophisticatedly, users are often unaware that their computer has been turned into a bot. This fact, combined with a general lack of knowledge and ineffective preventive measures on the part of users, has caused malware to spread far and wide.[2] Because of their well-hidden and decentralized nature it is very difficult to accurately estimate how many computers worldwide are part of a botnet, and the estimates that are there vary. Some researchers estimate that up to a third of all internet-connected computers worldwide were part of a botnet,[3] while more conservative estimations place the amount of infected computers around 5%.[4] Furthermore, while most malware still infects personal computers, there has been a large increase of infections of smartphones and other internet-connected devices (the so-called 'Internet of Things' or IoT). In October 2016 the largest DDoS attack[5] in history took place, and it was executed primarily by a botnet which resided on IoT devices.[6] With around 8.4 billion devices connected to the internet (up

[1] (Ramge, 2018), p.94
[2] (Bauer & van Eeten, 2008), p.18-19
[3] Idem., p.9
[4] (Eeten, Bauer, Asghari, Tabatabaie, & Rand, 2010) p.2
[5] DDoS stands for 'Distributed Denial of Service', a type of cyber-attack where a botnet is directed to flood a server with traffic so the server is unable to function properly.
[6] (US-CERT, 2016).

31% from 2016) and 20.4 billion devices projected to be connected in 2020, even an infection rate of 5% indicates there are currently hundreds of millions of compromised computers.[7] The size of individual botnets can be in the millions: for example, the Andromeda botnet was estimated to have infected roughly 2 million devices at the moment it was taken down.[8]

The growth of these botnets is of course only a means to an end for the botmaster. He can subsequently direct the infected machines to perform any number of illegal and harmful activities, such as delivering spam via email or message boards, organizing DDoS attacks, scouring computers for sensitive and personal data, hosting illegal content, or spreading malware and ransomware.[9]-[10] Types of malware that utilize the users' CPU to mine for cryptocurrency have even been detected.[11] The software needed to operate a botnet is relatively inexpensive to purchase, ranging from 5.000 to 15.000 U.S. dollars for an initial package.[12] Alternatively, one can choose to purchase the services of a third-party botnet for even less money with a near-zero chance of detection.

The damage caused by botnets is difficult to measure and estimations by experts vary wildly. To illustrate this fact: one older study collecting estimations on the damage caused by malware found that these range anywhere from 13 billion US dollars in direct damages to the global economy to 67 billion US dollars in direct and indirect damages to the United States economy alone.[13] Currently we see a trend away from trying to estimate the total damages caused by botnet in the first place, because the collateral damage caused by these threats is incredibly difficult to calculate accurately.[14] One study, which only looked at the direct financial damages caused by the Zeus Botnet (and which is therefore more likely to be reliable than those which try to account for indirect damages) estimated that this botnet caused at least 100 million US dollars in damages by the time it was taken down.[15] While the total damages caused by botnets are therefore difficult to estimate even semi-accurately, we can nonetheless conclude that the research that does exist on the matter points towards these damages being considerable. Juniper Research (a cyber-security firm) has predicted that damages caused by malware will exponentially rise over the coming years, mainly because of poor user security and the quick exploitation of successful business models (such as ransomware and mining) and vulnerabilities (such as the IoT and smartphones) by malware distributors.[16]

The negative impact of botnets goes beyond the economic damage caused by, for example, paid ransoms, stolen credit card information, damaged hardware and lost productivity, however. Experts have signaled an increase in the use of botnets for politically motivated attacks. Early significant examples of these were the DDoS attacks on Georgian digital infrastructure that corresponded with the on-the-ground war between Georgia and Russia in 2008, as well as the DDoS attacks on opposition media during the political conflict in Burma.[17] A more recent example (of which we still

[7] (Gartner Inc., 2017).

[8] (Europol, 2017), par.6

[9] Ransomware is a type of software that locks the user out of his computer, often promising to unlock it once a certain amount of money is paid to the party distributing the malware.

[10] (OECD, 2012), p.7

[11] (Huang, 2017).

[12] (Vihul et al., 2012), p.5

[13] Idem, p.6

[14] (Romanosky & Goldman, 2016), p.12

[15] (IBM Security, 2017), p.2

[16] (Juniper Research, 2015).

[17] (Nazario, 2009), p.5-6

not know the full extent or impact) is the use of bots by both campaigns during the United States elections to gain an online presence and influence debate. These bots were able to spread messages in large volumes at an astonishing rate: a sample of 500 suspected bot accounts on Twitter posted 400.000 messages related to Trump in a month's time.[18] While employees of both campaigns readily admitted to the use of botnets (albeit anonymously to an Oxford University researcher), it seems likely that a large amount of these bots were purchased from botmasters outside the United States: analysis of bot activity surrounding a (false) rumor related to the Clinton campaign indicated that a disproportionate amount of posts came from Vietnam, Cyprus and the Czech Republic.[19] Furthermore, there is considerable proof that countries outside the United States have attempted to influence public opinion during the elections by harnessing the power of botnets to spread their propaganda.[20]

It seems clear therefore that botnets have not only grown into sophisticated tools for the realization of a large and ever expanding set of criminal goals, but are also shaping up to be powerful political instruments aimed towards the spread of propaganda and the silencing of critics.

1.2 Research question

In light of the broad and increasing danger posed by botnets, it can be generally agreed that effective steps towards the mitigation of botnets (and the prosecution of their masters) are desirable. Nonetheless, agreeing thereupon does not necessarily make it so, and there are a myriad of obstacles standing in the way of effective mitigation. Examples of these include, but are not limited to: an aforementioned lack of user-security and awareness, the cross-national nature of botnets, a lack of interest shown by Internet Service Providers (ISPs) in policing their networks and the ease with which botmasters and their clients can obfuscate their identity.

While all these problems are interesting and deserve attention, this thesis will deal with one specific issue concerning the mitigation of botnets, and that is the legislative framework in place to facilitate or obstruct this mitigative process.

Research by Vihul et al. has indicated that there are many ways that 'the fight against botnets is touching the limits of existing law'.[21] They concluded at the time of writing (in the distant past of 2012) that there was a lack of accurate criminalization for many behaviors related to botnets, too few incentives for key players such as ISPs to fight botnets, and questions about privacy-infringements with regards to botnet detection methods. However, since the writing of this thesis botnet detection methods have changed, and substantive legislation related to cybersecurity and data protection has gone into force in the European Union. It is therefore worth considering whether these concerns raised by Vihul et al. have been addressed, are still relevant, or have been replaced by entirely new concerns instead.

Starting with the problems indicated by Vihul et al., this thesis aims to explore how European Union legislation affects botnet mitigation, with a focus on data protection and privacy. The scope of this thesis is deliberately wide because it aims to give an overview of the legislation relevant to botnet

[18] (Woolley & Guilbeault, 2017), p.11
[19] Idem, p.10
[20] (Twitter Public Policy, 2017).
[21] (Vihul et al., 2012), p.18

mitigation. Additionally, it will try to be a jumping-off point for those interested in more thoroughly researching the individual questions raised in this thesis.

The main research question of the thesis is:

'How does European Union legislation facilitate the mitigation of botnets?'

With the sub-questions being:

- **How does data protection and confidentiality of communications legislation in the European Union affect botnet mitigation?**
- **How does the European Union legal framework criminalize behavior related to the operating of a botnet?**
- **How does the European Union legal framework incentivize the participation of private parties in botnet mitigation?**
- **How can European Union legislation improve botnet mitigation while still respecting fundamental rights to privacy and data protection?**

1.3 Outline

Chapter 1 will give a brief introduction to the topic of botnets and present the research questions and outline.

Chapter 2 explains in more detail how botnets function, propagate, and are operated. It will also examine and explain the most common technical countermeasures used to detect, obstruct, and take down botnets.

Chapter 3 maps the European Union legislation relevant to botnet mitigation. It will do so by examining the fundamental rights established with regards to privacy and data protection, then go on to look at the legislation criminalizing botnet-related behavior, and finally it will explore current and upcoming data protection legislation (both in regard to private parties and law enforcement).

Chapter 4 will investigate what the positive effects of the legislation examined in chapter 3 are on the botnet mitigation methods discussed in chapter 2 (i.e. in what ways the current legislation facilitates botnet mitigation). I will do so by dividing the techniques up in three categories: 'general', 'technical' and 'procedural' botnet mitigation. In this chapter I will also make a case for why privacy and cybersecurity are not as diametrically opposed to one another as they are commonly presented.

Chapter 5 is in many ways the inverse of the chapter preceding it: it will examine the negative effects of the legislation examined in chapter 3 on the botnet mitigation techniques discussed in chapter 2. This in part entails the ways in which the current legislation obstructs botnet mitigation. It also includes negative effects on certain fundamental rights produced by the botnet mitigation itself, more specifically by something I have come to call 'black box botnet mitigation'.

Finally, in chapter 6 the thesis will give some tentative suggestions for improving or addressing some of the problems described in chapter 5. After this I will conclude by answering the research questions posited in this chapter.

Chapter 2: Botnet Propagation and Detection

Before I can examine the effect of European Union legislation on botnet mitigation I will first briefly introduce the fundamentals of the propagation and functioning of botnets, their detection, and the methods used to disable them through the deployment of technical countermeasures. At the end I will briefly examine two real-life takedowns of botnets to show how these elements work together and what parties are involved in coordinating them.

2.1. Propagation of Botnets

A botnet is a network of infected computers (bots) that are controlled by an operator (the botmaster). This infection happens when a malicious executable program (the bot binary) is installed on a computer. The spread of this infection can either happen actively or passively, a distinction that is made to indicate whether end-user intervention is necessary for the installation to occur. Active infection refers to a botnet that targets and infects computers autonomously without (human) intervention, scanning for other devices that are on the networks of the infected machines and subsequently exploiting security vulnerabilities to spread the bot binary. Passive infection on the other hand does require user intervention for the bot binary to be installed. Khattak et al. identified the three most widely used passive infection methods, which I will include here to illustrate how sophisticated these methods are in practice.[22]

- *Drive-By-Download***:** a ‘drive-by-download’ occurs when a user visits a webpage that runs malicious code which scans the computer for security vulnerabilities and subsequently uses those to install the bot binary without the user noticing. This method is highly insidious: while the infection can be launched from a specially prepared website that is owned by the botmaster or his associates, the bot binary can also be installed from the website of an unwitting third party’s website. This happens either through the hacking of those websites or even more covertly, by running the malicious code from ‘active elements’ (e.g. ads or plugins) that are active without the control of the original owner. This means that users can be conscientious enough to only visit websites from reputable sources and still end up with an infected computer.[23]

- *Infected Media:* in this case malware is present on media (such as a USB flash drive). The human intervention in this case is the act of connecting the media to a new computer. Often the presence of the bot binary is not obvious to the casual user and is it installed immediately and invisibly upon the connection of the media to a device.[24] The malware can be either pre-installed by parties having access to the media before it reaches the end-user or spread from an infected computer to the media. As an example, the former is likely what happened in 2017 when USB drives used by the technology company IBM to distribute an

[22] (Khattak, Ramay, Khan, & Khayam, 2012), p.2-3
[23] (Zaharia, 2016).
[24] (Khattak et al., 2012), p.3

activation key were found to also carry malware.[25] As for the latter, a bot binary on an infected computer can be programmed to copy itself to inserted media and subsequently spread itself when this media is connected to a new device.

- *Social Engineering:* social engineering entails the user being tricked into voluntarily downloading the bot binary on this device. This can be through the well-known example of misleading pop-ups claiming that the user needs to download a certain file or via extremely well-designed phishing emails with an infected attachment that purport to contain important information. A relatively newer development is the hacking of social media accounts so as to utilize the higher level of trust between users of social networks: hacked accounts will for example send messages containing a link that seemingly leads to a YouTube-page but which actually installs malware on the users' computer.[26]

When we examine these methods for propagating a bot binary we should take note of the fact that both passive methods as well as two out of three of the detailed active practices (with the possible exception of social engineering) do not involve the user being aware of the fact that a file is being installed in the first place. This unawareness not only decreases the chances of detection for the bot binary but also means that if detection were to occur (e.g. when antivirus software flags the bot binary or its activity) the user is less likely to trace back the origins of the attack and subsequently alter their behavior to avoid infection in the future.

2.1.1. Propagation of Botnets in the age of IoT

One (arguably impressive) trait of botmasters is that they have proven to be extremely quick to experiment with and incorporate technological developments into the functioning of botnets. Examples of these include the fact that botmasters were very early adopters of cloud technology to host their servers and have used social media pages to relay messages from a botmaster to its bots as far back as 2006.[27] Perhaps the most worrying of these trends is the quick growth of botnets that reside wholly or mostly on so-called 'Internet of Things' (IoT) devices. The 'Internet of Things' is a catch-all term for devices that mostly independent from human intervention harvest sensory information and interact with the world.[28] Examples of this could include industrial machinery collecting and relaying information, or a device worn by patients that sends periodical status updates. However, by far the largest and fastest-growing component of the IoT are consumer products such as network-connected cameras, smart meters, routers, or even fridges and solar panels.

IoT devices face a security risk for a number of technical reasons: one of these is the fact that IoT systems often use the same communication protocols, thereby ensuring that discovered vulnerabilities in these protocols immediately apply to a large number of devices.[29] However, as is often the case we find that the vulnerability of IoT devices is caused more by unforced human behavior than compounding technical problems. Manufacturers often eschew adequate security measures in light of a market that demands ever cheaper internet-connected products and

[25] (Forrest, 2017) .

[26] (Khattak et al., 2012), p.3

[27] (Burghouwt, 2007) p. 46

[28] (Gubbi, Buyya, Marusic, & Palaniswami, 2013), p.1646

[29] (Bertino & Islam, 2016) , p.77

majoritatively does not make purchasing decisions based on the security of a device.[30] One study by HP found that the IoT devices tested averaged 25 vulnerabilities per device, with 80% of devices using either no, standard, or weak passwords and with 60% running firmware or a user interface that contained security vulnerabilities.[31]

Technical vulnerabilities and weak security measures implemented by manufacturers compound to make IoT devices especially vulnerable to passive propagation of malware. In addition to this, once infection has occurred factors such as the frequent lack of a screen and the relative autonomy of these devices (meaning users often interact little with it) contribute to smaller chances of infection being detected by the consumer.[32] Speculatively, it does not seem unlikely to assume that factors such as poor consumer awareness of this phenomenon and the relatively innocuous functions performed by most IoT devices (users are probably more likely to be concerned about the health of their personal computer than that of their smart fridge) only lead to increase the infection rate of IoT devices. As an example of how easy it is for malware to propagate on IoT devices and the subsequent damages this can lead to one does not have to look further than the case of the Mirai botnet. Its tactic was shockingly simple: the bot trawled the web using a list of 62 common default usernames and passwords for a number of prevalent IoT devices. Through this method it created what is considered to be one of the largest botnets in history.[33] Over the course of 2014-2016 it was used to carry out a number of DDoS attacks (which increased in severity as the botnet grew exponentially) on security companies and webhost, inflicting millions of damages and resulting in the inaccessibility of prominent websites such as Twitter, Reddit, Netflix and Airbnb.[34]

With IoT devices entering the market at an ever-increasing speed, the rate of propagation (and therefore the scope and power) of botnets is only expected to accelerate.

2.1.2. Contact between the Bot and Botmaster

No matter the method used to initially infect a computer or the exact nature of the device infected, the next step for a bot is to discover its ‘Command and Control’ (C&C) server. The botmaster communicates with his bots through this server and it is this contact that sets botnets apart from many other viruses for two main reasons.[35] Firstly, it makes it possible for the botmaster to bundle the computing power of a large number of bots effectively: the most obvious application of this are the large scale DDoS attacks carried out by botnets. Secondly, his continuous contact with the bots also enables the botmaster to send out software updates (e.g. with countermeasures against detection) or change the bots’ settings so as to perform a different task. This makes botnets both highly versatile and resilient against mitigation.[36] The initial establishment of contact between a bot and the C&C server is called ‘rallying’.[37]

[30] (Mcdermott, Petrovski, & Majdani, 2017), p.1
[31] (HP News Advisory, 2014).
[32] (Mcdermott et al., 2017), p.77
[33] (US-CERT, 2016).
[34] (Williams, 2016).
[35] To even further decrease the chance of detection a botmaster will often deploy a number of proxies, called ‘stepping-stones’ between himself and the C&C server. For further literature on stepping-stones and how they work see Khattak et al.
[36] (Burghouwt, 2007), p. 3-4
[37] (Khattak et al., 2012), p.3

While this connection is the botnets' greatest strength it is also a weakness for a number of reasons. Firstly, both the rallying and later contact between bot and C&C server creates activity on the network which can be detected and monitored. Secondly, once access to the C&C servers is denied (or the C&C server seized) the botnet would be severely hampered in its functioning or even made defunct entirely.[38]-[39] This of course has led botmasters to take a number of countermeasures such as using multiple C&C servers for redundancy,[40] sophisticatedly hiding their bots' activities between regular internet traffic, as well as them obfuscating the digital locations of their C&C servers.[41] For example: bots would initially have the IP address of the C&C server it wanted to contact baked into its code, a method referred to as 'binary hardcoding'. While there are some advantages to this method (chief among them being that it creates relatively little activity on the network) its main downside is that once the bot binary is detected it is possible to reverse engineer its code and locate the IP address of the C&C server. Any attempts at communication between the bot and its C&C server can subsequently be blocked. As a response to this bots now often employ alternative methods of contacting their C&C servers, such as the use of multiple dynamic IP addresses ('fast-flux networks') or the use of randomly generated domain names, both of which make the C&C server more resilient to takedown and more difficult to detect. [42]

Finally, in addition to the communication between the C&C server and bots being crucial to the overall functionality of the botnet it should be noted that the botmasters other incentive to obfuscate the C&C server's location is the fact that law enforcement upon discovery of the C&C server might be able to trace any communication back to the botmaster personally.

