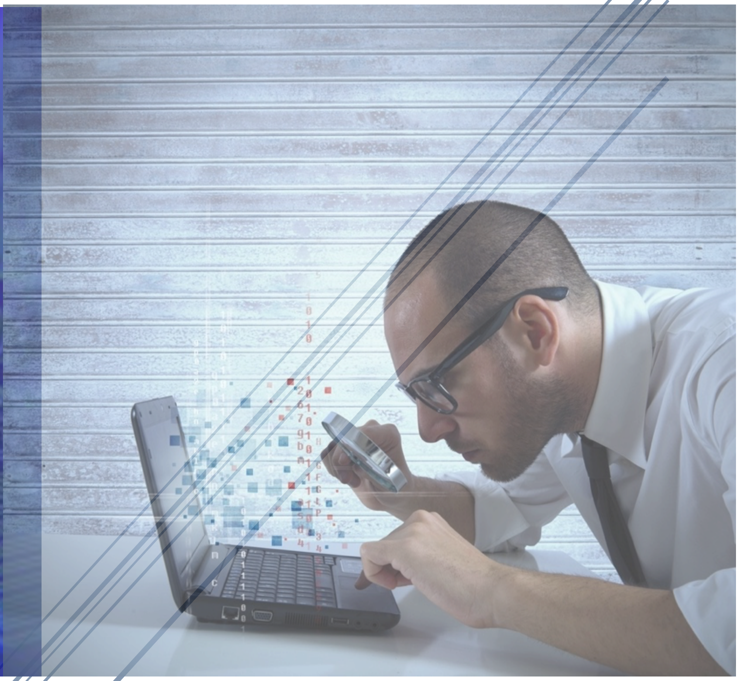
Strengthening the digital Achilles heel of the European Union:

Make use of ethical hackers to find vulnerabilities in information systems?



Gijs Peeters
S1584103
Master thesis
Leiden University
7 July 2017
Dr. Jan Oster
Dr. Eugenio Cusumano
16428 words

Abstract

Vulnerabilities in information systems have always been the Achilles heel of digital security. Ransomware-campaigns such as WannaCry and (Not)Petya highlighted the global and multi-dimensional nature of vulnerabilities and showed how substantial the impact of these could be for many aspects of the daily life. Vulnerability disclosure is a valuable instrument to report and solve these vulnerabilities to increase the security of information systems and prevent such events from happening. However, EU's legal landscape for vulnerability disclosure is fragmented, and vulnerability researchers have to deal with legal uncertainty.

Therefore, this thesis focuses on how the EU can increase the resilience of its cyber ecosystem through stimulating vulnerability disclosure. The purpose of this study will be to describe the different policy instruments the EU may use to stimulate coordinated vulnerability disclosure and prescribe which ones would be most valuable for increasing the EU's cyber resilience. Coordinated vulnerability disclosure refers to the approach of disclosing vulnerabilities in the security of information systems in a controlled and responsible manner.

This thesis will combine an analysis of primary and secondary sources – using technical and non-technical perspectives to bring these two worlds closer together to develop effective cybersecurity policies. To provide a deeper understanding of how the EU could construct a resilient cyber ecosystem: insight on cybersecurity, the resilience of ecosystems and security governance will be combined. Concluding, it is recommended that the EU uses a mix of regulatory instruments making optimal use of the expertise of the private sector to stimulate coordinated vulnerability disclosure. The outcomes are timely because in September 2017 a new EU Cyberstrategy will be presented.

Keywords: cyber resilience, cybersecurity, European Union, coordinated vulnerability disclosure, regulatory instruments.

TABLE OF CONTENTS

LIST OF FIGURES AND TABLES

ABBREVIATIONS

AIS	Directive on Attacks against Information Systems
CEN	European Committee for Standardisation
CoC	Convention on Cybercrime
cPPP	Contractual Public-Private Partnerships
CSIRT	Computer Security Incident Response Team
CVD	Coordinated Vulnerability Disclosure
DPP	Dutch Public Prosecutor
DSM	Digital Single Market
EC	European Commission
EEAS	European External Action Service
ENISA	European Network and Information Security Agency
EP	European Parliament
EPSC	European Policy Strategy Center
EU	European Union
EUISS	European Institute for Security Studies
FIRST	Forum of Incident Response and Security Teams
IEC	International Electrotechnical Commission
IGF	Internet Governance Forum
IS	Information systems
ISO	International Organisation for Standardization
MS	European Union Member States
NCSC	National Cyber Security Centre the Netherlands
NIST	US National Institute of Standards and Technology
NTIA	National Telecommunications and Information Administration
OECD	Organisation for Economic Cooperation and Development
PPP	Public Private Partnerships
TFEU	Treaty on the Functioning of the European Union
UK	United Kingdom
US	United States

1. INTRODUCTION

Cyberspace has been tremendously growing in the last two decades. This growth has had an enormous impact on all parts of society. Many aspects of our daily lives now depend on the continuous functioning of information systems[1] (European Commission (EC), 2013). However, because of this increasing dependency, the potential impact of the unavailability or insecurity of information systems – for all parts of society – has made us vulnerable to threats. Vulnerabilities in information systems have always been and still are the Achilles heel of digital security (Cavoukian & Chanliau, 2013; Schuster et al., 2017). This was once again underlined by the WannaCry ransomware, which used a known critical vulnerability in Microsoft Windows to encrypt files on computers that could only be decrypted and reaccessed after paying a fee (European Union Agency for Network and Information Security (ENISA), 2017b; Herns & Gibbs, 2017). Its broad and rapid distribution, affecting approximately more than 150 countries and infecting over 230.000 systems over the weekend of 12th – 14th May 2017, caused chaos all over the world (ENISA, 2017a). European manufacturers, service providers and critical infrastructure operators in various sectors were affected by WannaCry and could not access their systems (ENISA, 2017b). Britain's hospitals, among others, could not access their systems and had to divert patients in need of immediate treatment and reschedule operations (Gayle et al., 2017).

The global impact and quick spreading of WannaCry shows how substantial the impact of vulnerabilities in information systems can be. Over the last decade, the impact and amount of vulnerabilities in information systems demonstrates a constant increase.[2] Consequently, the social importance of dealing effectively with vulnerabilities and increasing cybersecurity[3] has become more prominent (Begum & Kumar, 2016; ENISA, 2015; Pawlak, 2017). Moreover, the levels, scope and damage of cybercrime in the EU have exceeded traditional crime levels (EC, 2013; Europol, 2016).

Therefore, the subject of cybersecurity has become one of the most important issues on the European Union's (EU) political agenda in the last decade (Christou, 2016; Leyden, 2011; Pawlak, 2017). After WannaCry, the EC has highlighted the urgent need to step up the EU's

[1] An information system: "refers to a collection of multiple pieces of equipment involved in the dissemination of information. Hardware, software, computer system connections and information, information system users, and the system's housing are all part of an Information system" (Techopedia, 2017).

[2] According to annual threat reports of the main cybersecurity companies, the last three years on annual basis more than 6.000 new vulnerabilities were found. Whereof 1000-1500 classified as high; 3000-3500 medium; and the remaining low looking at a wide variety of factors (Cisco, 2017; Microsoft, 2016; Symantec, 2017).

[3] "Cybersecurity is the organization and collection of resources, processes and structures used to protect cyberspace and cyberspace-enabled systems." (Craigen, Diakun-Thibault, & Purse, 2014).

efforts to become cyber resilient[4]. It will accelerate its work on cybersecurity, particularly through issuing a new updated Cybersecurity Strategy in September 2017 (EC, 2017d, 2017e). The EC is thus currently considering which actions and policies are necessary to deal effectively with cybersecurity issues the coming years. This thesis assesses how the EU can increase its resilience in cyberspace, which is topical and relevant.