2.2. Detecting a Botnet

Having briefly looked at methods of propagation of bots and the communication method between bots and the botmaster, I will now examine some widely-used methods for detecting bot activity and communication on a network. It should be noted that this thesis will mostly examine detection methods that focus on the measurement of bot activity and communication on a network or device, since these are the methods that have the most friction with existing privacy regulation. While there are other methods to detect a botmaster, bot, or C&C server, these should be considered outside of the scope of this thesis and will therefore not be discussed.

We can broadly categorize two different methods used to detect botnet activity on networks: 'passive and 'active' measurement. Passive measurement entails methodologies where activity on a network is observed without actively interfering with the data, the behavior of the botnet or its communication. Active measurement however goes a step further and communicates with or manipulates the data stream on the network. This allows for deeper insight into the botnet but might also create activity that can be detected by a botmaster who might subsequently deploy

[38] (Vihul et al., 2012), p. 16 & 35-36

[39] Note that while the botnet would be made useless to the botmaster, damaging activities carried out by the bot at the time of the takedown of the C&C server could continue on the computer of the end-user.

[40] (Vihul et al., 2012), p.6

[41] (Czosseck & Geers, 2009), p. 215

[42] (Khattak et al., 2012), p.3-5

countermeasures.[43] Parties are generally more reluctant to deploy active detection methods because there are more ethical and legal questions associated with these practices, something which I will explore further in a chapter 4 and 5.

2.2.1. Passive Detection Methods

- *Packet Inspection:* until recently one of the most common methods of detection, packet inspection means that certain parameters of sets of data ('packets') on a network are checked against a large database of known unusual or suspicious behavior. The large downside of this method is that it is not equipped to deal with a high flow of traffic (meaning it is much more successful on private networks than public ones), and that sampling traffic to reduce the flow of data will increase the chances of missing bot activity.[44] Packet inspection was long seen as a privacy-friendly method of botnet detection because it used a relatively small set of data to detect bot behavior. However recent developments have proven that it is in fact possible to identify users based on the packet data alone, which has raised questions about the legality of this method in many jurisdictions.[45] Furthermore, while the data that the packets are matched against is very limited, the packets themselves may contain personal information such as banking information, credit card information or passwords.[46] While most packet inspection methods will have it as general practice that any information in the package is not stored unless a match with suspicious behavior is found, the packet possibly containing personal data is still 'opened' and checked. Furthermore, packet inspection is often accompanied by decrypting and re-encrypting SSL-encrypted communications on a network, adding to the invasive nature of this technique.[47]

  Packet inspection on large networks (such as those operated by ISPs) for the purposes of botnet detection has mostly been abandoned because the alternative inspection method, flow analysis, has proven to be much more accurate on large networks and scales better.[48] Nonetheless, packet inspection is still carried out on private networks, such as office servers and cloud networks, often because the packet inspection is part of other security or maintenance tools.[49]

- *Analysis of Flow Records:* the most popular method of botnet detection currently. Similar to packet inspection it matches a set of parameters against a database of known suspicious behavior, however instead of inspecting a series of packets, this method analyzes the data stream (also known as 'flow' data) itself. The parameters used here are more general in nature than those used for packet inspection.[50] Because of this analysis of flow records allows for near-real time inspection of high traffic flows and it greatly reduces the amount of

[43] (Atluri & Tran, 2017), p.20
[44] Idem., p.16
[45] (Abt & Baier, 2011), p.42-43
[46] (INFOSEC Institution, 2018),
[47] (INFOSEC Institution, 2018).
[48] (Abt & Baier, 2011), p. 43
[49] Packet inspection gives network administrators more information than flow inspection does about possible threats, nature of software involved, diagnosis of errors, etc. (Dougherty, 2017).
[50] (Atluri & Tran, 2017), p.18

personal data collected. While some anonymization is still necessary (in particular of IP addresses), this means that it is easier to comply with existing privacy regulations.[51]

- *Honeypots/Sinkholing:* A honeypot is a computer which is purposely left vulnerable to outside intruders. Once this device has become a bot, it can be monitored closely so as to examine the behavior of the botnet (e.g. its goals, methods of propagation, nature of communication with the C&C server). Studying the nature of the infection can also help administrators to develop future security policies.[52]

  A network-based equivalent of a honeypot is called sinkholing. In this case a system administrator or network operator has a list of known malicious hosts and domains. Whenever a computer on the network tries to access one of the domains on the list (such as when a bot communicates back to its C&C server) it is instead redirected to a safe domain by the system administrator. This does not only hinder the botmaster because it is not able to communicate with the bots on this network, but it also allows the system administrator to see which clients on the network are bots. Sinkholing can also go the other way, where a network operator can divert incoming traffic from a known malicious source. By diverting traffic in this way sinkholing can be a very powerful anti-DDoS technique.[53]

  There is one problem affecting the utilization of this method and that is the large amounts of personal data that sinkholes might collect. Seeing how sinkholes collect the data that bots would originally send back to the botmaster, this might include everything from personal information, keystrokes, screenshots, credit card information or passwords. Additionally, this happens in a way that is much more systematic than with the already sensitive packet inspection (packet inspection runs the risk of accidentally retrieving sensitive information from a package through sampling, where sinkholing actively intercepts all information that is transmitted from known bots to the botmaster).[54]

- *Antivirus and Software Feedback:* many antivirus and software solutions monitor for bot activity based on databases. However, software will also learn from new viruses occurring by randomly monitoring activity on the machines of clients. This information will be subsequently used to update the existing databases and is therefore a valuable source of information on botnets and their functioning.

Besides these passive botnet detection methods there are active detection methods, most of which are rarely deployed because of their intrusive nature and therefore not worth examining in detail. However I will discuss one method ('infiltration'), because of its relatively prevalent use by law enforcement.

[51] (John, Tafvelin, & Olovsson, 2010), p.9
[52] (Atluri & Tran, 2017), p.19
[53] (Incapsula, 2019).
[54] (Abuse.ch, 2018).

2.2.2. Active Detection Method

- *Infiltration:* for this method a machine is disguised as a bot, which will subsequently be used to contact the C&C server (or another bot in the case of a p2p botnet) in order to learn more information about the functioning of the bot and the goals of the botmaster.[55] Sometimes the infiltration is followed by a takeover of the C&C server. The advantage of taking over the C&C server as opposed to simply taking it down is that the botnet can be very effectively mapped once the C&C server is controlled as bots in the network will inevitably attempt to contact the C&C server.[56] Theoretically this control over the C&C server would also allow an immediate cleansing of the botnet through a so-called 'remote clean-up', however this method bring along a number of legal and technical issues with it in practice, and is therefore rarely utilized.[57]

2.2.3. Involved Parties

It is important to distinguish the main parties involved with the detection and mitigation of botnets. Not only does the mandate to act differ from entity to entity but each party might also have certain legal responsibilities when it comes to botnet mitigation. What follows is a broad overview of the parties involved grouped by legal standing.

- *Law Enforcement Agencies:* these are government agencies that have a mandate to enforce the laws within their jurisdiction. Because of the international nature of botnets, law enforcement efforts are often coordinated by EU law enforcement agencies such as Europol.[58]

- *Botmasters:* the person or people operating a botnet.

- *Internet Service Providers:* Internet Service Providers (ISPs) maintain and control public internet infrastructure and are therefore uniquely positioned to detect and mitigate botnet activity on their networks. They are also incentivized to embrace this position since botnets take up valuable bandwidth on the ISP's networks.[59] Furthermore, research by van Eeten et al. has discovered that the majority of bots are located on a relatively small amount of the largest ISPs.[60] These factors compound to make ISPs natural control points for botnet mitigation, and suggest that these actors should have a leading role in fighting botnets.

- *Antivirus and Software Companies:* this is meant to refer to companies who provide software that is specifically meant to mitigate bot activity on a machine or network. Not only do these companies play an important role in stopping individual infections (which, while important, is not necessarily the focus of this thesis) as mentioned above they also actively track and collect information about many botnets.

[55] (Khattak et al., 2012) , p.16
[56] (Atluri & Tran, 2017), p.22
[57] (Vihul et al., 2012), p.42
[58] (Europol, 2017).
[59] (Pijpker & Vranken, 2016), p.24
[60] (Eeten et al., 2010), p.23

- *Public-Private Partnerships:* This refers to an increasingly common form of cooperation where law enforcement agencies work closely together (often at most or all stages of an investigation) with private stakeholders, such as ISPs but also large tech companies such as Microsoft and NGO watchdogs like the ShadowServer Foundation, so as to more effectively target botnets.[61] There has been an increase of these public-private partnerships in the last decade, especially in the field of cybercrime.[62]

- *Researchers:* by these I mean academic researchers that study botnets and their mitigation. While the mandate of these researchers is relatively limited (and, due to their public nature, much more scrutinized than that of many companies) their analyses of botnet behavior and detection methods nonetheless contribute heavily to botnet mitigation processes utilized by all involved parties.[63]

- *End-Users:* this refers to the end-users of machines or networks that run a risk of infection by a bot. This group plays no substantial role in the monitoring or mitigating of a botnet, and while there has been some legal discussion about the liability of owners of infected machines this has proven to be largely inconsequential.[64] The reason that this group is nonetheless included in the analysis is the fact that it is their privacy which is often at stake and which legislation largely attempts to warrant.

2.3. Taking Down a Botnet: In Practice

Because of the international and complicated nature of a botnet, implementing the above-mentioned botnet detection and mitigation techniques often requires a large amount of coordination between different parties. To illustrate this I will look at two real-life examples of botnet takedowns. The first case I will discuss is somewhat dated in terms of technological developments, but it is still relevant because the parties involved wrote a relatively extensive report detailing how the Bredolab botnet was tracked and terminated. It is a known problem that, because many botnet mitigation operations never go to trial, often the exact methods used to track the botnets and by which parties (public or private) cooperate are never publically revealed. This of course also means that these methods are seldom scrutinized publically.[65] In addition to being an exception to this rule, the Bredolab botnet takedown also serves as to illustrate as a good example of the way public-private partnerships function.

2.3.1. The Bredolab Botnet

The Bredolab botnet was first discovered by researchers and antivirus companies in 2009.[66] In 2010 a Dutch hosting provider (Leaseweb) was notified by a Swiss internet security NGO (Abuse.ch) that

[61] (Lerner, 2014) , p.247
[62] (Lerner, 2014), p.247
[63] (John et al., 2010), p.18-19
[64] (Vihul et al., 2012), p.60
[65] (Lerner, 2014), p.250
[66] (de Graaf, Shosha, & Gladyshev, 2012), p.5

Bredolab intersected with the networks of the hosting provider. Leaseweb would normally attempt to block the C&C servers from their networks themselves, but the botnet was large and complicated enough to prompt the provider to contact the National High Tech Crime Unit of the Netherlands (NHTCU), which started an investigation.

The NHTCU acquired data from Leaseweb, as well as by placing wiretaps on Leaseweb servers. The collected data consisted of source and destination IP addresses, networking protocols, and source and destination port numbers.[67] Through this the Bredolab communication infrastructure and its scope (it was estimated to have infected at least three million computers) were mapped and law enforcement infiltrated and took control of the server.

After control of the C&C server was achieved, malware distribution tasks were stopped. While this stopped the growth of the botnet, it did nothing to disinfect the end-users from the malicious software already on their computers. This is a common problem in botnet mitigation: viruses remaining on computers could still do damage to end-user devices or leave vulnerabilities that may be abused by future hackers. The NHTCU therefore kept the botnet infrastructure online for a few days in order to update all the bots on the network. This update showed end-users a message telling them to disinfect their computers. The servers, which were located in the Netherlands and France, were confiscated and an international arrest warrant was issued for the Armenian suspect, who ended up receiving a four-year sentence in his home country.

2.3.2. The Avalanche Network

The Avalanche Network was a delivery and management platform for different ‘families’ of botnets and malware.[68] First discovered in 2012 by German police, the investigation of the Avalanche Network took over four years and was carried out mainly by the German Federal Office for Information Security (BSI), the FBI, Europol, Eurojust, and select private parties.[69] The size of this investigation was warranted by the network its use of then-uniquely complicated methods of fast-flux networks and domain generation, as well as by the robust and redundant nature of many components of the infrastructure. The mapping and analyzing of the botnet structure itself was done mainly by the BSI and a private research institute, which also ‘extracted victim’s data’ and catalogued it for the BSI.[70] What type of data was extracted and by which methods this was done, was not disclosed.

After successfully mapping its infrastructure, the botnet was eventually taken down through a combination of physically seizing 39 servers, taking 221 servers offline, and sinkholing any traffic to the servers. The takedown and sinkholing were partially done by private parties. The data from these sinkholes provided much additional information about the infrastructure of the network, which was analyzed by the BSI in conjunction with other private parties

[67] (de Graaf et al., 2012). p.6
[68] (The Shadowserver Foundation, 2016a).
[69] (Europol, 2016).
[70] (Fraunhofer FKIE, 2016), p.2

2.3.3. Growing Dependence on Public-Private Partnerships and the Move to Disruption

Finally, to understand the current state of botnet mitigation we first need to establish two trends in botnet mitigation, which are an increased reliance by law enforcement on public-private partnerships and a move towards disrupting cybercrime instead of prosecuting it.

The Bredolab takedown serves as a good example of the extent to which law enforcement initially relied on public-private partnerships for botnet mitigation, which was mostly in early stages of detection. It was private parties which first noticed the botnet's activities and purpose, and the police used the infrastructure of Leaseweb to investigate the botnet. Alternatively, private parties can often be reliant on the extended powers and capabilities of law enforcement to truly take down a large and branching botnet. This division of labor, where law enforcement expects private parties to monitor and manage early stages of botnet activity on their networks themselves before stepping in for more serious cases, has proven to be realistic and effective to a point where it is codified to a certain extent: ISPs may be required under European Union law to communicate certain threats to authorities and cooperate with investigations, something which I will discuss further in chapter 3.[71]

The Avalanche network illustrates the changed nature of these public-private partnerships over the last few years. As botnets have gotten larger and more complex, law enforcement has gotten more dependent on public-private partnerships, and international coordination has gotten more necessary. Public parties were involved at every step (detection, analysis, takedown and end-user notification) of the investigation of the Avalanche network, and information was shared with law enforcement agencies from thirty-nine countries. From a privacy and data protection perspective this is important: where (personal) data is shared with more parties and on a larger scale, additional risks and legal responsibilities are created.

Nowadays private institutions, especially those dealing with network operation or cybersecurity, are often better equipped than law enforcement to perform these investigations. This is in part because they might operate the infrastructure on which the investigation takes place, and in part because they have the additional technological expertise to actually perform the investigation.[72] Secondly, the international nature of botnets means traditional law enforcement institutions often face challenges related to jurisdiction, seeing how cybercrime tends to not restrict itself to one single territory or to traditional geographic borders.[73] Internationally operating institutions are much more agile when facing these challenges because they are less restricted by traditional territorial jurisdiction.

Lastly, private institutions are incentivized to join these partnerships for a number of reasons. The first one is that operators of communication services have a financial incentive to keep their networks clean because botnets 'eat up' a lot of the available bandwidth on a network.[74] Another reason is the fact that private institutions might be able to gain a competitive advantage over their competition when partaking in these partnerships, something which I will discuss in more detail in chapter 5. The final factor that I believe incentivizes private institutions to cooperate in this manner is the legal uncertainties surrounding botnet mitigation and the data protection reform. Non-

[71] (Tjong Tjin Tai, Op Heij, E. Silva, & Skorvánek, 2015), p.59-60
[72] (Bossong & Wagner, 2017), p.266
[73] (Koops & Goodwin, 2014), p.40
[74] (Eeten, Bauer, Asghari, Tabatabaie, & Rand, 2010), p.10

compliance with the law in these areas can cost institutions heavily and public-private partnerships allow them to operate under the umbrella of law enforcement, which partially shields them from the responsibility and risks that otherwise comes associated with botnet mitigation.

These public-private partnerships have been central in Europol's new cybercrime strategy, which they have stated requires an approach where 'cooperation with the private sector is of critical importance.'[75] This is also reflected in practice: virtually every large-scale takedown of a botnet in the last few years has seen the involvement of a large group of private institutions. Some examples of this can be found in the takedowns of the Ramnit botnet and the Avalanche network.[76] Wil van Gemert (Deputy Director Operations of Europol at the time) said about the Ramnit takedown that the operation 'shows the importance of international law enforcement working together with private industry in the fight against the global threat of cybercrime.'[77] Before I go on to criticize the negative side-effects created in part by the current move to public-private partnerships it is important to note that van Gemert's assessment is very much accurate. Public-private partnerships have become an essential, effective and logical element of botnet mitigation for the reasons listed above, and contribute to the safety of our cyberspace.[78] This is reflected by the fact that these public-private partnerships have been provided a legal basis to some extent through Recital 11 of Directive (EU) 2016/680 (LED) which stipulates that third parties can process data for law enforcement under the directive as long as they are subject to a contract or other legal act.

The second development is the move towards the disruption of cybercrime instead of the prosecution of it. The transnational nature of cybercrime and the ever-more powerful encryption methods utilized are making it increasingly difficult for law enforcement to effectively prosecute cybercriminals.[79] This has made law enforcement opt for disrupting these criminal activities instead: in the case of botnet mitigation this will mostly entail taking down or sinkholing servers and bots instead of arresting those that are actually behind the criminal activity. Oerlemans while writing about this phenomenon mentions a marked decrease in Europol press releases about botnet mitigation mentioning the arrest of suspects, instead only talking about disruptive tactics such as sinkholing and server takedowns.[80] It should be noted that, as with public-private partnerships, Europol has laid out the move towards disruption (specifically mentioning botnet mitigation) as part of their new cybercrime strategy.[81] This development is in many ways a very pragmatic approach to the growing problem of botnets: while it is less than ideal to let suspects go unprosecuted it is important that botnets are effectively disrupted in some capacity when we consider their cost to society. Nonetheless, a lack of prosecution also brings with it some problems: not only will it feel unjust to many to let criminals go unprosecuted, but it also means that there is a decrease in judicial review (which mostly takes place in the prosecution phase) for the investigative practices deployed by law enforcement. In chapter 5 I will go on to explain how the practice of public-private partnerships and the move to disruption combine with a number of weaknesses in the European

[75] (European Commission, 2015), p.20
[76] (Europol, 2017).
[77] (Europol, 2015a), par.3
[78] (Lerner, 2014), p.250
[79] (Oerlemans, 2017b), p.363
[80] Idem., p.364
[81] (Europol, 2015b), p.12

Union data protection regime to lead towards a type of ‘black-box botnet mitigation’ where there is a systemic lack of oversight on botnet mitigation practices.

2.4. Conclusions for Chapter 2

In this chapter I have given an overview of the broad functioning of botnets, how they are propagated and how they are detected. A key takeaway here is that bots reside largely on personal devices, and that botnet detection methods analyze communication data from these devices. This means that these methods might seriously infringe upon the privacy of end-users as bot activity is intermingled with the personal communications of end-users. An example of this could be seen in the case of packet inspection, which might collect personal data such as credit card information in its search for bot activity. However, even detection methods that are considered to be more privacy-friendly (e.g. analysis of flow records) collect personal information such as IP addresses. These detection methods will therefore be (at least partly) governed by data protection and privacy legislation, and be subject to the restrictions and requirements laid out therein. I will discuss this legislation and its relationship to the botnet detection methods

One other important aspect to take note of is the important role of private parties in botnet mitigation, even in the advanced stages of law enforcement investigation, and the move towards disrupting cybercrime instead of prosecuting it. The examples of the Bredolab and Avalanche takedowns not only serve to illustrate how crucial a role these private parties play, but also as an example of how botnet mitigation has changed in less than a decade. However there are a number of concerns one can raise about these developments. The increase in public-private partnerships entails botnet mitigation moving away from ‘traditional’ law enforcement investigative avenues, which are subject to better established checks and balances. Additionally, a decrease in prosecution of cybercrime means there is less judicial oversight on investigations. [82] The investigative methods used in botnet mitigation operations bring with them a risk to fundamental rights of privacy and data protection, and therefore these developments should be considered cautiously. I will further discuss this problem of ‘black-box botnet mitigation’ in chapter 5 of the thesis.

In the next chapter I will present an overview of European Union legislation that is relevant to botnet mitigation.

[82] (Oerlemans, 2017b), p.363

Chapter 3: Relevant Legislation

In this chapter I will give an overview of the legislation and jurisprudence relevant to botnet mitigation in the European Union. While the area of law pertaining to botnet mitigation at least tangentially is obviously vast, for the purpose of brevity I will mostly focus on laws directly relating to cybercrime and data protection. These are also areas which have had or will receive major legislative updates in the European Union that make them worth examining specifically. Through this the European Union has laid a strong foundation of rights and responsibilities pertaining to data protection and cybercrime (that will be internalized by its member states) that heavily influences the possibilities for botnet mitigation. Furthermore, since botnet propagation is an international problem it is helpful to examine the strengths and weaknesses of the European Union-wide framework of legislation related to it.

I will go topic-by-topic through this chapter, starting with the general framework, cybercrime legislation and finally examining the data protection regime established within the European Union.

3.1 General Framework

Although it is tempting to view the subject of botnet mitigation through a purely technical lens, we must not lose sight of the fact that fundamental rights are at risk of being encroached upon in the process of detecting and disrupting botnets. Therefore I will start by establishing which rights relevant to our review are primarily established. I will include the European Convention on Human Rights (ECHR) in this as well as decisions by the European Court of Human Rights (ECtHR), which enforces the Convention. While botnet mitigation touches upon many fundamental rights tangentially, I will limit this summary principally to the right to private and family life, and the right to data protection. The European framework used for this thesis consists of three documents: the European Convention on Human Rights, the Charter of Fundamental Rights of the European Union ('the charter') and the Treaty on the Functioning of the European Union (TFEU).

3.1.1 The Right to Respect for Private and Family Life

- Article 8(1) of the European Convention on Human Rights establishes a right to respect for private and family life, including correspondence. Article 8(2) creates a general prohibition on governments to interfere with this right, except where in accordance with the law and 'where necessary in a democratic society' for national security or other legitimate interests.[83]-[84] Article 8 ECHR and the jurisprudence concerning it are considered to have established many of the standards for data protection and digital investigative methods.[85]

[83] Which entails, as per the wording of article 8(2): *"public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others"*

[84] (Council of Europe, 1950), art. 8

[85] (Oerlemans, 2017b), p.9

- Article 7 of the Charter of Fundamental Rights of the European Union establishes the same rights as article 8(1) ECHR, only changing 'correspondence' to the more future-proof 'communications' in its wording.[86] While article 7 of the charter does not have a limitations clause such as 8(2) ECHR, article 52(3) of the charter establishes that the meaning and scope of rights corresponding to those in the ECHR are the same as in the ECHR.[87] The Presidium of the European Convention (which drafted the charter) has confirmed that article 7 of the charter and article 8 ECHR are correspondent, and that the limitations established by 8(2) ECHR therefore apply.[88]

3.1.2 The Right to Data Protection

The concept of a 'right to data protection' as one separate from that of a right to privacy is relatively new and most commonly found within European legal traditions. 'Data protection' is not a right established within the ECHR, which was written in 1950. It should be noted nonetheless that the Council of Europe laid the foundation for much of modern data protection legislation when it adopted the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data ('Convention 108'), which introduced many concepts in regards to data processing (such as the right to access and correct information) that are used by the ECtHR and which subsequently influenced modern data protection legislation.[89] However, in some ways Convention 108 has been made largely redundant in the European Union by the more expansive and specific data protection legislation introduced since then.

- Article 16(1) of the Treaty on the Functioning of the European Union establishes a specific 'right to the protection of personal data concerning them'.[90] What sets this article apart from the other provisions discussed here is article 16(2), which ensures that compliance with any rules pertaining to the processing of personal data by European Union institutions or member states is subject to the control of an independent authority.
- Article 8(1) of the charter establishes the same right as article 16 TFEU.[91] In Declaration 21, an addendum to the charter, it is noted that legislation specifically oriented towards personal data collection by judicial and police institutions 'may prove necessary'. This codifies a policy by the European Union to have a data protection regime for judicial and police cooperation that is separate from the data protection regime for other situations, which I will come to discuss further below.

[86] (European Convention, 2000), art. 7

[87] Idem., art. 53

[88] (Praesidium of the European Convention, 2007), explanation on Article 7

[89] (Pajunoja, 2017), p.13

[90] (Treaty on the Functioning of the European Union, 2007), art. 16

[91] (Treaty on the Functioning of the European Union, 2007), art.8

3.2 Cybercrime Legislation

3.2.1 Directive 2013/40/EU

Cybercrime legislation in the European Union has been developing relatively quickly under pressure from advancing technologies and the rapid adoption of tools that were initially developed by criminals as weapons of cyber-warfare by governments.[92] The response to this was the implementation of Directive 2013/40/EU (the 'Botnet Directive') which aimed to modernize, expand and harmonize cybercrime legislation in the European Union.[93] The colloquial name of this document makes sense once we start reading the law: botnets and their mitigation are mentioned in three of the preambles.[94] The directive defines five categories of offences, most of which also clearly apply to botnet-related crimes. I will go through the relevant ones briefly:

- 'Illegal access to information systems' (art. 3) is a necessary step for the operation of a botnet that occurs with the installation of malware on a third parties' computer. [95]
- 'Illegal system interference' (art. 4) entails the 'seriously hindering or interrupting the functioning of an information system by [various methods]'; one famous example of this is the DDoS attack, which are of course carried out by botnets.
- 'Illegal data interference' (art. 5) means the deleting, damaging or otherwise rendering inaccessible of data on an information system. This can occur when malware from a botnet damages an information system but will also be an almost inevitable result of any illegal system interference.[96]
- 'Tools used for committing offences' (art. 7) makes illegal the production and sale of computer programs used for committing the crimes listed in article 3-6 as well the sale of passwords, code or similar data used to access an information system without permission. This is a powerful tool for the prosecution of those merely producing and selling the malware used for botnet propagation or fencing stolen data (something which was not clearly a crime in every European jurisdiction: data was not considered full property until relatively recently in the Netherlands for example[97]).

Outside of these five categories of offences the directive introduces a number of tools relevant to botnet mitigation:

- Article 9(3) introduces a new substantive criminalization and increased penalties for cases where a 'significant number' of information systems is affected through the use of tools described in article 7. This article was very much meant to more clearly criminalize botnet operation and propagation, as well as a number of their utilizations such as DDoS attacks.

[92] See chapter 1, p.5-6
[93] (Moise, 2015), p. 376
[94] (European Parliament, 2013), preambles 5, 13, 16
[95] 'Information systems' is a catch-all term in the language of the bill that includes personal computers, smartphones, smart devices, IoT devices, servers and other similar devices.
[96] (Moise, 2015), p.378
[97] (Oerlemans, 2017a), p.351

- Article 9(5) criminalizes using data obtained to gain the trust of a third person, which is a popular phishing method also common in the spreading of malware via infected links.

It should be noted that the law is a directive as opposed to a regulation, and concerns have been raised at the onset of the law about how effective the transposition of the directive into national law would be.[98] After all, the directive's intended effect of harmonization and the subsequent ease of cooperation between national LEAs that was to follow from this will not be achieved if there are substantial divergences in national legislation. Those concerned about this were proven to be only half right. In a 2017 report on the transposition of the Directive into national law the European Commission concluded that the Directive was adopted relatively consistently overall and was accompanied by a streamlining and strengthening of cooperation schemes, just as intended.[99] However it remarked that there was still room for 'considerable scope' for the Directive to reach its full potential, noting that, while new criminalization standards were adopted broadly, there still were discrepancies in the use of definitions and the inclusion of all actions in relation to an offence. To give an example of this, while Article 9(3) was generally implemented very well (a positive development for botnet mitigation), Germany used the language 'information systems which are of substantial importance to one another'. Bots within a botnet do not necessarily have to hold this relation to each other, somewhat defeating the purpose of the bill. Other similar discrepancies can still be found throughout the EU, which might frustrate national investigations and international cooperation.

3.2.2 Directive 2000/31/EC

Some of the most important concepts for European Union digital law are established in article 12 and 15 of 2000/31/EC ('the eCommerce Directive').

- Article 12 to 14 exempt ISPs from secondary liability for information transmitted, cached or hosted on their networks as long as they act as a 'mere conduit' (sometimes referred to as being 'neutral' or 'passive' towards data). This entails that they do not initiate, select the receiver of, or modify the information in any way unless ordered to do so by a court or an administrative authority.[100] This exemption made sense from a practical standpoint: if ISPs were to be held liable for all the content transmitted on their networks they would be either motivated to severely limit their services for fear of being liable, or the technical cost of surveilling their networks appropriately would be prohibitive to operating an effective service. Additionally, the fear for secondary liability could prompt excessive surveillance or censorship from ISPs.[101] At the same time the articles do allow for ISPs to interfere with data on their networks when ordered by a competent authority or when they become aware of unlawful activity themselves.
  However there has been criticism about whether the 'mere conduit' approach is the most effective one, as it can be a perverse incentive that makes ISPs reluctant to adopt more aggressive or effective security policies for fear of violating this 'mere conduit' principle and ending up liable for data transmitted through their networks. There are also questions about

[98] (de Muynck, Graux, & Robinson, 2013), p.9
[99] (European Commission, 2017), p.12
[100] (European Parliament, 2000), art. 12-14
[101] (Sartor, 2017), p.11

how this doctrine reconciles with legislation that facilitates (and often demands) a more active role from ISPs in securing their networks which I will discuss below.[102]

- Article 15(1) prohibits member states from imposing general obligations on ISPs to monitor their information transmission, caching or hosting, nor can they be obligated to actively 'seek facts or circumstances indicating illegal activity'. This is meant to prevent the infringements on the right to private life and data protection that such general monitoring would almost inevitably bring with them. Nonetheless, article 15(2) does allow member states to demand from ISPs that they promptly inform 'competent authorities' when taking notice of illegal activities on their network. They can also be obliged to share information enabling the identification of recipients of their services at the request of competent authorities.

3.3 Data Protection Legislation

Last I will examine the different data protection regimes of the European Union. The EU knows two data protection regimes: one general data protection regime (which consists of the General Data Protection Regulation and the upcoming ePrivacy Regulation) and one for law enforcement (which consists of the Law Enforcement Directive).

3.3.1 General Data Protection Regulation (Regulation (EU) 2016/679)

What is arguably the largest data protection regime (both in scope and the degree of protection it offers) in the world currently was created with the introduction of Regulation (EU) 2016/679, also known as the 'General Data Protection Regulation' or GDPR. It establishes far-reaching rights to data subjects and responsibilities for data processors and controllers.[103]

One of the most important aspects is that this new legislation is a regulation as opposed to a directive. Whereas a directive creates a binding common goal for member states but leaves discretion to individual states as to how to achieve this goal, a regulation is effective immediately for all members.[104] Therefore the GDPR immediately created one common data protection regime for the European Union, avoiding many of the discrepancies between national implementation that might follow directives, something which can be detrimental to effective cross-border cyber policy.[105]

Perhaps the most important aspect of the GDPR is Article 5, which expounds on the practices of good data processing. I will list the requirements most relevant to botnet mitigation here.

- Data must be collected for a specified and explicit purpose and cannot go on to be processed for another purpose (purpose limitation).
- Processing must be adequate, relevant and limited to the purpose specified (data minimization).

[102] (Tjong Tjin Tai, Op Heij, E. Silva, & Skorvánek, 2015), p.158-159

[103] Under article 3 GDPR and article 4 LED, the controller is the party which determines the purposes and means of the data processing. The processor is a party which processes data on behalf of the controller.

[104] (Treaty on the Functioning of the European Union, 2007), art. 288

[105] While EU countries generally have a history of good compliance with and implementation of cybercrime and/or privacy-related legislation, the indirect nature of directives often still presents obstacles that prevent these legislations from reaching their full potential. (European Commission, 2017), p.12

- Data must be kept in a non-anonymized form only for as long as is strictly necessary (storage limitation).
- Processing of the data must happen in a way that is secure and confidential (integrity and confidentiality).[106]

Article 6(1) establishes the prerequisite conditions for lawful processing of personal data. I will also only list the conditions most relevant to this thesis.

- Processing needs to have clear consent from the data subject or be necessary for the performance of a contract.
- Alternatively, it needs to be necessary for compliance with a legal obligation, however Recitals 45 to the regulation have made it clear that this legal obligation must be clear, precise and foreseeable; i.e. data processing is not lawful when mandated through blanket legislation.
- Data processing may also be done lawfully by institutions that are carrying a task out in the public interest or acting in a capacity of official state authority.
- Finally, data processing for the purposes of 'a legitimate interest' to the controller is allowed. Recital 49 specifically mentions that security of network and information systems as well as the prevention of unauthorized access or damage to electronic communication systems are a legitimate interest. Additionally, Recital 50 mentions that the reporting of criminal acts or threats to public security is a legitimate interest. However, it should be noted that Recital 47 mentions that a data controller must always weigh the fundamental rights of data subjects against the legitimate interest, in particular there where 'subjects do not reasonably expect further processing'.[107]
  This last part is of course relevant in cases where information concerning botnet activity is chained from one institution to the other, e.g. an antivirus software company sharing personal information they have with an internet service provider.

Even when these general conditions are met there are additional rights given to the data subject and obligations bestowed on the data controller. Examples of these include the right for the data subject to access their data (article 15) and the obligation for data controllers to implement 'appropriate technical and organizational measures' (article 25). Notable is Article 35, which requires controllers to perform a 'Data Protection Impact Assessment' (DPIA) when they plan on using new technologies to process or collect data. On top of that, cooperation and communication with the national Independent Supervisory Authority (ISA) (articles 31 and 33) are mandated by the GDPR.