Ransomware campaigns such as WannaCry and (Not)Petya highlight the global and multi-dimensional nature of vulnerabilities in information systems (Frenkel, Scott & Mozur, 2017). It underlines the need to combat cyber threats on all levels together with a broad range of actors involved in the cybersecurity ecosystem (Christou, 2016). To increase the EU's resilience and security of information systems, identification and solving vulnerabilities in these systems is essential (ENISA, 2015). In short, "vulnerabilities are flaws or mistakes in computer-based systems that may be exploited to compromise the network and information security of affected systems" (ENISA, 2015, p. 7). The result of the successful use of vulnerabilities is a compromised information system's security. Due to the nature of these systems, an infiltrator can "delay, disrupt, corrupt, exploit, destroy, steal and modify information with various implications" (Waltz, 1998). There are several ways in which the EU can decrease the number of vulnerabilities in information systems and prevent exploitation of them. Examples are introducing certification schemes for software and hardware, funding secure software development and stimulating coordinated vulnerability disclosure (CVD) (Schuster et al., 2017). The latter is "a process through which vendors and vulnerability finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability" (ISO, 2014). Furthermore, proper facilitation of vulnerability disclosure is of great importance to increase the EU's cyber resilience (ENISA, 2015). CVD is a valuable instrument to report and solve vulnerabilities in a responsible and timely manner, thereby decreasing exploitation of vulnerabilities (Falot & Schermer, 2016; Schuster et al., 2017; Timmerman, 2013). However, EU's legal landscape for vulnerability researchers is currently fragmented (ENISA, 2015). Vulnerability researchers must deal with legal uncertainty and the risk of being sued, as all forms of hacking are a criminal offense according to a wide variety of laws (Schuster et al., 2017). Consequently, researchers can choose to sell the information on the black market, make it public for others to exploit or use it to develop new ways to exploit the vulnerability. A properly designed CVD policy would stimulate

[4] Resilience can be "understood as the capacity of different layers of society to withstand, to adapt to, and to recover quickly from stresses and shocks and has gradually emerged as the answer to the growing complexity of the international security environment" (Pawlak, 2016, p.1).

researchers to responsibly disclose vulnerabilities because “the absence of a common practice often results in miscommunication, leading to ‘uncontrollable’ vulnerability handling, confused or angry customers and unnecessary windows of opportunity for malicious actions” (Takanen et al., 2004). According to Cavusoglu, Cavusoglu & Raghunathan (2005), ENISA (2015) and Falot & Schermer (2016), to prevent this from happening policymakers in the EU and its Member States (MS) should strengthen the legal landscape to stimulate the responsible reporting of vulnerabilities and come up with ways to proper facilitate CVD. Therefore, the following question will be answered in this thesis:

> How may the European Union use its regulatory instruments to strengthen the resilience of its cyber ecosystem through coordinated vulnerability disclosure?

The following structure will be followed to answer this question. Chapter 2 will introduce the debate about ethical, white hat and black hat hackers, the legality of (ethical) hacking and explain why proper facilitation of CVD is important for the EU. Followed by the theoretical framework, which includes insights about the resilience of ecosystems, security governance and EU regulation in Chapter 3. The methodology will be discussed in Chapter 4. Chapter 5 will introduce relevant EU strategies and legislation to assess whether extra measures are necessary to stimulate CVD. Leading to a discussion of the possible options the EU may use to stimulate CVD and increase its cyber resilience in Chapter 6. A conclusion of a prescriptive nature will be given assessing which combination of regulatory instruments the EU may best use to strengthen its cyber resilience through stimulating CVD.

2. ETHICAL HACKERS, COORDINATED VULNERABILITY DISCLOSURE AND THE EU

The process of disclosing vulnerabilities is essential because it is one of the first steps to fix information systems and protect data in cyberspace (van der Meulen, 2016; Tai & Koops, 2015): "as long as perfectly secure software is not available, the optimal distribution of vulnerability information is an important factor of the stability of a network society" (Böhme, 2006, p. 298). CVD can provide an incentive for developers to create secure software and make sure that they patch vulnerabilities before attackers can exploit them (Mason, 2012; Maurushat, 2014). While attackers work in secrecy and do not have to comply with law, ethics or public scrutiny, vulnerability researchers operate in the open, are restrained by ethics and must fear the ambiguity of the law. Researchers risk legal consequences when reporting a vulnerability, especially when they find this without the consent of the system's owner (Matwyshyn et al., 2010; Pfleeger & Pfleeger, 2006). In this Chapter, the relevance of CVD for the EU will be discussed by zooming into the differences between white hat, black hat and ethical hackers. Followed by a discussion on the legality of hacking, the best form of vulnerability disclosure and an overview of the current landscape for vulnerability disclosure in the EU.

2.1. WHITE HATS, BLACK HATS & ETHICAL HACKERS

In the literature two broad categories of hackers are distinguished: white and black hat hackers (Kirsch, 2014; Maurushat, 2014; Cencini, Yu & Chan, 2005). Some identify a third intermediary category: gray hat hackers (Lemos, 2002).

A white hat hacker is "someone who finds or exploits security holes in software for generally legitimate and lawful purposes, often to improve the overall security of products and to protect users from black hat hackers" (Cencini et al., 2005, p. 5). While a black hat hacker is an opposite: "someone who uses his computer knowledge in criminal activities to obtain personal benefits" (Maurushat, 2014, p. 76). White hats are those that usually use their skills to the advantage of society to expose vulnerabilities before black hats can detect and exploit them (Techopedia, 2017). Black hats go into systems for personal profits or to perform a crime (Kirsch, 2014). In between are the gray hats, who perform activities on the border of civil and criminal liability to find security vulnerabilities (Lemos, 2002). They are often prepared to break the law to achieve the goal of improved security without consent (Electronic Frontier Foundation, 2008).

The terms white hat and ethical hacker are often used interchangeably. The similarities become visible when comparing the definitions: "Ethical hacking is the non-violent use of a technology in the pursuit of a cause, political or otherwise which is often legally and morally ambiguous” (Samuel, 2004). An ethical hacker is defined as someone:

> Who identifies a security weakness in a computer system or network but, instead of taking malicious advantage of it, exposes the weakness in a way that will allow the system's owners to fix the breach before it can be taken advantage by others (Falot & Schermer, 2016, p. 1).

When comparing these characteristics of white hats and ethical hackers, a lot of recurring characteristics become visible. The activities they perform are non-violent and non-malicious, and pursue a cause with the overarching belief of making information systems more secure. In this thesis, the definition of Falot & Schermer (2016) will be used.

2.2. LEGALITY OF (ETHICAL) HACKING

It is important to briefly discuss the difference between solicited and unsolicited testing of the security of an organization’s network. The testing of systems is often done by security researchers who are hired by an organization to look for weaknesses in their systems. According to Maurushat (2014), these security researchers will not be subject to criminal sanctions because in the view of the law this will be proper authorization. The legal ambiguity grows when the same researcher comes across a vulnerability in its spare time, which he or she further examines without consent or authorisation from the system’s owner (Falot & Schemer, 2016). When disclosing such vulnerabilities, researchers risk criminal consequences and in many cases, will be found guilty of computer intrusion (Falot & Schermer, 2016). Nevertheless, it does not automatically mean that when one finds and discloses vulnerabilities, one will be prosecuted or face criminal indictment. This is mainly depended on prosecutorial will (Maurushat, 2014). The focus of this thesis will be on the latter, the so-called ethical hackers, which find vulnerabilities without the consent of the organization with as aim to make information systems more secure by responsibly disclosing vulnerability information to the system’s owner. As will be discussed later, there are several forms of vulnerability disclosure, but the legality of all these forms of vulnerability disclosure is not in dispute; it is illegal.

Finding and disclosing vulnerabilities can thus be seen as legally and morally ambiguous (Maurushat, 2014). According to Falot & Schermer (2017), Tavani (2007), Maurushat (2014) and Schuster et al. (2017), the practice of vulnerability disclosure and ethical hacking, should not be illegal per se when an ethical hacker finds and discloses the vulnerability in a controlled and responsible manner. They argue that reporting and fixing flaws timely is essential for cybersecurity and benefits society by increasing the security of information systems (ENISA, 2015; Falot & Schermer, 2016; Maurushat, 2014). This is the case when the information about the vulnerability will be shared directly with the organization, and this organization will be given a deadline to fix the vulnerability before the vulnerability will (possibly) be, in joint consultation, disclosed to the public (Falot & Schermer, 2016). This is called coordinated vulnerability disclosure (CVD), which will be discussed in-depth in Paragraph 2.3. Besides that, the threat of being sued in the current situation does not stimulate ethical hackers to report and disclose vulnerabilities responsibly. It rather stimulates and sustains the selling of vulnerabilities on the black market (Baumbauer & Day, 2010; Schuster et al., 2017). It can be argued that an 'ethical' intention would be sufficient in the absence of authorization since it does not change the common higher cause of improving the overall security of information systems (Matswyshyn et al., 2010; Maurushat, 2014).

The study of Falot & Schermer (2016) will briefly be discussed to illustrate the arguments about the situation in the EU. They analyzed the situation of ethical hacking and vulnerability disclosure in the Netherlands, Belgium and Germany. In all three countries, all forms of hacking are illegal, and there is no legal concept of ethical hacking.

In the Netherlands, a letter of the Dutch Public Prosecutor (DPP) has significantly increased the position of ethical hackers. The DPP stipulated that ethical motives and proportionality will be considered in cases of hacking. In Germany computer intrusion is an *antragsdelikt*, meaning that enforcement will only take place when an organization reports it. In Belgium, the motives of the ethical hacker are not relevant because there are no formal grounds for exclusion in the law. This is underlined by the Belgian Federal Public Service: "hackers that from the outside without authorization enter computer systems are always punishable, even when this is done with the right intentions" (www.belgium.be). These examples illustrate the legal fragmentation in the EU and make disclosing vulnerabilities crossing borders a risky endeavor (Falot & Schermer, 2016).

2.3. WHY IS VULNERABILITY DISCLOSURE RELEVANT FOR THE EU?

Looking closely at the relevant EU cyber strategies and documents that have been published the past years, the recurring message is that the EU wants to increase its cyber resilience and strongly reduce cybercrime (EC, 2013, 2016d; European External Action Service (EEAS), 2016; ENISA, 2015). The resilience of information systems is crucial for successfully completing the Digital Single Market (DSM) and ensuring the smooth functioning of the internal market (Tauwhare, 2016). The largest challenges for EU regulation in the cyber domain are the facts that the global information space does not respect national boundaries, technology develops rapidly, and many public and private actors are involved (Carr, 2016; Summers, 2015). Particularly, this cross-border dimension of cyberspace justifies EU actions in this domain (Summers, 2015).

One of the problems with strengthening the security of information systems is that vulnerabilities are already part of those when offered on the market (Mason, 2012). According to various sources (ENISA, 2015; National Cyber Security Centre (NCSC), 2015a; Tai & Koops, 2015), it is unlikely that this issue will be resolved anytime soon because in practice it is tough for developers to avoid vulnerabilities as information systems are built on huge amounts of complex lines of codes.

2.3.1. COORDINATED VULNERABILITY DISCLOSURE, MOST DESIRABLE?

One way to address this problem is to strengthen the EU's cyber resilience by using the tool of CVD. There are three different forms of vulnerability disclosure with its own pros and cons that are subject to debate for many years now: full-disclosure, non-disclosure and CVD (see Figure 1) (Arora & Telang, 2005; Berinato, 2007; Cavusoglu et al., 2005; ENISA, 2015; Falot & Schermer, 2016; Matwyshyn et al., 2010; NCSC, 2015a; Parker et al., 2004; Preston & Lofton, 2002; Schneier, 2000; Laakso, Takanen & Röning, 1999; van der Meulen, 2016).

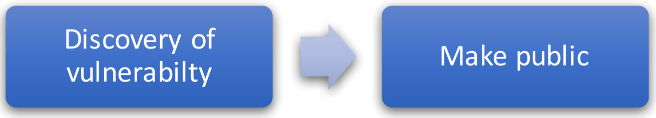


Figure 1a. Schematic overview of full-disclosure process.

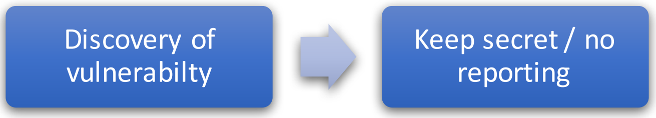


Figure 1b. Schematic overview of non-disclosure process.

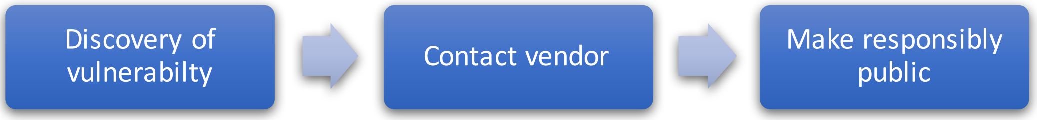


Figure 1c. Schematic overview of coordinated vulnerability disclosure process.

Full-disclosure is the term used for publically disclosing vulnerabilities without contacting the system's owner. It is based on the idea that vulnerabilities will be patched quicker through naming and shaming (Cavusoglu et al., 2005; NCSC, 2015a; Shepherd, 2003). In the long run, this could be an incentive to make properly designed, tested and secured by design products (Ellis, 2015; Preston & Lofton, 2002; Ryan & Heckman, 2003). It is thus rather a correction mechanism if companies do not want or do not fix the vulnerability quickly enough. Full-disclosure is seen as irresponsible and reckless because it provides a window for the vulnerability to be exploited for illegal purposes (Schneier, 2000; Ranum, 2008). Consequently, there is a significant risk that governments, companies or users are harmed – directly or indirectly (Cavusoglu et al., 2005; Ellis, 2015; Freeman, 2007; NCSC, 2015a).

Non-disclosure refers to the approach of keeping the vulnerability information secret so that the public never knows about the vulnerability, leaving systems vulnerable to exploitation until the information becomes public and the vulnerability is patched (Cencini et al., 2005; Shepherd, 2003). Non-disclosure has more disadvantages than advantages: it is argued that it does not provide a guarantee that the vulnerability is not already discovered by black hats and the risks for system's users are severe (Ellis, 2015; Zina, 2009).

CVD presents a middle way in which both the vendor and the ethical hacker can come to terms to ensure the security of information systems for society (Stone, 2003). It refers to the approach of disclosing vulnerabilities in information systems in a controlled and responsible manner (Falot & Schermer, 2016; Timmerman, 2013) where the vendor is first contacted about a vulnerability in their systems before going public enabling patching and preventing exploitation of the vulnerability (Ellis, 2015; NCSC, 2015a). A CVD policy[5] is based on a set of best practices about how the cooperation between ethical hackers and vendors should work to protect the users and prevent negative consequences of vulnerabilities (National Telecommunications and Information Administration (NTIA), 2016). Main elements of a CVD policy are the agreement that the ethical hacker will not publish details of the vulnerability before it is solved, and the affected organization promises that no legal action will be taken if the policy is followed (NCSC, 2016). In practice, after a specified time-limit – between 45 and 60 days is common – the vulnerability will be publicly released regardless of the vulnerability is patched by the vendor (Cavusoglu et al., 2005; Ellis, 2015). CVD is the most desirable approach because it has the least adverse consequences for governments, vendors and users. Moreover, nor the vendor or the ethical hacker can accuse the other of

[5] In Annex 1 and 2, two examples of CVD policies in practice are presented.

irresponsible behavior in a CVD process (Stone, 2003). The vendor will be given a strong incentive to fix the vulnerability without jeopardizing the security of information systems as is the case with full disclosure (Schiller, 2002). CVD offers a way for ethical hackers to straddle two worlds: "it allows them to receive prized recognition of their elite skills within the community of hackers, while signaling to corporate players that have lucrative security contracts to fill that they are in fact responsible actors" (Ellis, 2015, p. 6). A well-designed CVD policy is of critical importance to increase the security of information systems, counter cybercrime and lighten the workload of law enforcement (Maurushat, 2014; Schuster et al., 2017). Governments should, therefore, stimulate the use of CVD policies (Cavusoglu et al., 2005).