Outside of risk management through a DPIA or oversight by an ISA there is one more corrective instrument in the GDPR and that is the mandating of access to effective judicial remedies, which can be done by both ISAs (article 58) and data subjects (article 77-79).

The sharing of personal data between private institutions within the European Union can fall into two categories, both of which are relatively straightforward to comply with if an institution's practices are already GDPR-compliant. The first category constitutes time-limited or one-off sharing, for which

[106] (European Parliament, 2016b), art.5

[107] (Boardman, Mullock, & Mole, 2017), p.10-12

both institutions count as separate data controllers (Article 24 GDPR). The second category entails long-term or perpetual cooperation, during which both institutions will become joint controllers (Article 26 GDPR). The only significant difference for this analysis between these two constructions is that the joint controllership mandates more detailed documentation for the tasks and responsibilities of each party in regards to the processing.

3.3.2 Relevant Exceptions and Restrictions

- Article 2(2) clarifies where the regulation does not apply, which is for activities outside the scope of Union law (such as national security[108]), activities by member states relating to the common foreign security policy of TEU or the processing of personal data by competent authorities for the purposes of law enforcement. Especially in the latter example this might involve botnet mitigation for the purposes of a criminal investigation, while for example routine network maintenance (i.e. for the performance of a contract) would not meet this threshold.
  To add to this, article 2(3) states that the regulation shall be 'without prejudice' to 2000/31/EC, specifically mentioning the liability rules established by article 12-15 of that directive. Legal scholars assume that this article is to be read as saying that liability for user content for ISPs will still be governed by 2000/31/EC but that data processing by ISPs will fall under the GDPR. However, the exact delineation between these two laws is as of yet still not completely clear.[109]
- Article 23 allows for member states to restrict the right to data protection if taking care to respect the 'essence of fundamental rights and freedoms' and ensuring that these measures are 'necessary and proportionate'. We can see this wording is very similar to that used by the ECtHR and CJEU. These legitimate interests are almost all related to national security, defense and public security, but also include 'other important public interests, in particular economic or financial interests' such as taxation policy.[110]
- Article 89(1)(2) allows for scientific, historical or statistical research on data that does not permit anonymization or even pseudonymization as long as appropriate safeguards are in place.

3.3.3 ePrivacy Regulation

Much of the ePR proposal deals with subjects that are not entirely relevant to botnet mitigation such as cookie provisions, and the proposal has been criticized for overlapping too heavily with the GDPR to have a large impact on privacy regulations.[111] However, the main difference in scope between the two treaties is twofold.

- Firstly, the protections of the GDPR only extend to natural persons whereas the ePR per its article 3 also covers legal entities, something which could become relevant in the future

[108] (Boardman et al., 2017), p.3

[109] Idem.

[110] Idem, p.61

[111] See chapter 5, p.42

because it extends certain protections for machine-to-machine (M2M) communication. [112] This would apply to IoT devices communicating with each other and these devices have become popular targets for botmasters, as discussed in chapter 2.

- Secondly, the GDPR covers the processing and transmission of personal data while the ePR per article 2(1) applies to 'electronic communications data' carried in the provision of electronic communication services. This means that the scope of the ePR is narrower since it only applies to those providing 'electronic communication services' such as ISPs, email hosting companies and electronic messenger companies like WhatsApp or Facebook.[113]
- In article 4 the ePR divides electronic communications data into 'content' and 'metadata'. Content being 'text, voice, videos, images and sound' where metadata includes the information 'used to trace and identify the source and destination of a communication, data on the location of the device generated in the context of providing electronic communication services, and the data, time, duration and the type of communication.' While the former is unlikely to be used in botnet mitigation the latter definitely is and this is something that should be considered when looking at future botnet mitigation methods.

The ePR provides different levels of protection for content and metadata, for this thesis I will only look at the protection offered to metadata collection and processing.

- Article 5 features a general prohibition on interference with electronic communications data (following 2000/31/EC), where after it lists exceptions to this in Article 6. The most powerful of these exceptions is Article 6(1)(b), which allows for processing of data if it is necessary to the maintenance or restoration of security of the electronic communications network or device.
  Additionally, the processing of metadata is allowed under article 6(2)(b) for, among other things, the prevention of 'fraudulent or abusive' use of the service. A convincing argument can probably be made that both these exceptions would apply for botnet mitigation methods.

When it comes to the subject of botnet mitigation the ePR seems to provide much of the same rights and responsibilities as the GDPR does, although some of its developments, such as the extension of protections to M2M communications, could proof problematic in the future. Finally, it should be observed that the text studied here is a proposal version, although it is not thought likely to be substantially altered before likely being adopted somewhere in 2019.[114]

3.3.4 Directive (EU) 2016/680

The European data protection regime for law enforcement is somewhat different in nature than the general data protection regime. It is established through Directive 2016/680 on data protection in the police and criminal justice sectors (LED).

- Article 2(1) declares the scope of the directive as applying to 'competent authorities involved with the prevention, investigation, detection or prosecution of criminal offences or the

[112] Something which legal scholars have warned about is that this new extension will create uncertainty as to who needs to provide consent to data collection in some scenarios: the legal entity, natural person or both? (Zwenne, Kroes, & van Eymeren, 2018), p.36

[113] (Emma-Iwuoha, 2017).

[114] Idem., p.4

> execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.'[115]

While one might have an intuitive image of what 'competent authorities' entail, in practice the directive has been criticized for its unclear delineation as to what this constitutes. For example, Mireille Caruana has stated in an analysis on the law that '[i]t is unclear to what extent, if at all, processing of data generated by airline companies, **telecommunications operators** and financial institutions falls to be regulated by Directive 2016/680' (emphasis added).[116] This is somewhat clarified by Recital 11 to the law stating that 'a body (…) which processes personal data on behalf of such [competent] authorities (…) should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive (…).' It can therefore be argued that these organizations do fall under the scope of the directive (as processors) when processing or collecting data for competent authorities when bound by a contract or other legal act, and that actions outside of that are governed by the GDPR. However this interpretation has not been clarified by the legislator or tested in front of a judge as of writing, so the exact delineation between the LED and the GDPR still remains uncertain.[117]

- Article 47 also institutes an Independent Supervisory Authority (ISA) as supervisory bodies. While these do not expressly need to be the same as the ISA instituted for the GDPR it is expected that most countries will have one body supervise both the regulation and the directive.[118] The power of these ISAs is limited when compared to the GDPR, though. Unlike the GDPR the ISA under the LED has no power to impose fines or penalties, cannot suspend data flow to third countries or organizations, have very little investigative powers and cannot order a controller/processor to comply with data subject requests for erasure/deletion/rectification. The most powerful corrective tool ISAs have (and this is not insignificant) is that they are allowed to issue a temporary or indefinite limitation or ban on processing. [119]
- DPIA's (as part of 'prior consultation' with the ISA) in cases of automated processing with a high risk factor are necessitated by article 28, and ISAs need to be consulted on legislation being drafted that is in regards to the automated processing of data by law enforcement.[120]

Finally, the transferring of personal data by law enforcement bodies is subject to the LED and follows the same general principles as the GDPR. The controller/joint controller distinction is the same in both pieces of legislation, including the requirement of an arrangement between the joint controllers (Article 19 and 21). Law enforcement will have to show under Article 8(1) LED that the sharing is necessary for the pursuit of an investigation.

[115] (European Parliament, 2016a), art.2
[116] (Caruana, 2017), p.6
[117] (Caruana, 2017), p.7
[118] Idem., p.11
[119] Idem., p.12-13
[120] Idem., p.13

3.4 Conclusions for Chapter 3

We can find from the above overview that the legislation pertaining to botnet mitigation in the European Union is relatively modern: most of it is less than a decade old. Probably in part because of this fact, I find that a lot of the legislation has been developed with an eye towards the needs of botnet mitigation and cybersecurity efforts. Examples of this can be found in Directive 2013/40/EU (the Botnet Directive), which explicitly attempts to criminalize behaviors related to the operating and propagation of botnets, and the current law enforcement data protection reform, which has relaxed rules for transfer to third parties, likely to aid with cross-national cybersecurity efforts. At the same time we see that rights for data subjects and responsibilities for data controllers/processors have been expanded greatly under the GDPR and ePR. However, both of these legislations offer certain derogations in case of legitimate interests for the data controller. In chapter 4 and 5 I will examine what the effect of this new data protection regime is on the botnet mitigation efforts discussed in chapter 2. Finally, we see that cybercrime legislation imbues operators of essential services with certain rights and responsibilities that seem somewhat contradictory at times. These operators are both required to secure and monitor their networks to the best of their abilities and to remain a mere conduit to the data on their networks, something which seems to be somewhat mutually exclusive. I will discuss this problem further in chapter 5. First however, I will examine the positive effects of the European Union legislative framework on botnet mitigation in the next chapter.

Chapter 4: Positive Effects of the EU Legislative Framework

In this chapter I will attempt to examine the positive impact of current European legislation on botnet mitigation. This will be done by analyzing the likely effects the legislative framework discussed in chapter 3 will have on the botnet mitigation methods described in chapter 2.

After general observations on the legislative framework, the methods discussed in chapter 2 will be divided here into two categories: a 'technical' and a 'procedural' one. The technical category concerns the methods deployed to detect botnets. The procedural category concerns what parties are involved, in what ways these parties cooperate, and how data is shared between them. The methods are categorized in this way because, while both categories are majoritively affected by the same legislation, we will see in chapter 6 that addressing any conflicts between the methods and existing legislation requires different approaches. Therefore it is sensible to categorize the methods along these lines so we will have a clear delineation between the two when it comes to proposing solutions to any problems encountered.

4.1 General Observations

4.1.1 General Framework

The European Union has a framework with elaborate clarification from judicial review underlining (and in some cases predating) its data protection regime. Article 8 ECHR (and Article 7 of the charter) regarding respect for private and family life is well-defined with clear jurisprudence by the ECtHR as to what it encompasses and when exceptions are allowed. Importantly, the ECtHR has treated the ECHR as a 'living instrument which should be interpreted according to present-day conditions', meaning the courts have generally been very well able to incorporate new technological developments into the application of these articles.[121] This combination of a clear legal interpretation creating normative standards for member states and a dynamic approach to changes has created an influential legal framework regarding data protection.[122] This influence of the ECtHR is due to a number of factors (e.g. positive public reputation, an expansive interpretation of the Convention) and the Court has been referred to as 'without exaggeration (…) the world's most effective international human right's tribunal.'[123] The result of this is that jurisprudence on article 8 ECHR has had, and is continuing to have, a significant contribution to the strength of data protection rights in the European Union.

These rights have been further expanded under the EU general framework, namely through the codification of data protection as a specific right (separate from a right to privacy) by way of Article 16 TFEU/Article 8 of the charter. This is significant because this development ensures that the right to privacy no longer needs to be awkwardly retrofitted by the judiciary or claimants to fit a right to

[121] (Lawson & Schermers, 1999) , p.50
[122] (Oerlemans, 2017b), p.69
[123] (Helfer, 2008), p.126

data protection.[124] This has certainly been achieved more or less successfully up to this point (as illustrated by the ECtHR), something which is not altogether remarkable considering the overlap between the two rights in many situations. However, the volume of data processed is predicted to grow at an exponential rate from here on out, and will be processed and interacted with in ways that we cannot yet accurately predict. This will require to either keep expanding the definition of the right to private and family life, as the ECtHR is likely to do, until it perhaps reaches a breaking point or to particularize data protection as a fundamental right, as the European Union has done.[125] When keeping an eye on the future, I believe this to be a pertinent development in data protection legislation.

4.1.2 Data Protection Regime

The General Data Protection Regulation and legislation using the same principles have transformed data protection rights for citizens in the European Union, offering protections and tools for redress that are relatively wide-ranging. Whereas the original 1995 Data Protection Directive was already considered by many to be one of the strongest data-protection regimes on Earth (establishing many principles of lawful processing, oversight and redress still present in the current data protection regime), the GDPR has taken steps to improve on this even further.[126] Key among these are the many additional and modernized prerequisite conditions established for the lawful processing of data and the additional and clarified remedies and rights (such as the right to correct your data and the right to be forgotten) bestowed upon data subjects.

In addition to this is the harmonization it achieves in numerous ways, which is arguably the most important feature of the GDPR. Implementation obstacles are of course still present to some extent with Regulations (given the sovereignty of member states and the possibility of legislation being interpreted and applied differently by individual states), however the transposition from the EU-level to the national one is definitely eased by the clarity and harmony that a Regulation offers.[127] Although a comprehensive analysis about the degree to which the GDPR achieves harmonization falls outside of the scope of this thesis (and can likely only be accurately assessed a few years onward), it can be generally agreed upon that the GDPR takes steps toward a harmonized data protection regime.

Looking further than the GDPR, harmonization is achieved through policy, namely the treatment of the GDPR as foundational legislation beyond its original scope, which has led to much of its terminology and protections carrying over to other legislation. A good example of this is Directive 2016/680 (LED), which borrows large sections of the GDPR, down to the precise wording of certain sections. Data Protection Impact Assessments, access to legal remedies for data subjects and even the structuring of the law being near-identical to the GDPR shows a commitment from the European Union to a uniform vision for data protection across multiple sectors (civil and law enforcement) of society, which can strengthen implementation and internalization of this framework. Not all legislation follows this model however (notably, the ePrivacy Regulation utilizes slightly different

[124] (de Hert, 2015).
[125] (Hijmans, 2016), p.65
[126] (de Hert & Papakonstantinou, 2016), p.193-194
[127] (Caruana, 2017), p.4

terminology and approaches to data protection), and it of course remains to be seen if and how these principles will be carried over to coming data protection laws.

Nonetheless, it is probably safe to assume that the data protection regime in the European Union has not only gotten more substantive, but also more harmonized across countries, something which is generally agreed upon to 'increase legal certainty and predictability of norms in these distinct sectors [where harmonization has taken place].'[128] The net result of these developments is a stronger data protection regime for EU citizens.

4.1.3 Desirability of a Strong Data Protection Regime

At this point there is one obvious question that is being raised, and that is whether a strong data protection regime can be said to have a positive effect on botnet mitigation in the first place. After all, an argument can and has been made that data protection prevents optimal approaches to botnet mitigation, especially when it comes to monitoring and tracking of botnets and their masters.

It has been said by Tjong Tjin Tai et al. that 'cybercrime is the price we pay for our principles', reasoning that a society which wants an open and private internet will inevitably have to allow for more cybercrime because the conditions for said internet require restrictions on investigative methods performed on networks.[129] One example of this is researchers struggling with the added time and cost investment related to receiving consent for their data collection, or alternatively, with obtaining usable research data after anonymization for situations where consent is difficult to receive, such as large-scale passive data collection.[130] An even more critical example can be found in the position of ISPs, who are widely regarded as being 'natural control points' against botnets and who, as some of the largest victims of botnet activity, should be naturally incentivized to actively address this problem.[131] Unfortunately presently ISPs are in some ways disincentivized to fight botnets to the full extent of their abilities. One of the reasons for this is that restrictive privacy and liability legislation gives ISPs little in way of discretion when it comes to monitoring network security.[132] This, when accompanied by increasingly large penalties for non-compliance, has caused these companies to err on the side of caution when balancing privacy and security, resulting in keystone actors not acting effectively against botnets on their networks.[133] This example clearly shows how in protecting one set of rights (privacy, data protection) other commonly shared interests (network security, end-user safety) may get compromised to an extent that is ultimately undesirable. I will explore these problems more in-depth in chapter 5, but it serves here as a clear illustration of the negative effect privacy legislation can have on botnet mitigation.

Nonetheless, while I would generally agree that privacy and security are often balanced against each other and might be exclusionary at times, I would say that Tjong Tjin Tai et al.'s view is a somewhat pessimistic and narrow one. Leaving aside well-trodden normative arguments for why privacy- and data protection ought to be considered a general priority, we should not lose sight of the ways in which a properly constructed data protection regime might also be conducive to botnet mitigation.

[128] (Hugenholtz, 2013), p.65

[129] (Tjong Tjin Tai et al., 2015), p.164

[130] (John et al., 2010), p.6

[131] (Eeten et al., 2010), p.10

[132] Other factors include such disincentives as customers not valuing network security in their purchasing decision and the technical complexity (and therefore, initial costliness) of botnet mitigation. (Eeten et al., 2010)

[133] (Tjong Tjin Tai et al., 2015), p.163-164

In fact, during the initial review stages of the GDPR it has been argued by Maria Grazia Porcedda that good privacy and data protection legislation 'may be more a support than an obstacle [to solving the problems of cybercrime], contrary to the zero sum game depicted by the classic dichotomy.'[134] She puts forward the idea that data security is often an explicit goal of cybersecurity, and that it is therefore helpful to think about privacy- and data protection as an integral part of cybersecurity instead of one separate or opposed to it. Doing this, she argues, will make it easier to craft legislation which facilitates cybersecurity (e.g. by harmonizing good data collection practices for investigations) or at least better accounts for the interests of cybersecurity, without losing sight of the balancing that is sometimes necessary between conflicting interests.[135] Good privacy- and data protection legislation therefore compliments and particularizes cybersecurity legislation, exactly because the two fields are very much convergent. One interesting thing to note is that this vision of privacy and functionality as complimentary instead of dichotomous is a core tenet of so-called 'Privacy by Design', which is the heuristic approach to privacy protection adopted by (among others) the European Union.[136]

Moreover, this is a line of argumentation which in my opinion can be extended towards the recently introduced data and privacy legislation in the European Union. To use Porcedda's framing: while the new legislation does create some unwanted or unnecessary obstacles (which I will come to discuss), it also supports cybersecurity efforts in a number of ways. Chief among these being that harmonization in the long term should serve to decrease confusion of actors as to what investigative methods are permissible, which in turn should decrease the reluctance of these actors to take decisive action.[137] As mentioned, one contributing factor to current inaction is the adoption of an overly cautious approach towards cybercrime out of fear for the large penalties associated with non-compliance with privacy legislation. Clear and widely adopted guidelines will reassure actors wanting to invest in cybercrime-prevention techniques as to what their exact options and tools are. The embeddedness of ISA's and DPIA's in the EU's privacy legislation is a positive factor in this regard, ensuring that parties have an authoritative source to turn to when legislation needs specifying or final interpretations need to be made. The size and scope of the data protection regime could have an accelerating effect on this harmonization because knowledge on privacy and data protection will better translate across the European Union, meaning actors will have a larger quantity of high quality sources on best practices, considerations, etc. related to botnet mitigation to gather from before deciding on a course of action. This will reduce cost and risk for parties that are interested in botnet mitigation and who might currently find that there is simply too much uncertainty surrounding certain investigation techniques to actually follow through on this interest. All-in-all, the harmonization and specification of privacy and data protection legislation might have certain compounding effects that ultimately will prove beneficial instead of harmful to botnet mitigation in the European Union.

Through these examples I have hoped to illustrate that, if we choose to value privacy and data protection highly (and the EU has affirmed in words and actions that this is indeed the case), we should elect to approach it as an integral part of cybersecurity instead of as an element antagonistic

[134] (Porcedda, 2012), p.67
[135] Idem., p.67-69
[136] (Cavoukian, 2009), p.3
[137] In the short term this effort was obviously less successful: especially the introduction of the GDPR was accompanied by a large amount of confusion for citizens, the private sector and even governments. (Ismail, 2017).

to it. These two interests do not inevitably have to be solely at odds with each other and might in fact contribute to one another's strength when interwoven correctly. Of course, much is dependent on how successful the GDPR will actually be in achieving its goals of increasing harmonization and clarity, which is something that will not be entirely clear in the immediate future. Lastly, we should also not be naïve about the problems data collection and privacy regulation might introduce for those interested in botnet mitigation: not all privacy legislation will be conducive to cybersecurity and, as I will come to discuss, legislators can certainly do a better job of creating an environment where actors have more discretion to take steps towards botnet mitigation (without necessarily having to compromise on privacy).

4.1.4 Cybercrime Legislation

Cybercrime legislation is an area which the European Union has attempted to harmonize and modernize on an EU-level over the last decade, something which is sensible given the cross-national aspects of cybercrime and its growing threat level. The main goal of these modernizations was to properly criminalize certain practices that had developed in the area of cybercrime which were not properly addressed in the laws of member states. Finally, the EU hoped to ease and promote cooperation between national law enforcement bodies through harmonization and modernization of the EU-level legislation.[138]

One contributor to achieving these goals in the field of cybersecurity was Directive 2013/40/EU, also known as the Botnet Directive. When compared to its predecessor (Council Framework Decision 2005/22/JHA) there are relatively few radical substantive changes.[139] Nonetheless, there are some new elements included that are beneficial to botnet mitigation. Article 9(3)'s criminalization of large scale computer interference enables prosecutors to specify the operating and propagating of a botnet, as well as many of its utilizations such as DDoS attacks, as a stand-alone crime; one that is in addition to the crimes that are concurrent with running a botnet (illegal data interference, illegal access to information systems, etc.) but do not really encompass the full extent of its harmful nature. This will allow law enforcement and prosecutors to build a more accurate legal argument when prosecuting these cases, as well as enable judges to more easily punish those running an extremely dangerous botnet differently than criminals who 'merely' hacked into a number of computers, reflecting the issue of Botnets as a unique danger that is in many ways separate from other forms of cybercrime more accurately. Furthermore, article 7 and 9(5) criminalize behaviors which are associated with the operating and propagating of botnets (fencing stolen data and using stolen data to gain the trust of a third party), something which again will make it easier for law enforcement to accurately prosecute these actions.

Apart from these new additions we can find that the offences which are (mostly) carried over from the previous Framework Decision listed in article 3 and 7 of the Directive pretty comprehensively criminalize the propagation of Botnets. Article 3 criminalizes 'illegal access to information systems', which a botnet by its very nature has to engage in through the spreading of malware and this will necessarily entail illegal access to an information system, whether this is through drive-by-download, infected media or social engineering. Article 7, aside from criminalizing the aforementioned fencing of stolen data, criminalizes producing and selling the tools necessary for crimes described in Article 3-

[138] (Moise, 2015), p.375
[139] (Beales, 2014).

6. This includes the malware to propagate botnets, but also the software to operate the botnet with. In light of the large market of vendors who merely distribute malware and botnet software without necessarily running one themselves, this is an important distinction to make.[140] I find here that both stages of botnet propagation, i.e. creating the malicious software necessary as well as the actual infecting of information systems with the bot binary, are criminalized under EU law.

Lastly, some behavior of botnets is also criminalized in this directive albeit less comprehensively; this is not strange to think when we consider that all botnet propagation involves illegal access to information systems while the ultimate botnet behavior may vary widely from botnet to botnet, and is therefore harder to criminalize with what is to be a general-purpose directive. Article 4 (hindering or functioning of an information system), Article 5 (illegal data interference) and Article 9(3) (large scale system interference) combine to form a very comprehensive criminalization of DDoS attacks, which hinders the functioning of servers or networks (article 4), thus rendering data on a server inaccessible (Article 5) on a very large scale (Article 9(3). Additionally, Article 5 criminalizes certain bot binary behaviors, which often have the (not always intended) side-effect of deleting, damaging or moving of data on the information systems that they occupy.

On the whole the Botnet Directive is a step in the right direction towards adequately criminalizing behavior related to botnet propagation and operation. One footnote that could be placed here is that, as law enforcement increasingly moves from prosecuting cybercrime to 'disrupting' it, the positive effects of more accurate criminalization of cybercrime, especially when it comes to botnet mitigation whose offenders often reside outside of the EU, will probably diminish somewhat.[141] This move towards disruption will be discussed in more detail in chapter 5. Of course, just because the positive effect of accurate criminalization is diminished does not mean that it is not present at all, and we should be careful to adopt an overly defeatist attitude when it comes to legislating for cybercrime: comprehensive and harmonized cybercrime legislation has been argued to have a knock-on effect, making it both easier to investigate and prosecute legislation nationally as well as increasing cross-national cooperation.[142]

Finally, while it falls somewhat outside of the scope of this thesis, it should be noted that the European Union has a number of initiatives and bodies which attempt to increase harmonization of law and cooperation between law enforcement bodies through other means than purely legislation. Examples of these include the European Union Agency for Network and Information Security (ENISA) which attempts to harmonize practices across member states among other things through the installation of an EU-wide CERT in 2011, and Europol's 2013 instituting of a dedicated European Cybercrime Centre which coordinates cross-national cooperation between law enforcement.[143] One other notable example apart from European Union is the Council of Europe's efforts to harmonize cybercrime legislation and cooperation on a global scale, using the 1981 Convention 108 as a basis.[144] This should serve as a reminder that harmonization cannot be achieved through legislation alone, but is equally (and likely even more) so a matter of political willingness, cooperation and coordination.

[140] (Burghouwt, 2007), p.4

[141] (Oerlemans, 2017b), p.363

[142] (UNODC, 2013), p.77

[143] 'CERT' stands for Computer Emergency Response Team, which are expert groups that quickly respond to cybersecurity threats.

[144] (Koops & Goodwin, 2014), p.83

4.2 Technical Aspects

The most important factor that we must look at when examining the feasibility of botnet detection methods (described in chapter 2) under European Union law is whether the collection of data necessary for these techniques is compatible with current data protection legislation.

As it stands, I find that the legislation generally attempts to facilitate the needs of actors interested in botnet mitigation. The primary method is through allowing private parties to process personal data where they can claim a legitimate interest (article 6(1) GDPR) as a legal basis. According to an analysis by Silva and Coudert, a good argument can be made that much processing for the purposes of botnet mitigation falls under this.[145] Of course, the legitimate interest claimed depends on the party involved, as well as the exact nature and purpose of the processing.[146] Examples of relevant legitimate interests they give are that of parties fulfilling a contractual obligation (article 6(1)(b) GDPR) or complying with a legal obligation (article 6(1)(c) GDPR).[147] They also note a number that the legitimate interests of a task carried out in the public interest or in the exercise of official authority vested in the controller (article 6(1)(e) GDPR) can be claimed but likely very narrowly, since they find it unlikely that anyone other than semi-governmental institutions (such as CERTs) would meet this threshold.[148] Recital 49 GDPR also mentions the security of network and information systems as a legitimate interest. Finally, Article 89(1)(2) GDPR allows for scientific research even when the data cannot be anonymized or pseudonymized.

Of course, even with a legitimate interest parties still need to observe the relevant principles laid out in article 5 GDPR and take certain precautions (such as the performance of a DPIA where required by Article 35 GDPR). Notably, the data processing needs to be proportional to the goal it aims to achieve. This could for example mean that in a situation where analysis of flow records prove sufficient for botnet detection, the method of packet inspection (which carries a lot more privacy risks with it) would be considered unnecessarily intrusive and would therefore not be allowed.

A legitimate interest does furthermore not mean that every method described in chapter 2 is automatically allowed. For example, it has been argued that honeypots, given their high risk of collecting large amounts of personal data, would generally not be available to anyone but law enforcement, researchers, or perhaps semi-governmental institutions, even where there is a legitimate interest.[149]

In the case of law enforcement (or authorities processing data on their behalf) legislation allows them to process personal data in the pursuit of an investigation (article 8(1) LED). Of course here too certain practices need to be observed, which are laid out in article 4 LED, and precautions such as a DPIA where there is a high risk of collecting sensitive data (article 28 LED) need to be taken.

The fact that botnet detection methods can be included as a legitimate interest in many cases supports the idea put forward earlier that a strong data protection regime and effective cybercrime

[145] (E. Silva & Coudert, 2014), p.36
[146] It should be noted that Silva and Coudert´s analysis looked at botnet detection under the 1995 Data Protection Directive, however it has been argued that their analysis still is relevant to the GDPR. (Cormack, 2016), p.267
[147] (E. Silva & Coudert, 2014), p.38
[148] Idem., p.39
[149] (Cormack, 2016), p.268

legislation do not necessarily have to be mutually exclusive. In practice however there is still a large grey zone surrounding the legality of much of the data processing related to botnet mitigation. This is something which I will further discuss in chapter 5.

4.3 Procedural Aspects

This section will discuss the positive aspects of current legislation on the procedural aspects of botnet mitigation, focusing mainly on the cooperation and the transferring of data between involved parties (both public and private).

As discussed in chapter 3, the transfer of personal data between private institutions or by law enforcement is relatively straightforward if these institutions already comply with data protection legislation. This is very important to botnet mitigation because of the complicated nature of this mitigation. As botnets grow more and more sophisticated, we can see a trend developing towards the involvement of a larger number of players with the detecting, mapping and disrupting of these networks. Furthermore, the LED accounts for the role of private parties in public investigations through Recital 11, which states that private parties can process data on behalf of a 'competent authority' as long as there is a contractual or legal basis for this cooperation. This means that private parties can process personal data under Article 8(1) LED and would presumably fall under the law enforcement data protection regime while doing so.

For the purposes of botnet mitigation this is obviously desirable and a positive aspect of the law. However from a data protection perspective this practice still raises a number of questions, seeing how weak oversight and unclear delineation between data protection regimes might lead to purpose creep and the neglect of good practices. This is something which I will discuss further in chapter 5.

As we can see, the text of the law provides all major parties involved with the competencies they need to share data for the purposes of botnet mitigation, as long as good practices are observed. While this does by no means is meant to indicate that the legislation in place is flawless or without negative consequences (which is something I will examine in chapter 5), it does mean that the law facilitates the needs of those interested in botnet mitigation very well from a procedural standpoint.

4.4 Conclusions for Chapter 4

In concluding this chapter, I believe it is safe to argue that the text of the law was developed with attention to the modern needs of botnet mitigation, despite the fact that data protections having gotten more substantive. The key takeaway is that parties involved with botnet mitigation also have to observe certain good practices with regards to data processing if they want to be in compliance with the law. In this way the legislation still allows for cybersecurity efforts while also improving the protection of data subjects, supporting the theory that these two elements do not have to be mutually exclusive. Botnet mitigation is of course dependent on much more than just privacy and data protection legislation, and it finds itself supported by cybercrime legislation that criminalizes behaviors related to botnets. Nonetheless, I find that the legislation still has a number of unintended consequences, posing a risk to both botnet mitigation and certain fundamental rights. I will examine these in the next chapter.

Chapter 5: Negative Effects of the EU Legislative Framework

In this chapter I will examine the negative impact of current European Union legislation on botnet mitigation. Mirroring the approach used in chapter 4, this impact will be estimated by analyzing the likely effects the legislative framework discussed in chapter 3 will have on the botnet mitigation methods described in chapter 2. The grouping of the subjects discussed into 'general', 'technical' and 'procedural' categories will likewise be the same as in chapter 4. One deviation from the template used in chapter 4 is the inclusion of not only negative effects *on* botnet mitigation produced by EU legislation but also of a negative effect produced *by* EU legislation itself. This effect, which I refer to as 'black box botnet mitigation', does not necessarily negatively impact botnet mitigation; in fact it might benefit it in some ways. However, the potential negative societal impact it might have, especially from a privacy and data protection rights perspective, warrants its inclusion in this chapter.

5.1. General Observations

The legislative framework for privacy, data protection and cybersecurity establishes the foundation that much of botnet mitigation is built on: therefore it stands to reason that any weaknesses in this framework will weaken the entire process of botnet mitigation.

5.1.1. Data Protection Regime – Uncertainty and the Chilling Effect

The downside to a reform on the scale of the GDPR is that where the legislation has left vacuities or uncertainties, especially when combined with large fines for non-compliance, a so-called 'chilling effect' can occur. This refers to a phenomenon where actors are reluctant to engage in certain activities for fear of being in violation of the law.[150] Any uncertainties about legislation do not necessarily have to originate in the body of the text, either: misunderstandings can also occur during the implementation of the legislation.

In the specific instance of actors involved with botnet mitigation, one might assume actors already primarily working in an IT-field are better equipped to handle data security than most. They could therefore suffer less from the chilling effect described above. While this claim seems to make some sense intuitively unfortunately no data could be found that researches the impact of the data protection reforms per sector. It is also likely that too little time has elapsed since the implementation of these reforms for an accurate image to be formed on this matter. However one thing that is certain is that IT-related services are being impacted by the GDPR at least to some degree, with one analyst noting that IT-security businesses face a number of insecurities surrounding the GDPR and have to divert resources away from their core business to ensure compliance, at least temporarily.[151]

[150] (Hudson, 2017), p.1
[151] (Garber, 2018), p.15

I believe the insecurity surrounding the data protection reform can be attributed to two factors. The first factor is the open-endedness of much of the data protection legislation: the GDPR isn't very prescriptive in what methods constitute good data processing, giving only a handful of explicit suggestions (e.g. pseudonymization) in the entire text. This encourages multiple interpretations of the law to arise initially, increasing confusion for actors. This open-endedness is a deliberate design decision. The idea behind it is that a focus on the philosophy of data processing as opposed to on an explicit list of data processing requirements ensures the legislation is future-proof, avoids a 'tick-box' mentality, and inspires a more holistic approach to data processing by the involved parties.[152] While I personally agree with this approach to legislating a field that is as quickly evolving as data protection, we should not be blind to the downside of this approach, which is exactly the absence of an easy-to-follow list of boxes to tick for compliance. Especially in the short term (when there is a dearth of established practices) this will lead to more confusion and therefore to more reluctance to act for involved parties.

When it comes to botnet mitigation it is not difficult to find instances where the legislation has left matters non-prescriptive. To give an example, it stands to reason that to adhere to the principle of data minimization any personal data collected will have to be deleted once it is no longer needed.[153] However, these tenets will need to be inferred initially, are often highly situational, and will invariably meet questions that do not have a clear-cut answer. For example, at what exact moment is data no longer needed? One other example of this can be found in the 'weighing the rights of the subject against the legitimate interest of the controller' that controllers are expected to do in a DPIA. In practice this of course is a highly specialized and difficult task that has to take into account many variables if to be done correctly, for which the GDPR provides very little prescriptive guidelines. One final example is that of anonymization, which is actually a prescriptive data protection method introduced by the GDPR. Nonetheless, still much uncertainty exists as to what constitutes good *enough* anonymization for it to be considered GDPR compliant.[154]

The second factor has been mentioned already, and that is the uncertainty surrounding the data protection reform for actors. As pointed out, even in areas where a scholarly consensus forms as to what constitutes good practices a chilling effect can occur when actors are ill-informed about what is permitted under the law.