In this thesis, the term CVD will be used instead of the original name responsible disclosure. The latter was disapproved because it implies that only the ethical hacker is responsible, while both the ethical hacker and the vendor have responsibilities (NCSC, 2015a). Moreover, ethical hacking and CVD will be used interchangeably because they are closely intertwined and both about responsibly disclosing vulnerabilities.

2.3.2. EU'S FRAGMENTED LEGAL LANDSCAPE FOR ETHICAL HACKERS

The legal landscape is still fragmented on EU-level which makes it harder to implement a well-functioning CVD policy. Moreover, it does not stimulate ethical hacking and thereby the legal search for vulnerabilities (ENISA, 2015; Schuster et al. 2017). Operating in this area means that you risk being prosecuted on a broad range of laws, among others: "criminal law for hacking, civil liability, breach of contract and copyright issues" (van der Meulen, 2016, p. 8). However, it should be noted that even if MS acknowledge the services of ethical hackers, an ethical hacker can still be prosecuted in another MS, even when its activities are legal in the home MS because of the lack of EU harmonization (ENISA, 2015; Falot & Schermer, 2016). This can be a major reason for the EU to act as has also happened in aviation sector[6].

In Chapter 5, an overview will be given of the relevant strategies, regulations and policies on the EU level relevant for a discussion about CVD, most notably the Convention on Cybercrime (CoC) and the Directive on Attacks against Information Systems (AIS).

In the last years, an increasing amount of MS have taken measures or are actively considering the possibilities to increase the legal certainty of ethical hackers by

[6] See EU (2014a) on the reporting, analysis and follow-up of occurrences in civil aviation.

implementing national frameworks for CVD or using other means. The Netherlands[7] and Finland[8] have been active proponents of CVD for a couple of years now. Belgium[9], Italy[10] and Latvia[11] are currently working on a national framework for CVD. France[12] and the United Kingdom (UK)[13] have chosen to create a certification scheme for ethical hackers. Besides that, Hungary, Romania and the Netherlands are involved in a so-called cyber capacity building initiative to share CVD best practices about how to set up a national framework in support of less-developed countries (www.thegfce.com).

2.4. CONCLUSION

It is important to note that vulnerabilities are already part of information systems offered on the market leaving governments, companies and users vulnerable. A solution for the EU to increase its cyber resilience would be to decrease the number of vulnerabilities by making it harder for actors to misuse information systems for illegal purposes. The EU could achieve this by making use of the unsolicited services of ethical hackers and stimulate CVD, which is the most popular form of vulnerability disclosure among the EU and its MS, vendors and many ethical hackers. However, stimulating CVD is hard because all forms of hacking are illegal according to a wide variety of laws in the EU and the legal landscape in the EU is fragmented. Nevertheless, there are many arguments why the activities of ethical hackers and well-designed CVD policies should be stimulated in the EU to strengthen the security of information systems and thereby strengthen the EU's cyber resilience. In the next Chapter the methodology will be discussed.

[7] The Netherlands is one of the fore-runners in Europe according to ENISA (2015). The Netherlands actively distributes the idea of CVD, has an own CVD policy, a letter of the Public Prosecution Service about how they would deal with cases of CVD and a guideline for companies how to implement it (NCSC, 2013, 2015a; Openbaar Ministerie, 2013).

[8] Finland's national CERT (CERT-FI) is already playing an active role for some years now in vulnerability disclosure (ENISA, 2015).

[9] The Belgium Minister of Justice has pledged, in response to parliamentary questions, that the Cybersecurity Centrum Belgium will in 2017 present a manual for responsible disclosure (van Leemputten, 2016).

[10] Italian Digital Team has started working to define and publish a national policy for responsible disclosure in collaboration with CERT Nationale and CERT-PA (Bajo & Varisco, 2016).

[11] Latvia is chosen because they are currently working on a CVD policy and intend to put it into law of which it is the first country in the world to do this (Bergman, 2015).

[12] More information on https://www.ssi.gouv.fr/en/regulation/eidas-regulation/trusted-list/.

[13] NCSC-UK works closely together with CREST (non-profit organization which certifies ethical hackers) and has recently launched the NCSC Vulnerability Co-ordination pilot (T, 2017).

3. METHODOLOGY

This thesis will use a qualitative approach because it is about understanding and explaining the complex relations and interests of a wide variety of actors in a complex context and environment (Creswell, 2012; Denney & Tewksbury, 2013; Miller & Yang, 2007) – the cyber ecosystem of the EU. The study object cannot be expressed in numbers, causally determined and predicted, and therefore a quantitative approach is not suitable (Algozzine & Hancock, 2006). Moreover, a qualitative approach is useful because the subject of this thesis is a relatively new area of research and it provides an opportunity to look in detail at the current situation in the EU concerning cybersecurity and resilience.

A single policy study design will be applied, which is one of the most used forms of EU research (Kronsell & Manners, 2015). Single policy studies are used to understand the role the EU plays in a domain and can provide for public policy prescriptions. Advantages of this method are that the choice of method or theory is not determined, it can be used to give a critical academic perspective on public policy and allows for acquiring in-depth knowledge of processes, actors and factors relevant to a specific policy (Kronsell & Manners, 2015). This thesis will employ a pragmatic and critical approach constructed by Christou (2016) which blends literature on resilience and security governance to create a security as resilience approach.

Furthermore, a hybrid form of theory applying analysis will be used (Kronsell & Manners, 2015) – combining a contemporary policy-descriptive and policy-prescriptive perspective focusing on current developments and conditions (van Evera, 1997). Description must precede prescription and therefore it is necessary to be descriptive first because little is known about the subject of cyber resilience and CVD (van Evera, 1997; Yin, 2013). Moreover, policy-prescriptive analyses are very well suited to present options for future public policies, although, there are some criticasters that state policy-prescriptive analysis is not theoretical enough (Kronsell & Manners 2015). This is countered by the fact that all policy proposals are based on forecasts about the effect of policies (van Evera, 1997). Therefore, it is important that in this thesis projections are substantiated with strong arguments and build upon a clear theoretical framework. To go beyond a purely descriptive thesis, the analysis in this thesis will focus on how and which different regulatory instruments the EU may use to properly facilitate vulnerability disclosure in the context of Morgan and Yeung's (2007) theoretical framework of regulatory instruments. This is placed in the broader context of conditions for the EU to become cyber resilient based on insights of Christou (2016).

Besides that, to build a strong argument and combine technical and non-technical perspectives, a literature review of secondary literature will be combined with an analysis of a wide variety of primary documents in Chapter 4 – 6 to. Among others, EU and MS documents (e.g. policies, regulations, strategies), industry best practices and non-EU examples of facilitating CVD will be used. Primary sources are an essential condition for a proper research and will be used to get as much information as possible on the table (Algozzine & Hancock, 2006; Moumoutzis, 2011; Trachtenberg, 2009). In this thesis, an analysis of primary sources is appropriate because it will provide meaningful and original options for the EU to facilitate vulnerability disclosure, which is not available in secondary documentation.