Some of the confusion and uncertainty surrounding the current data protection reform is likely unavoidable; no reforms are completely frictionless, after all. Much of the confusion as to what constitutes good data processing practices will dissipate as scholarly and industry consensus arises over time. The European Union hopes to speed up this consensus-building through Independent Supervisory Authority (ISA) oversight and EU-level coordination efforts such as the European Data Protection Board. Furthermore, information about best practices can more easily be shared between actors across borders as the data protection regime harmonizes further.[155] However, some areas will have to be addressed by the judiciary or national legislation, and it is here that we see larger obstacles to botnet mitigation develop. Firstly, it seems likely that in these high-uncertainty areas actors will be especially reluctant to utilize the tools at their disposal as long as no final ruling has

[152] (Mansfield-Devine, 2017), p.16-17
[153] (Dougherty, 2017), p.10
[154] (John et al., 2010), p.9
[155] See chapter 4, p.33

been made, which will hurt botnet mitigation. Secondly, there is a risk of divergence between the judicial interpretations or national legislation of member states. This would hurt the harmonization efforts of the data protection reform and subsequently frustrate botnet mitigation techniques or cooperation between law enforcement agencies, which are often highly dependent on cross-border cooperation. While identifying these exact areas goes beyond the general analysis provided by this thesis, one example that could be given is the current uncertainty surrounding the use of anonymization and pseudonymization techniques. As mentioned in chapter 4, it is currently unclear what degree of anonymization and pseudonymization will meet GDPR standards for any given situation involving botnet mitigation. It is likely that situations like this will need to be further clarified through judicial interpretation or national legislation. However given the highly technical nature of these techniques and the large moral grey area surrounding much of the issues concerned (meaning there is no one 'natural' consensus for actors to arrive at) member states may arrive at very different answers to these questions, unless a coordinated effort takes place to prevent this.

The above discussion focuses on the effect of uncertainty on non-law enforcement actors. In the case of law enforcement I believe this chilling effect is likely to be diminished. The main reason for this is that contributors to this effect are uncertainty about the law and fear of reprisal.[156] It stands to reason that law enforcement agencies (or other competent authorities) have shorter lines of communication between them and regulatory agencies, which could lead to a reduction in uncertainty. Additionally, the GDPR imposes the possibility of high penalties for non-compliance of up to €20 million or 4% of annual worldwide turnover, whichever is highest (article 83 GDPR) and ISA's have wide-ranging investigative and corrective abilities. These penalties are absent in Directive 2016/680 and the corrective measures of ISA's are severely limited: they lack investigative powers, for example. Less severe penalties and oversight combined with the aforementioned higher information level among law enforcement agencies I believe will add up to make this group less reluctant to act when compared to non-law enforcement actors.

5.1.2. Data Protection Regime – ePR

One final aspect of the data protection regime which might have an adverse effect on botnet mitigation is the proposed ePrivacy Regulation (ePR), which is a good example of the ways in which the current regime, despite substantial steps forwards, still isn't fully harmonized. Firstly, there is considerable discussion about the necessity of this regulation, seeing how it heavily overlaps with the GDPR. One of the main purposes of the ePR (recital 5 ePR) is to complement and particularize the GDPR where necessary, something which is perhaps desirable given the uncertainty left by the open-ended nature of the GDPR (described in the previous section). However, in its recent state the proposal fails to introduce many particularizations relevant to botnet mitigation, with the principal additions being the inclusion of legal entities in its data protection regime and its metadata/content distinction.[157] While these additions are not entirely irrelevant, the proposal largely seems to opt for restating principles already covered by the GDPR.

This was also the general conclusion from a 2018 study done by Zwenne et al., which stated that 'where the ePR intends to add or deviate from the GDPR, it does not actually always do so', and that

[156] (Hudson, 2017), p.2

[157] For a more extensive discussion of this legislation see chapter 3, p.26

the two laws 'heavily overlap'.[158] I will introduce a number of examples of this overlap between the two laws that they found.

The ePR is meant to particularize the protections of personal data in electronic communications, but the vast majority of electronic communications are between individuals, a class protected by the GDPR already.[159] This alone makes the ePR overlap heavily with GDPR. One other example is that the ePR adds stipulations that processing is only allowed where otherwise not possible with anonymous data or without the processing of content (article 6 ePR), but these are just rephrasings of the data minimization principle found in the GDPR (article 5). Finally, the ePR's general prohibition on 'interference with electronic communications' (article 6 ePR), is something that would quite obviously already not be possible given the GDPR's general data protection principles. Even where the law does actually deviate from the GDPR, such as with the introduction of protection for legal entities, Zwenne et al. found that these protections were likely already covered by international legislation such as the Convention on Cybercrime, making the proposal redundant even further.[160]

The examples given here are certainly non exhaustive and introduced quite summarily, but they should serve as an indication as to how much this proposal (which is unlikely to be altered significantly in the next few months) feels like a lost opportunity to effectively particularize and complement the GDPR.

One final negative effect is that the ePR actually risks de-harmonizing the EU data protection regime by insisting on rephrasing principles that were already established clearly in the GDPR (i.e. data minimization, general prohibition on processing personal data). This is a move away from the treatment of the GDPR's core principles as foundational for other legislation, and something which can only serve to create unnecessary confusion when these principles have to be interpreted.

5.1.3. Cybercrime Legislation

Cybercrime legislation establishes the framework within which botnet mitigation takes place and plays a large role in determining what parties are involved and what exact measures they are able to utilize. One aspect of European Union cybercrime legislation which could be criticized is the position it places ISPs in, which is somewhat contradictory at times.

The eCommerce Directive (article 12 to 14) exempts ISPs from secondary liability for data on their services only when they act as a 'mere conduit' for data.[161] As mentioned in chapter 3, this mere conduit (or 'passive') approach is useful because imposing stricter secondary liability would not only severely limit ISPs in the operation of their services, it might also incentive them to impose intrusive surveillance or censorship measures for fear of otherwise being held liable.[162] However, this approach also has the for botnet mitigation undesirable effect of discouraging ISPs from utilizing all the tools at their disposal for monitoring and filtering the data on their networks: after all, too active an approach might end up violating this mere conduit principle and cause ISPs to be liable for the

[158] (Zwenne et al., 2018), p.37
[159] Idem., p.16
[160] Idem., p.38
[161] For a more extensive discussion of this legislation see chapter 3, p.26
[162] (Sartor, 2017), p.11

content on their networks.[163] This is at odds with the role of ISPs as natural control points against botnets, as they are otherwise uniquely equipped and incentivized to participate in botnet mitigation. Seeing how passivity towards data is currently considered the norm in the European legal tradition, ISPs are likely to default to this approach in a situation where there is uncertainty about the legality of certain mitigation methods. [164] I believe this will end up harming the security of their networks.

While some of the tension described here is likely necessary because of divergent aims (privacy versus security), I have made a case in chapter 4 that these two principles do not actually have to be as dichotomous as often presented when we legislate intelligently.[165] Indeed, I will present some solutions offered by scholars on the subject in chapter 6 of this thesis.

5.2. Technical Aspects

In chapter 4 of this thesis I have examined where legislation facilitated botnet detection methods, which makes it stand to reason that this chapter will examine where legislation does either not facilitate it, or facilitates it poorly.

5.2.1. Infiltration

As explained in chapter 2, 'infiltration' is an active detection method (i.e. one that interferes with the data it processes instead of just passively analyzing it) that entails disguising a machine as a bot in order to learn more about the functioning of the botnet. After a successful infiltration by the bot the botnet's C&C server can be hijacked, shut down remotely and the attached bots could even be remotely cleaned from the bot binary.[166]

In the case of ISPs, this active manipulation of the data stream method (which is done when injecting the disguised bots) would most likely violate the 'mere conduit' approach to data processing, voiding the exemption for secondary liability that is otherwise granted to them under the eCommerce Directive. This alone makes infiltration (or any active detection method, for that matter) in practice extremely unattractive for ISPs.[167]

This of course is not a problem for those private parties (security companies, researchers) which are not operators of a network and therefore do not have to worry about secondary liability. Unfortunately for them, infiltrating a botnet is a highly privacy-invasive method because once the C&C server is hijacked it is possible to catalog most, if not all, of the communication that is done between the C&C server and its bots, most of which will contain end-user communications. Similarly to honeypots/sinkholes, this communication has a high risk of carrying personal data with it, and would therefore not likely to be available to private parties.[168] The invasion of privacy is exacerbated by the fact that the party controlling the C&C server has access to the same security vulnerabilities in

[163] (Tjong Tjin Tai et al., 2015), p.159
[164](Tjong Tjin Tai et al., 2015), p.75
[165] See chapter 4, p.32-33
[166] See chapter 2, p.14
[167] (Tjong Tjin Tai et al., 2015), p.158
[168] (Vihul et al., 2012), p.39

the attached bots that were used to install the bot binary in the first place, theoretically given the controlling party far-reaching access to the compromised systems.

That leaves us with the use of infiltration by law enforcement or other competent authorities. Because this is a thesis discussing the impact of European Union legislation on these methods we can be relatively brief about this, because EU law specifically does not regulate hacking carried out by law enforcement currently.[169] Instead, the EU leaves legislating this practice to its member states following the subsidiarity principle. However, in reality only a handful of member states have taken the opportunity to specifically legislate hacking by police (as a tool that is fundamentally different from 'real-world' searches and seizures), but it seems like botnet takedowns through infiltration would likely be possible under most of these laws. For example, the recently adopted Dutch Computer Crime Bill III specifically allows law enforcement more leeway in the hacking of computers, as well as the takedown and blocking of malicious traffic, something which was singled out by the Dutch legislator as an anti-botnet provision.[170] In practice we also see that national and EU law enforcement agencies such as Europol routinely assist in the hacking and taking down of botnets, in fact it is an important tool in the move towards disrupting cybercrime.[171]

The main problem with this approach is that it leaves something of a regulatory vacuum and a low level of harmonization between member states level, something which is undesirable given the international nature of botnet mitigation. In the current situation we find that a majority of member states have no specific regulation concerning the hacking of systems by competent authorities, while one study found that the countries which do have specific legislation often have vastly different tolerances, levels of oversight and remedies between each other.[172] This lack of harmonization is likely to lead to more problems in the future as hacking by law enforcement gets utilized more often and cross-national cooperation between law enforcement agencies gets more intense.

5.3. Procedural Aspects

When in chapter 4 I looked at the legislation governing the procedural aspects of botnet mitigation (i.e. that legislation which deals with cooperation and the sharing of data between different parties), I noted that the existing regime facilitates the transfer of data between parties. However there are certain developments of botnet mitigation which, while not necessarily negative to botnet mitigation, still lead to a situation that is largely undesirable from a data protection and human rights perspective.

5.3.1. Black Box Botnet Mitigation

Already in 2014 Zach Lerner, writing for the Harvard Journal of Law & Technology, warned that the increased reliance on public-private partnerships could lead to a decrease in accountability for botnet mitigation methods in the United States.[173] He mentions two main reasons for this, the first being the practice of holding so-called ex-parte hearings, which are legal proceedings that take place

[169](Gutheil, Liger, Heetman, Eager, & Crawford, 2017), p.39
[170] (Oerlemans, 2017a), p.358
[171] Idem., p.359
[172](Gutheil et al., 2017), p.56
[173] (Lerner, 2014), p.250

despite one or more parties (in this case the extra-judicial botnet masters) being absent. This means that there will be little to no push back from the prosecuted party to closely examine the investigative methods used. Lerner adds that, given the highly technical nature of botnet mitigation, judges are often ill-equipped to provide this push back independently.[174] The second reason Lerner finds is that law enforcement and private parties often attempt to keep the exact investigative techniques utilized confidential for 'security purposes', which means that there is almost no possibility for review from third parties such as privacy watchdogs or academics.[175] While Lerner does not mention this, it stands to reason that private institutions might also have an incentive to keep their investigative methods a secret because these give them a competitive advantage in whatever market place that they operate in.

This problem of accountability has only been exacerbated by the move to disruption that has taken place since Lerner's article, which has caused botnet mitigation operations to be subject to even less judicial review.[176] Oerlemans has pointed out that the (often far-reaching) investigative methods used in these disruption operations were bestowed upon law enforcement in the understanding that they were subject to strict judicial review once prosecution began, but that this last step often does not take place anymore. This weakens the checks and balances that we as a society demanded to be in place if we want our law enforcement to deploy these intrusive investigative methods.[177]

This would of course be less of a problem if the EU legal framework provided a robust system of internal or external review for law enforcement and their associates, but unfortunately I find that not to be the case currently. As discussed in chapter 3, the LED institutes Independent Supervisory Authorities (article 47 LEA) that are supposed to supervise the data processing of law enforcement. However, these ISA's have no power to impose fines, cannot suspend data flow to third parties or organizations, have very little investigative powers and cannot order a controller/processor to comply with data subject requests. They do have the very powerful tool of issuing a temporary or indefinite limitation or ban on data processing, but this is of course weakened by their almost non-existent investigative abilities.[178] Furthermore, law enforcement agencies are themselves incentivized to present the data processing done as relatively harmless and executed as responsibly as possible, because doing otherwise would mean them risking access to certain powerful investigative methods. This is exactly the reason why ex post judicial review (preferably with the involvement of the accused party) of these investigative methods is very important, and why we should be concerned about this diminishing.

One problem that is aggravated by this lack of accountability is that of one called 'purpose creep', which is the reusing of data for a purpose different from that for which it was originally collected legally, without getting further consent from the data subject.[179] The risk of purpose creep increases when there's less accountability and more parties sharing the data, which are both occurring at the moment. Purpose creep in this instance can happen both ways, i.e. law enforcement repurposing data collected for a legitimate purpose by a private party such as an ISP, but also private parties

[174] Idem., p.258

[175] Idem., p.247

[176] See chapter 2, p.17

[177] (Oerlemans, 2017b), p.363

[178] (Caruana, 2017), p.12-13

[179] (Porcedda, 2012), p.65

repurposing data that was originally collected in the course of an investigation for commercial or other purposes. It is not hard to imagine scenarios where data collected for investigative purposes could be used to give a private party a competitive advantage: a security company could use data on botnet or malware behavior to further improve its products, for example. One real world example of this can be found in the case of the Avalanche network takedown: after this takedown was completed one NGO that helped analyze the data offered a package of analytical insights compiled from this analysis. They did so for free, but the data was still collected for a different purpose originally (i.e. for that of a criminal investigation) and the NGO can with this data offer a unique value that might help it secure future funding, contacts, and so on.[180] As data processing gets more complicated and is carried out by an even larger number of parties, it will only get harder to prevent this purpose creep from taking place.

All these factors combine to lead to a type of botnet mitigation which I have come to refer to as black box botnet mitigation. The term comes from the phenomenon of 'black box artificial intelligence', which talks about a type of artificial intelligence of which the creators are unable to understand or trace back how the artificial intelligence reaches certain conclusions in its reasoning.[181] Black box botnet mitigation, while likely not as incomprehensible as the decision making of certain artificial intelligences, shares the same level of opaqueness as black box artificial intelligence. In black box botnet mitigation we find that there is very little oversight on, or larger understanding of, botnet mitigation methods possible, because these mitigation methods are not scrutinized adequately. This is due to this mitigation being spread across a large number of public/private parties, weak internal and judicial review, and a diminished possibility of academic review because the methods used are often kept secret for the remaining public sector. One might cynically argue that in some ways this type of botnet mitigation could actually help botnet mitigation: after all, if law enforcement is freed from being overly scrutinized and regulated, they are also liberated at using the full arsenal of abilities available to them. However, I believe that this approach to botnet mitigation will prove undesirable in the long run because effective review and analysis of methods deployed also help guarantee that these methods actually achieve the effect they purport to have (i.e. the effective mitigation of botnets).[182] Black box botnet mitigation frustrates review of methods used and thereby frustrates progression of these methods (which is only possible when we can effectively review these methods).

A more immediate worry is the effect black box botnet mitigation has on due process and the protection of certain fundamental rights such as the right to private life and the right to data protection. Even botnet mitigation methods that focus on disruption instead of prosecution have an enormous impact on individuals, targeted or otherwise, (e.g. servers being taken offline, internet access denied, being subjected to far-reaching surveillance methods) and ideally we would want to see measures like this being subjected to proper judicial review, something which is currently lacking. This increases the chance that fundamental rights of subjects are continuously and systematically encroached upon in botnet mitigation operations. Looking further than merely the suspects, I have hoped to illustrate that most botnet mitigation methods carry with them great risk towards the data security of any end-user that operates on the same network as the botnet targeted. While I have

[180] (The Shadowserver Foundation, 2016b).
[181] (Bathaee, 2018), p.893
[182] (Lerner, 2014), p.256

shown that most of these methods can be utilized legally and safely when certain safeguards are considered, a lack of oversight and review increases the risk that the privacy of end-users is seriously affected. Additionally, the risk that not enough adequate steps are taken once such a breach of privacy has taken place is also increased once there is no effective supervision. This is not to say that such a violation of privacy rights necessarily takes place currently, but rather that the system as it stands increases the risk of such violations, and subsequently frustrates their detection and remedial. It is especially in an area that is as quickly developing and involves as much risks to fundamental rights as botnet mitigation that review and oversight should be more considerable as opposed to less.