The suggested approach also has some limitations. The first is inherent to a single policy study with a focus on EU policy and is about setting boundaries (Denney & Tewskbury, 2013). Due to the multilevel and multi-state context of EU policy, a broad variety of actors, levels and institutions are involved, which makes it hard to decide on the research's scope (van der Vleuten, 2012). It is important to use clear theoretical concepts and frameworks to guide the study (Yin, 2003). For that reason, the focus will only be on the instrument of CVD in the context of an EU that wants to become cyber resilient. Other instruments that can also limit the number of vulnerabilities and contribute to the EU's goal such as security by design and the development of certification schemes will be disregarded. An accompanying disadvantage is that the study does not per se consider the larger (political) context and related developments in other sectors (Kronsell & Manners, 2015). Besides that, prescriptions will always be a forecast build upon the current situation, but due to factors such as the fast development of technology, evolving threat landscape and political situation in MS and the EU, it will be hard to predict the effectiveness of proposed instruments. Lastly, the analysis of primary sources can have some limitations because only public documents in a few EU languages can be studied, while many MS still publish governmental documents in their native language and there is still much secrecy surrounding cybersecurity issues.

4. THEORETICAL FRAMEWORK

The EU has the ambition to increase the EU's cyber resilience but does not adequately define and deconstruct what cyber resilience is and which governance forms are necessary to achieve it. In the first paragraph, this thesis will be placed in the broader body of literature on cybersecurity. This will be followed by discussing the essential preconditions for creating a resilient cyber ecosystem and how this can be understood and analyzed. In the third paragraph, these ideas are combined with four categories of regulatory instruments the EU can use to strengthen its cyber resilience.

4.1. LITERATURE ON THE EU AND CYBERSECURITY

There is no abundance of theoretically informed literature focusing on cybersecurity and cybercrime. This body of literature is, however, growing quickly. The same goes for related literature about cyber warfare, cyber defense and cyber terrorism. The latter are outside the scope of this thesis and will not be further discussed.

The main body of literature on cybersecurity uses traditional and critical theories of International Relations such as the concept of cyber power (Betz & Stevens, 2011; Klimburg, 2011; Klimburg & Tiirmaa-Klaar, 2011; Nye Jr, 2010; Sliwinski, 2014) and securitization of cyber issues in the UK the US (Eriksson 2001; Bendrath, Eriksson & Giacomello, 2007; Dunn Cavelty 2007, 2008). Betz and Stevens (2011) and Nye Jr (2010) focus on cyber power, state strategy and the use soft and hard powers by states to counter cyber threats. They acknowledge that the importance of non-state actors and network governance is growing but reach the conclusion that states are still most powerful in the cyber domain. Klimburg (2011) rather believes that the third dimension of cyber power –public-private cooperation – is most valuable looking at the nature of cyberspace (Klimburg, 2011). Particularly because of the many actors involved, fast technological developments and the privatization of critical infrastructures (Carr, 2016). Betz and Stevens (2011), Nye Jr (2010) and Klimburg (2011), however, mainly assess the issue of cybersecurity from a traditional international relations perspective as a new area of conflict between the great powers. If they address the EU at all, it is about the resilience of the EU vis-à-vis other great powers and not about cyber resilience inside the EU.

Few authors do address the EU and cyber resilience within the EU. Klimburg and Tiirmaa-Klaar (2011), for example, argue that the public-private cooperation dimension in the EU is underdeveloped and should be strengthened. This is underlined by Swilinksi (2014), who argues that the EU, its MS and other non-state actors must work together and create a collective vision to strengthen cybersecurity. Moreover, works on cybersecurity (Bossong & Wagner, 2016; Carrapico & Barrinha, 2017; Christou, 2014, 2016; Klimburg & Tiirmaa-Klaar, 2011; Schellekens, 2016; Sliwinski, 2014; van der Meulen, Jo & Soesanto, 2015) and public-private cooperation in cyberspace remain rather limited (Carr, 2016; Dunn Cavelty, 2013, 2014).

These works do not address forms of hacking and vulnerability disclosure in the EU. In general, the concepts of ethical hacking and vulnerability disclosure are under-researched from non-technical perspectives, while in the technical literature it are no new phenomena (Cavusoglu et al., 2005; Laakso et al., 1999). Most books on (ethical) hacking and vulnerability disclosure are manuals (e.g. Engebretson, 2013; Graves, 2010; Harper et al., 2011) or use a quantitative approach looking at statistics of vulnerability disclosure to assess whether the process is effective (Algarni, 2016; Böhme, 2006; Cavusoglu et al. 2005; Havana, 2004; Arora, Telang & Xu, 2008). Moreover, a limited body of works focus on the ethical aspects (Dudley, Braman & Vincenti, 2012; Matwyshyn et al., 2010; Maurushat, 2014; Takanen et al., 2004; Wolfs & Fresco, 2016) or legal aspects of vulnerability disclosure in the US (Baumbauer & Day, 2010; Bergman, 2015; Preston and Lofton, 2002; Schwartz & Knake, 2016).

Unfortunately, all listed literature does not bring the technical and the non-technical (e.g. policy, legal and political) worlds closer together. It is often argued that it is essential for policymakers to bridge the gap between these two worlds because both sides need each other to develop effective and efficient cybersecurity policies (OECD, 2012; Kleiner, Nicholas & Sullivan, 2013). Besides that, the non-technical side of vulnerability disclosure and ethical hacking is still under-researched. Some positive exemptions are Falot & Schermer (2016) who analyzed the legality of ethical hacking in cross-border cases in the EU; Schellekens (2016) who investigated whether car hacking should be regulated in the EU and US, and if so how this could be done; and Christou's book (2016) which integrates ideas about resilience, ecosystems and security governance, and applies these to cyber issues in the EU. The latter will be discussed in the next paragraph.

4.2. UNDERSTANDING CONDITIONS FOR DEVELOPING A RESILIENT CYBER ECOSYSTEM

Resilience can be "understood as the capacity of different layers of society to withstand, to adapt to and to recover quickly from stresses and shocks and has gradually emerged as the answer to the growing complexity of the international security environment" (Pawlak, 2016, p.1). A resilient state is not immune to challenges but can respond flexibly and rapidly to guarantee an appropriate level of state functioning (EUISS, 2017).

Christou (2016) is one of the first that used notions of resilience and applied these to the cyber domain, academically introducing cyber resilience. The concept of cyber resilience has returned in various EU documents without properly defining what this concept entails (EC, 2013, 2016). Christou's (2016) framework helps to explain "the evolution of the EU governance system for cybersecurity to provide a deeper understanding of how the EU can construct an ecosystem of resilient security governance" (p. 12), which is "underpinned by instruments, tools and mechanisms that allow the EU to achieve a more secure cyberspace" (p. 21).

Christou's (2016) framework combines concepts of resilience and security governance to develop a *security as resilience* approach (Kavalski, 2009, p. 532). The security as resilience approach does not only look at governance mechanisms applicable to cybersecurity but rather provides an understanding of the instruments, relationships, characteristics and processes that can stimulate the development of a cyber resilient EU. This approach is more suitable to the issue of cybersecurity than the traditional concept of *security of control* that only focuses on change within and between systems (Webber et al., 2004; Kirchner and Sperling, 2007; Wagnsson, Sperling & Hallenberg, 2009). In resilient systems, it should be possible for new adaptable regime(s) to develop in reaction to new conditions and incentives (Handmer and Dovers, 1996). Handmer & Dovers (1996), introduced three typologies of resilience as displayed in Table 1.

Table 1
Typologies of Resilience

Type		Characteristics
1.	**Resistance and Maintenance**	Sovereignty, hierarchical governance, state control of information, resistance change
2.	**Change at the Margins**	Risk management underpinned by traditional linear risk assessment, acknowledgement of problems & need for change, problem-solving approach, no transformability but effect outcomes at the margins, addressing symptoms instead of cause
3.	**Openness and Adaptability**	Partnerships, flexibility, adaptability, address causes, self-regulating, non-hierarchical

Note. Based on information from "A typology of resilience: rethinking institutions for sustainable development", J. Handmer & S. Dovers, 1996, *Organization & Environment*, *9*(4), 495-499).