5.4. Conclusions for Chapter 5

I believe that the negative effects produced by the European Union legislative framework mainly stem from one of two scenarios: poor implementation or a failure from the legislation to account for changing circumstances. The former scenario can be seen in the chilling effect surrounding the current data protection reform. While in chapter 4 I have found the data protection regime to offer enough leeway where necessary to data controllers, in practice we see that the reform has been pared with so much uncertainty that actors become reluctant to act. While some of this uncertainty is likely normal for a reform on this scale, it is still imperative that the European Union promotes harmonized best practices as soon as possible. This is not only to reduce the chilling effect, but also to prevent de-harmonization from taking place as actors begin interpreting the law in divergent ways (something which would defeat much of the purpose of the reform and likely add to the confusion). A complicating factor in this is the ePR, which seems poorly thought out in its heavy-but-not-quite overlap with already existing data protection legislation such as the GDPR, and which will risk garnering further confusion when it is introduced.

Alternatively, we see a failure to account for changing circumstances when it comes to cybercrime legislation, where I have found that restrictive requirements for ISPs prevent these parties from acting to the fullest of their potential. The demand (established in the eCommerce Directive) to act as mere conduits towards data stems from the year 2000, but since then the threats on operators' networks have grown much more substantial. Given their position as natural control points against botnets, a passive position becomes increasingly untenable and a reform of this aspect of the eCommerce Directive seems to be desirable to me, which is something that I will go into more detail about in chapter 6.

Finally, the largest failure to account for changing circumstances can I believe be found in the example of black box botnet mitigation. A number of developments (e.g. move to disruption, reliance on public private partnerships) have come together independently to create a situation where there is a systemic lack of oversight on botnet mitigation methods, something which I have argued harms the effectiveness of these methods and also risks violating a number of fundamental rights. Legislation will have to be amended to address this issue, which is something that I will elaborate upon in chapter 6. This chapter will offer a number of tentative solutions to the problems presented here, as well as conclude the thesis.

Chapter 6: Improvements and Conclusions

In this final chapter I will summarize the answers to the research questions that were posited in chapter 1 of this thesis, after which I will introduce further research questions sparked by this discussion and subsequently conclude my thesis. Before doing so, however, I will summarily discuss a number of possible solutions to the problems discussed in chapter 5. Elaborating too much on these would be outside the scope of this thesis, but as this thesis is meant to be a jumping-off-point for further research into the effect of EU legislation on botnet mitigation I feel that I would be remiss not to at least mention a number of approaches that I have found to be worth exploring in the future.

6.1. Possible Improvements to EU Botnet Mitigation

The improvements proposed here are a combination of solutions offered by others that I encountered while researching this thesis, and of those proposals that I deem to be 'common-sense' solutions based on the problem described. This list is not meant to be exhaustive, nor does it address every problem raised in the previous chapter or offer complete solutions to the problem they are addressing. Instead, this list is to be viewed as a starting point for those interested in studying this subject more particularly.

6.1.1. General Observations – Chilling Effect

In chapter 5 I have explained how I believe a chilling effect on botnet mitigation is produced by EU legislation for two reasons. Firstly, the open-endedness of the data protection regime and a lack of guidelines create uncertainty. Secondly, actors lack confidence in their ability to make adequate decisions based on the law due to the scale of the data protection reform.[183] While I have argued that this open-endedness serves a certain purpose (to future-proof legislation and to encourage a more holistic approach to data protection), there are still steps that can be taken on a European Union level to improve access to information and decrease uncertainty for actors in the cybersecurity field. For example, this would entail the creation of clearer guidelines as to what is permitted under the current level of technology, likely by EU-level organizations such as Europol or ENISA. While it is of course desirable to target this information campaign to as broad as possible a group of actors involved in cybersecurity, we must also be aware that (given limited recourses) this is likely to lead to a more diffuse set of guidelines than is perhaps desirable. Research by Tjong Tjin Tai et al. has suggested that the primary group to target initially with such an information campaign would be ISPs, given their relative size, controlling role on networks and their natural incentive to fight cybercrime.[184] Factoring all this in, Tjong Tjin Tai et al. argue that extensively informing and cooperating with ISPs as to what is permitted to them currently could have a large impact on cybercrime prevention.[185] Lessons learned from this process could subsequently be incorporated in information campaigns targeting smaller actors such as security companies and network

[183] See chapter 5, p.39
[184] See also chapter 2, p.14 for more on ISPs as 'natural control points'.
[185] (Tjong Tjin Tai et al., 2015), p.160

administrators. Additionally, the establishing of clearer guidelines on an EU level could also prevent the de-harmonization of botnet mitigation methods that could occur as member states interpret the EU legislation in different ways.

Finally, I have observed that the current ePrivacy Regulation Proposal rephrases principles that were actually clearly established in the GDPR already (such as those regarding data minimization), and that it is currently unclear what the intended overlap between the two pieces of legislation is.[186] The effect of this could not only lead to de-harmonization but also increase the chilling effect on actors, who become increasingly reluctant to act as legislation becomes more and more unclear. While the ePR is currently in its final stages (and therefore unlikely to be significantly amended), the EU would do well to either revise these aspects to incorporate GDPR terminology or to better establish how ePR terminology overlaps and/or differs from already existing terminology.

6.1.2. General Observations – Cybercrime Legislation

I have discussed a tension created by legislation for ISPs which currently hinders botnet mitigation efforts, stemming from the requirement to act as a 'mere conduit' towards the data on their networks.[187] One solution to this suggested by Giovanni Sartor is to look towards the way the United States resolves this tension, and that is by having so-called 'good Samaritan' rules apply to initiatives by ISPs to restrict access to illegal content on their networks. This means that these ISPs do not automatically lose their immunity to secondary liability when they actively interfere with the data on their networks, as long as that interference is in the service of preventing criminal activity.[188] Of course, this rule would not translate one-to-one to EU legislation: the EU (which is a civil law system) doesn't immediately recognize the common law concept of 'good Samaritan' laws for one, but the idea behind it could be translated somehow.[189] Of course this should not mean that ISPs can wantonly interfere with the data on their network: there should be careful parameters and conditions to this exception. However, many scholars find that the current strictness of the mere conduit principle disincentivizes ISPs from securing their networks to the fullest of their potential, and that is an issue which will need to be addressed at some point as cybercrime becomes an increasingly large threat. [190]-[191]

6.1.3. Procedural Aspects – Black Box Botnet Mitigation

Of all the negative effects produced by the current EU legislative framework I have discussed in the previous chapter, that of black box botnet mitigation is likely the most complex one, as it is predicated on many factors (public-private partnerships, the move to disruption, weak oversight mechanisms) compounding. It is therefore difficult to offer straightforward solutions to this problem, other than generally recommending that this problem be examined further. One suggestion offered by Zach Lerner is a more systematic involvement of the academic and research community in public-private partnerships, as currently the 'private' aspect of these partnerships is heavily weighted

[186] See chapter 5, p.41
[187] See chapter 5, p.42
[188] (Sartor, 2017), p.17
[189] (Gulam & Devereux, 2007), p.478
[190] (Burghouwt, 2007), p.40
[191] (Tjong Tjin Tai et al., 2015), p.164

towards commercial parties such as ISPs.[192] According to Lerner this relatively simple change could improve the level of public oversight on the methods utilized by these partnerships, improve the methods utilized, as well as increase the focus on privacy- and human rights concerns.

Additional suggestions would be to increase the investigative competencies for Independent Supervisory Authorities (ISAs), who are currently often unable to adequately investigate processing carried out by competent authorities. Doing so would increase transparency for investigative methods and reduce the risk of purpose creep, as the data would be better accounted for. Of course, this would likely also necessitate increased funding for these organizations, as ISAs are currently already stretched to a breaking point when it comes to time and resources.[193] While complete transparency is undesirable (given the important

One final suggestion would be to improve judicial training with regard to cybercrime and cybercrime investigation techniques, as a lack of expertise in these matters has been signaled to contribute to the problem of black box botnet mitigation. Again, while likely necessary, this is easier said than done. Cybercrime is of course not the only area of investigation which has gotten more complex, and in the Netherlands for example judges are already struggling to keep up with their supplementary training.[194] Addressing this will likely require large investments in judicial capacity, something which national governments might be reluctant to do.

6.2. Answering the Research Questions & Further Research

As this thesis comes to a close I will summarize the answers to the research questions put forward in the first chapter.

6.2.1. How does data protection and confidentiality of communications legislation in the European Union affect botnet mitigation?

The data protection regime in the European Union is quite comprehensive and without doubt the largest of its kind, both in scope and in the level of protection it offers to data subjects.

While the requirements and responsibilities put forward by this legislation are relatively strict and offer very important protections to data subjects, I have found that this legislation also generally attempts to provide for the needs of botnet mitigation. The legislation further harmonizes data processing: this makes cross-border cooperation easier within the EU, something which is vital for the needs of botnet mitigation. The legislation also provides exceptions for the processing of personal data for a variety of techniques (packet inspection, analysis of flow records) necessary for botnet mitigation, given that good practices are observed. The legislation recognizes that these techniques might be required for legitimate interests such as performance of contract, network security, scientific research, or for the purposes of an investigation by law enforcement. So-called 'active' botnet detection methods are likely not allowed to private parties (but they are to law enforcement) given their invasive nature and the existence of less compromising 'passive' methods.

[192] (Lerner, 2014), p.261
[193] (Stupp, 2019), p.2
[194] (BNR webredactie, 2018).

However, it should be noted that these methods were already disallowed under the pre-GDPR data protection regime.[195]

Positive as these findings are, it should still be worrying that the open-ended nature of the legislation brings some amount of confusion with it for actors (especially private ones), something which creates a chilling effect that prevents them from applying their abilities in full. While some of this confusion will dissipate with time, governments and other regulatory bodies should still take steps to reduce this uncertainty if they want private actors to contribute as effectively as possible to botnet mitigation. It should also be noted that some of this confusion might be increased by the upcoming ePR, which unfortunately uses different terminology than its counterparts. Finally, I have found that the oversight from Independent Supervisory Authorities with regards to data processing done by law enforcement is often lacking due to the weak investigative powers given to these institutions.

6.2.2. How does the European Union legal framework criminalize behavior related to the operating of a botnet?

I have concluded that the European Union legal framework has introduced more substantive criminalization of behavior related to the operating and propagating of a botnet. This is done mostly through Directive 2013/40/EU, which among others had as a stated goal to better criminalize botnet-related behavior. In my opinion it has done so quite successfully. It criminalizes the spreading of bot binaries (both for hacking and through social engineering), the distribution and ownership of the tools necessary for botnet operation and propagation, as well as the most common applications of botnets such as DDoS attacks. Importantly, the directive also imposes an additional substantive criminalization for instances where a significant number of information systems are affected, something which is highly relevant to positioning botnet-related crimes as more serious than merely the sum of the crimes (hacking, system interference, phishing, etc.) necessary for operating a botnet.

Through this legislation the European Union has achieved an important step. Law enforcement no longer has to ‘translate’ old legal concepts to a digital environment when modern cybercrime activities are accurately criminalized. This makes prosecution easier and less prone to errors. Because this criminalization is done on an EU-level a harmonizing effect is to be expected, which in turn benefits mutual legal assistance efforts throughout the European Union. Studies performed by the European Union on the implementation of the directive support this theory, finding that the directive was overall implemented consistently between member states. This does not mean that there is no room for improvement however, as there are still discrepancies between member states in the use of definitions and the criminalization of certain behaviors. The European Union will have to promote further harmonization if f we want to complete the criminalization of behaviors related to the operating of a botnet. Nonetheless I have overall found that the criminalization of these behaviors is achieved very well in the European Union.

6.2.3. How does the European Union legal framework incentivize the participation of private parties in botnets mitigation?

Given the important role of actors such as ISPs and security companies in the mitigation of botnets it is important that these parties are properly incentivized to contribute to these efforts. I have found

[195] (Khattak et al., 2012), p.15

that there are a number of factors present in the current legislation that actively promote this contribution.

First is the fact that the current data protection regime allows for many botnet detection methods to qualify under legitimate interests if good practices are observed, allowing private parties (mainly ISPs, but also security companies and researchers) to aid botnet mitigation in this way. This is added to by the fact that the law enforcement data protection regime (Directive 2016/680) allows law enforcement to utilize private parties, who often have knowledge and recourses unavailable to law enforcement, as processors of data in pursuit of an investigation. This enables law enforcement and private parties to more easily cooperate in public-private partnerships, which have become a cornerstone of botnet mitigation efforts.

The second method of incentivization is through legal obligations. Directive 2000/31/EC (the eCommerce Directive) article 15(2) allows Member States to impose certain obligations on ISPs with regards to monitoring their networks, as well as notifying and cooperating with competent authorities.

However, the effects of this are undermined somewhat by the mere conduit principle introduced in this same directive, which requires ISPs to remain passive towards data or risk being liable for the data transmitted on their networks. This principle heavily disincentivizes operators from taking too rigorous steps in detecting botnets on their networks. This tension will have to be resolved at some point if we want to properly incentivize ISPs to act against botnets to the fullest of their potential.

6.2.4. How can European Union legislation to improve botnet mitigation while still respecting fundamental rights to privacy and data protection?

Much literature on botnets, including that by Vihul et al. and Tjong Tjin Tai et al., present privacy and cybersecurity as largely dichotomous to one another. In this thesis I have attempted to argue a viewpoint that is more optimistic about the possibility of co-existence between these two values, while still acknowledging the tension that can be found between them. I believe that good privacy legislation should actually contribute to cybersecurity efforts, and vice versa. Examples of this can be found in the new data protection regime that was implemented with the GDPR and LED. This legislation aids cybersecurity efforts by harmonizing legislation, clearly positioning cyber-and network security as a legitimate interest, and facilitating public-private partnerships, while at the same time intensifying data protections throughout the European Union. Of course, this does not mean that the legislation is without flaws, or does not have any unwanted negative effects on botnet mitigation efforts. However, it does signify that one piece of legislation can concurrently contribute to both privacy- and cybersecurity interests.

It should be noted that that there is bound to be a steep learning curve to striking the difficult balance between competing values: that does not mean that it is impossible. Furthermore, it is important to be aware of the negative effects privacy legislation can have on cybersecurity if we want to keep continuously improving the balance between these two. However, I have found that the worst detrimental effects can be found in privacy and data protection legislation that is either outdated, poorly thought out, or operating through blanket measures (or through a combination of all three; e.g. in the eCommerce Directive's application of the mere conduit principle). Rather than taking these pieces of legislation as a sign that privacy and cybersecurity are mutually exclusive, I would advocate that we use these as lessons towards refining and modernizing our privacy legislation to better address cybersecurity needs. I believe that it is only through this lens that we begin shaping legislation that truly addresses the needs of citizens for both strong data protection as well as better cybersecurity.

Conversely, we should also not be blind towards the ways in which cybersecurity efforts can have a detrimental effect on privacy rights. In this thesis I have concluded that a number of developments in botnet mitigation (the move to disruption, reliance on public-private partnerships, weak oversight mechanisms) have amalgamated to form a so-called ‘black box’ of botnet mitigation. In this situation there is too little public or judicial review of the botnet mitigation practices used, which leads to an increased risk of rights violations taking place. In these instances cybersecurity efforts need to be designed with privacy rights in mind (e.g. by incorporating more academic review of techniques used), once again illustrating how cybersecurity and privacy legislation can only be safeguarded if they are implemented with both needs in mind.

6.2.5. Further Research Questions

This thesis has attempted to broadly map the European Union legislation relevant to botnet mitigation, as well as some its positive and negative effects on these mitigation efforts. In doing so, I have hoped to present a large amount of avenues for future research. One obvious candidate for this would be a more in-depth analysis of the risks and effects of public-private partnerships, especially in regard to privacy and data protection rights. Another aspect that is worth researching more thoroughly is the legal position of Internet of Things (IoT) botnets, as opposed to botnets residing on personal devices. Much of the communication between IoT devices might not fall under what we currently consider ‘personal data’, something which could have implications for botnet mitigation.[196] As botnets increasingly move towards IoT devices, a thorough examination on the legal protections of IoT communications is warranted. A topic also worth researching is the sharing of personal data with countries outside of the European Union, something which is also relevant to botnet mitigation due to its international nature, but which was not discussed in this thesis. Finally, a European Union-level analysis of botnet mitigation legislation of course offers a limited image, since much of cybercrime (and to a lesser extent data protection) legislation is left to individual member states under the subsidiarity principle. Research into the effect of national legislation on botnet mitigation efforts would therefore be a logical next step.

6.3. Conclusion

I have started this thesis with the question whether Vihul et al. their 2012 assertion that ‘the fight against botnets is touching the limits of existing law’ still holds true currently. In many ways the answer to that question depends on the angle one chooses to look at it from. If we examine Vihul et al. their original concerns we can indeed conclude that modernized legislation has addressed most of these concerns to at least some degree. After all, Vihul et al. were among other things concerned with the criminalization of botnet-related behaviors, the few incentives for key players, and the questions regarding the legality of botnet detection methods with regard to privacy. Botnet-related behavior has been criminalized better, privacy legislation has gotten more substantive and derogations under it are clearer, and private actors and law enforcement have found each other in

[196] For a brief discussion of this see chapter 3, p.32

the construction of public-private partnerships. All of these developments positively contribute to botnet mitigation efforts.

Of course, we can still see that legislation leaves uncertainties and gaps that disincentivize actors and these should be addressed as soon as possible; however the situation has been overall improved since 2012. In this regard one might conclude that the European Union legal framework does a relatively good job overall of facilitating botnet mitigation efforts.

Looking at it from another angle, however, we can see that the increasingly complex nature of botnet mitigation has forced certain developments to take place that might end up having severely negative consequences. These developments (such as the move to disruption instead of prosecution and an increased reliance on public-private partnerships) might very well be necessary in this day-and-age; however our legislation has failed to keep up with these new realities. Many of the investigative powers bestowed upon law enforcement (and conversely on private parties that are enlisted as controllers under the LED) are given to them in the understanding that they will be subject to public scrutiny. This is for good reason: botnet mitigation methods bring with them serious risks to the privacy of any person that uses the network that is being researched. Unfortunately, I have found that this oversight is currently lacking. Botnet mitigation increasingly takes place behind closed doors, which leads to an increased risk of rights violations for suspects and data subjects alike.

The next large reform in cybersecurity- and privacy legislation will have to address these concerns, at which point new concerns will undoubtedly have arisen that will have to be addressed, and so on. While this may sound defeatist, I do believe that the speed at which technology currently develops means that we will have to accept this cycle and embrace it. Looking at the concerns noted by Vihul et al. in 2012 shows that the European Union has proven itself capable of addressing the questions it faces with regard to cybersecurity. I am cautiously optimistic that the European Union will continue to do so, however it is key that it does so in a way that treats privacy and cybersecurity as two sides of the same coin. We cannot effectively move forward until we reconcile the tension between these two values, and it is only then that we can develop holistic, future-proof botnet mitigation methods. Achieving this will involve solving technical problems, of course, but it will just as much require our legislators to show the political courage to truly adopt the tenets established by ‘privacy by design’.

Here’s to hoping that in another seven years we can read a thesis concluding that we have indeed taken important steps in that direction – I will be looking forward to reading it.

Bibliography

Abt, S., & Baier, H. (2011). Towards Efficient and Privacy-Preserving Network- Based Botnet Detection Using Netflow Data. *Proceedings of the Ninth International Network Conference*, 42–50.

Abuse.ch. (2018). Sinkholes and Internet Hygiene. Retrieved June 4, 2019, from https://abuse.ch/blog/sinkholes-and-internet-hygiene/

Atluri, A. C., & Tran, V. (2017). Information security practices: Emerging threats and perspectives. In *Information Security Practices: Emerging Threats and Perspectives* (pp. 1–104). https://doi.org/10.1007/978-3-319-48947-6

Bathaee, Y. (2018). The Artificial Intelligence Black Box and the Failure of Intent and Causation. *Harvard Journal of Law & Technology*, *31*(2). Retrieved from https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf

Bauer, J. M., & van Eeten, M. J. G. (2008). ITU Study on the Financial Aspects of Network Security: Malware and Spam. *ITU Final Report*, *July 2008*(July). Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

Beales, A. (2014). An Analysis of Directive 2013/40/EU – attacks against information systems. Retrieved June 4, 2019, from http://iglezakis.gr/2014/12/02/an-analysis-of-directive-201340eu-attacks-against-information-systems/

Bertino, E., & Islam, N. (2016). Botnets and Internet of Things Security. *IEEE Computer Society*, 76–79.

BNR webredactie. (2018). “Forensische bijscholing rechters schiet tekort.” Retrieved June 4, 2019, from https://www.bnr.nl/programmas/juridische-zaken/10354841/forensische-bijscholing-rechters-schiet-tekort

Boardman, R., Mullock, J., & Mole, A. (2017). *Guide to the General Data Protection Regulation*. Retrieved from https://www.twobirds.com/~/media/pdfs/gdpr-pdfs/bird--bird--guide-to-the-general-data-protection-regulation.pdf?la=en

Bossong, R., & Wagner, B. (2017). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, *67*(3), 265–288. https://doi.org/10.1007/s10611-016-9653-3

Burghouwt, P. (2007). *Detection of botnet command and control traffic in enterprise networks*. *12th ICCRTS*.

Caruana, M. M. (2017). The reform of the EU data protection framework in the context of the police and criminal justice sector: harmonisation, scope, oversight and enforcement. *International Review of Law, Computers & Technology*, 1–22. https://doi.org/10.1080/13600869.2017.1370224

Cavoukian, A. (2009). Privacy by design: The 7 foundational principles. *Information and Privacy Commissioner of Ontario, Canada*. Retrieved from https://www.iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf

Cormack, A. (2016). Incident Response: Protecting Individual Rights Under the General Data

Protection Regulation. *SCRIPTed*, *13*(3), 258–282. https://doi.org/10.2966/scrip.130316.258

Council of Europe. European convention on human rights (1950). https://doi.org/10.1017/S0008197300013908

Czosseck, C., & Geers, K. (2009). *The Virtual Battlefield: Perspectives on Cyber Warfare*. IOS Press.

de Graaf, D., Shosha, A. F., & Gladyshev, P. (2012). BREDOLAB: Shopping in the Cybercrime Underworld. *Digital Forensics and Cyber Crime*, 302–313. https://doi.org/10.1007/978-3-642-39891-9_19

de Hert, P. (2015). The Right to Protection of Personal Data. Incapable of Autonomous Standing in the Basic EU Constituting Documents? *Utrecht Journal of International and European Law*, *1*. https://doi.org/http://doi.org/10.5334/ujiel.cz

de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? *Computer Law and Security Review*, *32*(2), 179–194. https://doi.org/10.1016/j.clsr.2016.02.006

de Muynck, J., Graux, H., & Robinson, N. (2013). *The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on*.

Dougherty, J. (2017). Netflow vs Packet Capture: Have Both. Retrieved June 4, 2019, from https://www.plixer.com/blog/netflow-traffic-analysis-2/netflow-vs-packet-capture-have-both/

E. Silva, K., & Coudert, F. (2014). *ACDC - Legal Requirements*. Leuven. Retrieved from https://acdc-project.eu/wp-content/uploads/2015/05/ACDC_D1.8.1_Legal_Requirements.pdf

Eeten, M. Van, Bauer, J. M., Asghari, H., Tabatabaie, S., & Rand, D. (2010). The Role of Internet Service Providers in Botnet Mitigation An Empirical Analysis Based on Spam Data. *Workshop on Economics of Information Security*, *2010/05*, 1–31. https://doi.org/10.1787/5km4k7m9n3vj-en

Emma-Iwuoha, L. (2017). Who is an Electronic Communications Service Provider (ECSP)? Retrieved June 4, 2019, from https://www.michalsons.com/blog/electronic-communications-service-provider-ecsp/17697

European Commission. (2015). *The European Agenda on Security*. Strassbourg. Retrieved from http://www.europarl.europa.eu/cmsdata/125863/EU agenda on security.pdf

European Commission. (2017). *Report from the Commision to the European Parliament and the Council assessing the extent to which the Member States have taken the necessary measures in order to comply with Directive 2013/40/EU*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017DC0474&from=EN

European Convention. The charter of Fundamental Rights of the European Union, Official Journal of the European Communities § (2000).

European Parliament. Directive 2000/31/EC (2000). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000L0031&from=EN

European Parliament. Directive 2013/40/EU (2013). Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040

European Parliament. Directive (EU) 2016/680 (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L0680&from=NL

European Parliament. Regulation (EU) 2016/679 (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN

Europol. (2015a). Botnet Taken Down Through International Law Enforcement Cooperation. Retrieved June 4, 2019, from https://www.europol.europa.eu/newsroom/news/botnet-taken-down-through-international-law-enforcement-cooperation

Europol. (2015b). *The Internet Organised Crime Threat Assessment (IOCTA) 2015*.

Europol. (2016). Avalanche Dismantled in International Cyber Crime Operation. Retrieved June 4, 2019, from https://www.europol.europa.eu/newsroom/news/'avalanche'-network-dismantled-in-international-cyber-operation

Europol. (2017). Andromeda Botnet Dismantled in International Cyber Operation. Retrieved June 4, 2019, from https://www.europol.europa.eu/newsroom/news/andromeda-botnet-dismantled-in-international-cyber-operation

Forrest, C. (2017). IBM admits it sent malware-infected USB sticks to customers. Retrieved June 4, 2019, from https://www.techrepublic.com/article/ibm-admits-it-sent-malware-infected-usb-sticks-to-customers/

Fraunhofer FKIE. (2016). *»Avalanche« – Ermittlern gelingt Schlag gegen organisierte Cyberkriminalität*. Retrieved from https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/Projekte/Avalanche/Avalanche_Folder.pdf

Garber, J. (2018). GDPR – compliance nightmare or business opportunity ? *Computer Fraud & Security Bulletin*, *2018*(6), 14–15. https://doi.org/10.1016/S1361-3723(18)30055-1

Gartner Inc. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Retrieved June 4, 2019, from http://www.gartner.com/newsroom/id/3598917

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, *29*(7), 1645–1660. https://doi.org/10.1016/j.future.2013.01.010

Gulam, H., & Devereux, J. (2007). A brief primer on Good Samaritan law for health care professionals. *Australian Health Review : A Publication of the Australian Hospital Association*, *31*(3), 478–482. https://doi.org/10.1071/AH070478

Gutheil, M., Liger, Q., Heetman, A., Eager, J., & Crawford, M. (2017). *Legal Frameworks for Hacking by Law Enforcement: Identification, Evaluation and Comparison of Practices*. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583137/IPOL_STU(2017)583137_EN.pdf

Helfer, L. R. (2008). Redesigning the European Court of Human Rights: Embeddedness as a Deep Structural Principle of the European Human Rights Regime. *The European Journal of International Law*, *19*(1), 126–159. https://doi.org/10.1093/ejil/chn004

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy* (Vol. 31). https://doi.org/10.1007/978-3-319-34090-6

HP News Advisory. (2014). HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Retrieved June 4, 2019, from http://www8.hp.com/us/en/hp-news/press-release.html?id=1744676

Huang, K. Y. (2017). Security 101: The Impact of Cryptocurrency-Mining Malware.

Hudson, D. L. (2017). Chilling Effect Overview. Retrieved June 4, 2019, from https://www.thefire.org/chilling-effect/

Hugenholtz, B. (2013). Is Harmonization a Good Thing? The Case of the Copyright Acquis. In *The Europeanization of Intellectual Property Law: Towards a European Legal Methodology* (pp. 57–74). Oxford Scholarship Online. https://doi.org/10.1093/acprof:oso/9780199665105.003.0004

IBM Security. (2017). *The Inside Story on Botnets*. Retrieved from https://www.ibm.com/downloads/cas/V3YJVYZX

Incapsula. (2019). What is DDoS Mitigation? Retrieved June 4, 2019, from https://www.incapsula.com/ddos/ddos-mitigation-services.html

INFOSEC Institution. (2018). Deep Packet Inspection in the Cloud. Retrieved June 4, 2019, from https://resources.infosecinstitute.com/deep-packet-inspection-in-the-cloud/

Ismail, N. (2017). Businesses and their employees admit to GDPR confusion. Retrieved June 4, 2019, from https://www.information-age.com/businesses-admit-gdpr-confusion-123469044/

John, W., Tafvelin, S., & Olovsson, T. (2010). Passive internet measurement: Overview and guidelines based on experiences. *Computer Communications*, *33*(5), 533–550. https://doi.org/10.1016/j.comcom.2009.10.021

Juniper Research. (2015). Cybercrime and the Internet of Threats 2017.

Khattak, S., Ramay, N. R., Khan, K. R., & Khayam, S. A. L. I. (2012). A Taxonomy of Botnets : Features , Detection and Defense. *Pakistan National ICT R&D Fund*, *V*, 1–48.

Koops, B.-J., & Goodwin, M. (2014). *Cyberspace, the cloud, and cross-border criminal investigation*. Tilburg. Retrieved from https://www.wodc.nl/binaries/2326-volledige-tekst_tcm28-73009.pdf

Lawson, R. A., & Schermers, H. G. (1999). *Leading Cases of the European Court of Human Rights* (2nd ed.). Leiden: Ars Aequi Libri. Retrieved from http://hdl.handle.net/1887/3157

Lerner, Z. (2014). Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigitating Botnets. *Harvard Journal of Law & Technology*, *28*(1), 237–261.

Mansfield-Devine, S. (2017). Meeting the needs of GDPR with encryption. *Computer Fraud & Security Bulletin*, *2017*(9), 16–20. https://doi.org/10.1016/S1361-3723(17)30100-8

Mcdermott, C. D., Petrovski, A. V, & Majdani, F. (2017). Towards Situational Awareness of Botnet Activity in the Internet of Things. Retrieved from https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/

Moise, A. C. (2015). Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level. *Journal of Law and Administrative Sciences*, *1*, 374–383.

Nazario, J. (2009). Politically motivated denial of service attacks. *Cryptology and Information Security Series*, *3*, 163–181. https://doi.org/10.3233/978-1-60750-060-5-163

OECD. (2012). Proactive Policy Measures by Internet Service Providers against Botnets. *OECD Economy Papers*, (199). https://doi.org/10.1787/5K98TQ42T18W-EN

Oerlemans, J.-J. (2017a). De Wet computercriminaliteit III : meer handhaving op internet. *Strafblad*, (Oktober), 350–359.

Oerlemans, J.-J. (2017b). *Investigating Cybercrime*. Universiteit Leiden. Retrieved from https://openaccess.leidenuniv.nl/handle/1887/44879

Pajunoja, L. J. (2017). *The Data Protection Directive on Police Matters 2016 / 680 protects privacy - The evolution of EU's data protection law and its compatibility with the right to privacy*. University of Helsinki. Retrieved from https://www.tandfonline.com/doi/pdf/10.1080/13600869.2017.1370224?needAccess=true

Pijpker, J., & Vranken, H. (2016). The Role of Internet Service Providers in Botnet Mitigation. *2016 European Intelligence and Security Informatics Conference*, 24–31. https://doi.org/10.1109/eisic.2016.12

Porcedda, M. G. (2012). *Data Protection and the Prevention of Cybercrime: The EU as an Area of Security?* (European University Institute Department of Law No. 2012/25). Florence. Retrieved from http://cadmus.eui.eu/bitstream/handle/1814/23296/LAW-2012-25.pdf?sequence=1&isAllowed=y

Praesidium of the European Convention. (2007). Explanations Relating To the Charter of Fundamental Rights. *Official Journal of the European Union*, *2*(2), 17–35. Retrieved from http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF

Ramge, T. (2018). *Mensch und Maschine* (5th ed.). Stuttgart: Philipp Reclam jun. GmbH & Co. KG.

Sartor, G. (2017). *Providers Liability : From the eCommerce Directive to the future*. Retrieved from http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/614179/IPOL_IDA(2017)614179_EN.pdf

Stupp, C. (2019, April 12). European Privacy Regulators Find Their Workload Expands Along With Authority. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402

The Shadowserver Foundation. (2016a). Avalance - Law Enforcement Takedown. Retrieved June 4, 2019, from https://avalanche.shadowserver.org/

The Shadowserver Foundation. (2016b). Avalanche: Stats. Retrieved June 4, 2019, from https://avalanche.shadowserver.org/stats/

Tjong Tjin Tai, E., Op Heij, D., E. Silva, K., & Skorvánek, I. (2015). Duties of care and diligence against cybercrime, (March).

Treaty on the Functioning of the European Union, Official Journal of the European Union § (2007).

Twitter Public Policy. (2017). Update: Russian Interference in 2016 US Election, Bots, & Misinformation. Retrieved June 4, 2019, from https://blog.twitter.com/official/en_us/topics/company/2017/Update-Russian-Interference-in-2016--Election-Bots-and-Misinformation.html

UNODC. (2013). *Comprehensive Study on Cybercrime*. Retrieved from https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

US-CERT. (2016). Heightened DDoS Threat Posed by Mirai and Other Botnets. Retrieved June 4, 2019, from https://www.us-cert.gov/ncas/alerts/TA16-288A

Vihul, L., Czosseck, C., Ziolkowski, K., Aasmann, L., Ivanov, I. A., & Brüggemann, S. (2012). Legal Implications of Countering Botnets, 1–67.

Williams, C. (2016). Today the web was broken by countless hacked devices - your 60-second summary. Retrieved June 4, 2019, from https://www.theregister.co.uk/2016/10/21/dyn_dns_ddos_explained/

Woolley, S. C., & Guilbeault, D. R. (2017). Computational Propaganda in the United States of America : Manufacturing Consensus Online, 1–29.

Zaharia, A. (2016). How Drive-by Download Attacks Work – From Disbelief to Protection. Retrieved June 4, 2019, from https://heimdalsecurity.com/blog/how-drive-by-download-attacks-work/

Zwenne, G.-J., Kroes, Q., & van Eymeren, J. (2018). *EPR vis-à-vis GDPR: A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation*.