Typology 3 is most suitable to reflect on the resilience of the developing ecosystem of resilient cybersecurity governance in the EU. It is "characterized by flexibility and the ability and preparedness to adopt new basic operating assumptions and institutional structures" (Handmer & Dovers, 1996, p. 602). From a governance perspective, it shall lead to a significant change in power relationships, participation and inclusiveness – self-organized and non-hierarchical. Actors are expected to seize new ideas and embark major changes in developing an ecosystem that can decrease its vulnerability to threats.

Another feature of Type 3 is that its success depends on to what extent the coalitions of actors can work together to tackle the problems occurring in cyberspace (Christou, 2016). Not only dealing with the symptoms but also with the causes of cybersecurity problems at all levels. Moreover, it helps us to understand the characteristics and relationships that originate in the cyber ecosystem of the EU and enables an analysis of the general conditions that are necessary for creating a resilient cyber ecosystem in the EU (see Table 2).

Table 2
Conditions for developing a resilient cyber ecosystem

Ability (including resource and mandate) and preparedness to adopt new basic operating assumptions and institutional structures;
Assumption of efficiency abandoned in favour of complexity in governance logics in order to avoid single points of threat and failure;
Coalitions of actors working together in 'partnerships' based on trust to share information, construct new flexible and adaptive institutions and operating procedures, set the agenda and construct/implement policies;
Convergence amongst stakeholders on a 'common' understanding, logic(s), 'norms', laws and standards of security as resilience;
Evolution of a culture of cybersecurity at all levels and layers (technical, legal, policy) among all stakeholders (awareness, education, learning and so on);
An integrated approach (coherence and consistency across layers, levels, actors).

Note. Conditions for achieving effective security as resilience in cyberspace. Adapted from "*Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*", by G. Christou, 2016, New York, NY: Palgrave Macmillan.

The framework of Table 2 is very suitable for this thesis because it attaches great value to collaboration between stakeholders and the unique nature of cyberspace where different public and private actors are involved which calls for coordination and communication (ENISA, 2015; Schellekens, 2016).

4.3. FOUR REGULATORY INSTRUMENTS FOR THE EU

Legislation in cyberspace is no silver bullet and developing a resilient cyber ecosystem is not something which can be achieved solely by legislation (Dunn & Cavelty, 2009; Schellekens, 2016). The relationship between black hats and those that try to decrease vulnerabilities is characterized by competition: an arms race between those that are looking to discover and exploit vulnerabilities versus those that seek to solve vulnerabilities. The consequence of this relation is dynamism which makes it very hard to regulate in this domain (Schellekens, 2016). Consequently, governments should not legislate without involving other actors as is in line with the ideas of Christou (2016) about a resilient cyber ecosystem.

Christou’s framework will be combined with four categories of regulatory instruments developed by Morgan and Yeung (2007) to analyze which policy options the EU can use to strengthen the resilience of its cyber ecosystem through CVD. Morgan and Yeung (2007) have combined insights from a wide range of academic disciplines. One important common element of all this literature is that they all try “to understand and explore instruments and techniques by and through which social behavior may be regulated, and the relationship between those techniques and their context” (Morgan & Yeung, 2007, p. 79). They emphasize that the framework not explains regulation, but rather reviews how to regulate. Morgan and Yeung (2007) introduce five groups of regulatory instruments with its accompanying modalities in which they try to control behavior: “command, competition, consensus, communication and code (or architecture)” (Morgan & Yeung, 2007, p. 80).

The code-based instruments are based on works of Lawrence Lessig (1999, 2006). He argues that regulation in cyberspace can perfectly reach its goals by changing software codes, foreshadowing the idea that “law as code is the start to the perfect technology of justice” (Lessig, 1999). This group of instruments will not be used for further analysis because the EU or its MS cannot provide code itself because of the nature of the cyber domain. It goes beyond the scope of this thesis to discuss how governments can sway the international private sector to develop hundred percent secure code (Brownsword, 2005).

Furthermore, the boundaries between these four instruments are not watertight, and many instruments can use different mechanisms and are thus rather hybrids (Morgan & Yeung, 2007). Moreover, no single instrument will provide the solution, rather a broad lens and a right mix of instruments is needed to increase cybersecurity in the EU (Schellekens, 2016).

4.3.1. COMMAND

This category of mechanisms includes the creation of laws by governments to regulate and compel specified behavior, supported with coercive sanctions if the rules are violated (Morgan & Yeung, 2007). This refers to traditional command-and-control regulation wherein the government creates laws to achieve policy objectives (Daintith, 1997). Important in the EU is that regulation should adhere to the principles of subsidiarity and proportionality: the EU must show that it can better solve the problem than the MS, and EU action must not go further than required to achieve the objective (Chalmers & Arnull, 2015).

Command-and-control rules are important but are most suitable to set the framework. Actual security measures and effective regulation, especially in the cyber domain, requires detailed and practical information which is usually not available to the legislator. Close collaboration with stakeholders is, therefore, essential. Self-regulation can provide a solution and build upon command rules (Morgan & Yeung, 2007; Schellekens, 2016).

4.3.2. COMPETITION

The last decades, command-based instruments have lost their attraction because of a wide range of shortcomings such as high costs, negative incentives and difficulties when used in cases of uncertainty (Morgan & Yeung, 2007; Ogus, 1994) – one of the major characteristics of cyberspace. In cyberspace, technological developments evolve quicker than regulation, which increases the level of uncertainty about the effectiveness of these rules.

Competition is about the group of instruments that use the competitiveness of markets to regulate social behaviour. This does not mean the law is not involved: it can play a vital facilitative role (Morgan & Yeung, 2007). Relevant (economic) instruments in this regard are: "charges, taxes, subsidies, . . . , liability rules" (Schellekens, 2016, p. 312). In short, charges and taxes are used to correct misallocations derivative of externalities (Morgan & Yeung, 2007). Subsidies are the positive opposite: money is given to motivate actors to decrease undesirable behavior. Liability rules can help to ensure a higher level of security and safety users would receive without these rules (Breyer, 1982).

4.3.3. CONSENSUS

Law also has a facilitative role in the third broad group of regulatory instruments: Consensus. The biggest difference with the other groups of instruments is that these build upon the consent of its participants. Moreover, sanctions for violating consensus instruments are, for example, social disapproval or ostracism, rather than legal coercive sanctions. The threat of law is still present in some form but can also be constructed with the consent of the community (Morgan & Yeung, 2007). Regulation could help to build trust between public and private actors and create the frame in which information could be exchanged between actors (Schellekens, 2016). There are a wide variety of consensus-based instruments, but the focus will be on two variants: self-regulation and public-private partnerships (PPP). One of the big advantages of self-regulation and PPP is that the expertise of the private sector can be fully utilized. Cybersecurity is a highly technical subject and, therefore, it can be a good area for self-regulation (Schellekens, 2016). A pitfall of self-regulation can be its liability to regulatory capture: cybersecurity is not always on the top of mind of companies and a regulatory capture looms (Ogus, 1995; Schellekens, 2016).

4.3.4. COMMUNICATION

The power of social norms and consensus are underpinning the power of the communication-based instruments. These instruments regulate behavior by improving the information vis-a-vis the target audience and thereby make it possible for them to make more informed choices about how to behave. Consequently, "the aim is therefore to bring indirect social pressure to bear on individual decision-making in the hope that it will lead to behavioral change" (Morgan & Yeung, p. 96). Communicative regulatory instruments are, for example, public education campaigns, mandatory and voluntary disclosure regimes, public communication management, and transparency measures (Yeung, 2005).

4.4. CONCLUSION

Blending the ideas of resilience and security governance gives valuable insights in the EU's developing cyber ecosystem. Table 2 and the concept of security as resilience provides more understanding about how the EU can strengthen the resilience of its cyber ecosystem paying attention to the involved actors, networks, institutions and instruments. It is important that the EU can quickly adapt and react to new technological developments and fast changing threat landscapes. This framework will be used to analyze the role the EU plays and should play in the cyber domain and sketches the context in which there will be zoomed in on the CVD process and the four possible instruments the EU can use to stimulate this. It should be noted that this model is fluent and many instruments are based on more than one mechanism to regulate behavior, so-called hybrid instruments.

5. EU STRATEGIES, REGULATIONS AND INTERNATIONAL NORMS

Before continuing to the analysis of possible options for the EU to stimulate ethical hacking and CVD, it is important to review which legislation is already in place relating to (ethical) hacking and CVD to assess whether extra measures are necessary. Consequently, this Chapter will focus on the relevant EU strategies, regulations and EU's agreements in multilateral fora important for stimulating CVD.

5.1. EU POLICIES AND STRATEGIES

Over the past few years, many documents have been published that guide the EU activities concerning cybersecurity, including the:

1. European Cybersecurity Strategy (EC, 2013);
2. European Agenda of Security (EC, 2015a);
3. Digital Single Market Strategy (EC, 2015b);
4. Joint Framework on Countering Hybrid Threats a European Union Response (2016a);
5. The EU's Global Strategy for its Foreign and Security Policy (EEAS, 2016);
6. Communication on Strengthening Europe's Cyber Resilience System (EC, 2016d).

For the EC, there are three top priorities concerning cybersecurity for the coming years: increasing cybersecurity capabilities in the EU and strengthen cooperation; making the EU a strong (international) player in cybersecurity; and mainstream cybersecurity in EU policies (EC, 2017a).

5.2. EU REGULATIONS

Several regulations have been adopted and are implemented, or currently being implemented by the EU, of which the most relevant for cybersecurity and CVD are the:

1. **Directive on Attacks against Information Systems (AIS)** (EU, 2013) which has been fully implemented on September 2015 and builds upon the Convention on Cybercrime (CoC). It focuses on cybercrime.
2. **The General Data Protection Regulation (GDPR)** (EU, 2016a) which applies from 25 May 2018 with as focus data protection.
3. **Directive on Network and Information Security (NIS)** (EU, 2016b) which needs to be implemented before 9 May 2018 and focuses on cybersecurity.

5.2.1. EU CYBERCRIME REGULATION

As mentioned before, ethical hackers face legal uncertainty when disclosing vulnerabilities, particularly because of the criminalization of hacking in the CoC (Council of Europe, 2001)[14] and the AIS Directive (EU, 2013). The CoC is signed by all 28 EU MS[15] and is built on the idea that there should be some degree of global harmonization if effective cybercrime regulation is to be achieved (Clough, 2014).

Consequently, finding a vulnerability and responsibly disclosing this as ethical hacker will be punishable because, among others, it can qualify as a form of unauthorized access (art. 2 CoC; art. 3 Dir AIS), illegal system interference (art. 5 CoC; art. 4 Dir AIS), or illegal data interference (art. 4 CoC; art. 5 Dir AIS). Mandated testing of an information system on request of a company or vendor is exempted from criminal liability according to the AIS Directive. In both the CoC and the AIS Directive there is no public interest exemption included. This means there is no exception that unauthorized access or modification can be justified by an overriding public interest (Maurushat, 2014). The only absolute is that it is unsettled and vulnerability disclosure – responsible or not – could expose a discoverer of a vulnerability to criminal sanctions and civil liability (Maurushat, 2014). However, according to Maurushat (2014), “we must always believe that the application of law is reasonable and that there are many mitigating factors the legal system would take into account” (p. 51). In Chapter 6, it will be further discussed what mitigating factors can be and how these can be shaped.

Moreover, the AIS Directive was an attempt of the EC to harmonize criminal codes related to cybercrime (Summers, 2015). There was a broad consensus on the need for harmonization; however, it remains questionable whether harmonization is possible in this area. The evaluation of the previous Framework Decision (EU, 2005) which has been replaced with the AIS Directive showed different interpretation and implementation among the 20 MS back then (Summers, 2015). On 4 September 2017, the EC will submit an evaluation report on the implementation of the AIS Directive which will show whether the AIS Directive did lead to more harmonization of criminal codes related to cybercrime (EU, 2013). Until today, both the CoC as the AIS Directive have thus not resulted in more legal certainty for ethical hackers or stimulation of CVD. MS still have various interpretations of how to judge CVD from a

[14] Often called the Budapest Convention on Cybercrime.

[15] But has not been ratified and entered into force in all 28 MS: Ireland and Sweden have not yet done so (www.coe.int).

criminal law viewpoint and do not have specific legislation or jurisprudence that demonstrates how CVD is approached in practice (Biancuzzi, 2008; ENISA, 2015).

5.2.2. EU CYBERSECURITY REGULATION

The NIS Directive (EU, 2016b) is the first EU-wide cybersecurity regulation (Tauwhare, 2016). It is based on a form of minimum harmonization which leaves many details to be decided on by individual MS with the accompanying risk of less impact (Tauwhare, 2016). The Directive is a significant step forward to increase the EU's cyber resilience and construct a joint response to cyber threats in the EU (Tauwhare, 2016). The legal basis of the NIS Directive is Art. 114 TFEU[16] and its aim is "achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market" (EU, 2016, p. 11). The NIS directive is based on three main pillars (EU, 2016):

- Guarantee MS readiness by requiring equal baseline levels of security;
- Ensure cooperation among all MS by creating the:
  - Cooperation Group to facilitate strategic collaboration and information exchange among MS;
  - Computer Security Incident Response Team (CSIRT)[17] Network to stimulate effective operational coordination in the case of specific cybersecurity incidents and information exchange about risks;
- Guarantee a culture of security across vital sectors by:
  - Introducing a duty of care for operators of essential services under the NIS Directive to take appropriate measures;
  - Making it mandatory for operators of essential services to report serious incidents to the relevant national authority.

It is up to MS to decide which organizations in their country fall under the NIS Directive's definitions of operators of essential services (EU, 2016b). The NIS Directive also introduces slightly different notification and security requirements for digital service providers. For clarity sake, these will be disregarded because it will not change anything for the analysis. CVD is not directly mentioned in the NIS Directive but could be a useful instrument

[16] Art. 114 TFEU is the legal basis for EU action in this area under the denominator of harmonization of laws to ensure the proper functioning of the internal market.

[17] The terms CSIRT and Computer Emergency Response Teams (CERT) are often used interchangeably. A CSIRT is "a team of experts that responds to computer security incidents" (IGF, 2014). The current term used by ENISA is CSIRTs because it better underlines other activities CSIRTs perform nowadays on top of solving incidents (ENISA, 2006; IGF, 2014).

supporting the goal of the Directive to achieve a common level of cybersecurity and give substance to the duty of care for operators of essential services. More leads are (EU, 2016b):

- Recital 4 emphasizes the importance of stimulating a culture of risk management and the implementation of necessary security measures to achieve this;
- Recital 44 states that responsibilities for guaranteeing network security lies, to a great extent, with the operators of essential services themselves;
- Article 3 stipulates that MS can implement additional measures to achieve a higher level of security.

The options the NIS Directive provides for stimulating CVD will be discussed in Chapter 7.

5.2.3. EU DATA PROTECTION REGULATION

The GDPR (EU, 2016a) "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data" (EU, 2016a, p. 108). It is beyond the scope and not relevant for this thesis, to discuss this 261 pages long Regulation in depth. Concerning CVD, one element is of particular importance. Organizations in violation of the GDPR can receive a fine up to 4 % of their annual global turnover for the most severe infringements, and a fine of 2 % of their turnover if they have not implemented appropriate measures to guarantee the security of personal data (EU, 2016a). It is not clear yet what will be assessed as appropriate measures by national supervisory authorities. Nevertheless, this can be an extra reason for organizations to implement a CVD policy to stimulate the search for vulnerabilities in their information systems. Thereby, they decrease the risk of exploited or publically announced vulnerabilities, which could prevent organizations to lose data and possible subsequent fines.

5.3. INTERNATIONAL NORMS

It is important to shortly elaborate on the EU's and its MS' activities in multilateral fora to outline the international context and relevant agreements affecting the EU's cyber activities and CVD. The CoC has already been discussed in this Chapter.

Firstly, the United Nations Group on Governmental Experts (UN GGE) on Developments in the Field of Information and Cyber Telecommunications in the Context of International Security is an influential group of 25 states[18] that aim to build consensus on the applicability

[18] The list of participants is secret, however in previous UN GGE's (2009/2010; 2013/2014) several influential EU MS were participating (www.un.org).

of international law, norms of responsible state behavior, and confidence building measures (CBMs) in cyberspace. The UN GGE has already produced three reports (2011, 2013, 2015) and the discussions about a new one in 2016-2017 have ended in a deadlock (Segal, 2017). The reports of the UN GGE are also highlighted in recent European Council Conclusions concerning cyberdiplomacy (European Council, 2015, 2017). In the 2015 report, it was stated that "states should encourage the responsible reporting of ICT vulnerabilities" (UN GGE, 2015, p. 2) and the following norm was included on vulnerability disclosure (UN GGE, 2015, pp. 7 – 8):

Table 3
UN GGE Article 13

"13. Taking into account existing and emerging threats, risks and vulnerabilities. . . the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment: (j) **States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure."**

Note. Adapted from *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (pp. 7 - 8),* by the United Group of Governmental Experts, 2015, www.un.org [2017].

Secondly, the Organisation for Security and Cooperation (OSCE) works in the area of cybersecurity mainly on CBMs. CBMs are practical, risk-reduction measures created to increase transparency and decrease misperception and escalation between states (Trimintzios et al., 2017). The OSCE agreed on an initial set of eleven CBMs in December 2013 (OSCE, 2013) and a second set of an additional five CBMs on 10 March 2016 (OSCE, 2016). Most notable, CBM 16 was agreed upon (OSCE, 2016, p. 4):

Table 4
OSCE Confidence-Building Measure 16

"Participating States will, on a voluntary basis, encourage responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and share associated information on available remedies to such vulnerabilities, including with relevant segments of the ICT business and industry, with the goal of increasing co-operation and transparency within the OSCE region."

Note. Adapted from *Decision No. 1202 OSCE Confidence-Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies* (p. 4), by the Organization for Security and Cooperation, 2016, www.osce.org [2017].

The CBMs are the first step to normative development and create an environment where more ambitious norms can be built upon (Trimintzios et al., 2017). Both the norms agreed on in the UN GGE and the CBMs in the OSCE's are non-binding, voluntary, and act as a point of reference for expected behavior (Osula & Roigas, 2016). The EU and its MS have committed to implementing these norms and CBMs, which could be another motivation to make work of stimulating CVD.

5.4. CONCLUSION

CVD or ethical hacking has until today not been directly addressed by the EU in its strategy or regulations. Nevertheless, there are various links under which the EU could progress and stimulate CVD such as the NIS Directive and to a lesser extent the GDPR because it is a directly applicable and leaves less room for introducing clauses for CVD. Besides that, the agreements the EU and its MS reached in international fora such as the UN GGE and the OSCE on norms and CBMs include voluntary commitments to stimulate CVD. Until today, there has been little visible effect in the EU and its MS that these agreements changed something in the situation for ethical hackers in the EU. The previously described difficulties for ethical hackers to responsibly disclose vulnerabilities in the EU are thus not solved yet and thus there is still room and need for extra measures.

6. REGULATORY OPTIONS FOR THE EU TO STIMULATE CVD

This Chapter will answer the question whether stimulating CVD to increase the EU's cyber resilience is a task the industry can and will take up voluntarily or driven by concern for their reputation or financial consequences. Alternatively, the question will be answered whether additional, more coercive, regulation is needed as a safeguard.

Something to mention beforehand is that regulation of cybersecurity is not easy and straightforward (Carr, 2016; Morgan & Yeung, 2007). Therefore, this Chapter will also identify several open questions for further research. The analysis will follow the classification of means for regulation of Morgan and Yeung (2007). Note that no single instrument will provide the solution, but a right mix of instruments is required (Morgan & Yeung, 2007; Schellekens, 2016).

6.1. COMMAND

Command-and-control rules prohibit behavior underpinned with coercive sanctions for non-compliance (Morgan & Yeung, 2007). The focus will be on the NIS Directive and the GDPR because the CoC and AIS Directive are already implemented. There is thus very little room for maneuver left to change clauses to facilitate CVD better. It is not expected that there will soon be a new or a strongly adapted version of the CoC making an exemption for CVD because this will require a new agreement between 67 states. Besides that, harmonization of criminal law legislation concerning information systems is challenging. It is grounded in the belief that the EU is better suited to regulate such issues than MS individually (Summers, 2015). Even if an agreement is reached on what, and to what extent, cybercrime should be criminal, questions pop up about how much harmonization and whether harmonization is even an option (Summers, 2015).

6.1.1. REGULATORY OPTIONS UNDER NIS DIRECTIVE

The NIS Directive (Art. 15 (1); Art. 21) and the GDPR (e.g. Art. 84) both include coercive sanctions for non-compliance. Both regulations set the framework, wherein other measures can be taken to better facilitate CVD, without the harmonization of criminal law. Particularly the NIS Directive offers room to combine a coercive legal instrument with other instruments, which will be discussed in the following paragraphs.

Representatives of all 28 MS, the EC and ENISA are currently discussing the implementation of the NIS Directive in the newly established Cooperation Group and CSIRT Network.

This gives the EU and its MS a chance to introduce guidelines that stimulate the use of CVD under the denominator of Article 1 and 14 of the NIS Directive (EU, 2016b, pp. 11 - 20):

Table 5
NIS Directive Article 1

“1. This Directive lays down measures with a view to achieving a high common level of security of network and information systems within the Union so as to improve the functioning of the internal market.

2. To that end, this Directive:

> (d) **establishes security and notification requirements** for operators of essential services and for digital service providers”

Note. Adapted from *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union* (p. 11), by the European Parliament & the European Council, 2016, www.eur-lex.europa.eu [2017].

Table 6
NIS Directive Article 14

“1) Member States shall ensure that operators of essential services take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems which they use in their operations. Having regard to the state of the art, those measures shall ensure a level of security of network and information systems appropriate to the risk posed.”

Note. Adapted from *Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union* (p. 20), by the European Parliament & the European Council, 2016, www.eur-lex.europa.eu [2017].

Both articles of the NIS Directive include the need of taking appropriate security measures and are norms with an open character, which leaves room for the norm to be context depended - which is a key characteristic of EU Directives - and not prescribe a specific level of security. It is complicated to specify a concrete level of cybersecurity and receive the information to enforce it. Companies are in general reluctant to share data on (failed) hacking attempts (Schellekens, 2016). Besides that, these norms are relatively vague about the amount of protection which aligns with the idea that security of information systems is a rat race between hackers and those protecting systems (Schellekens, 2016).

The MS, the EC and ENISA could agree in the Cooperation Group on the content of the security requirements for essential operators. In the Implementing Decision laying down the procedures of the Cooperation Group (EC, 2017b), it is stated that the Cooperation Group is the committee for strategic cooperation between MS to share best practices relating to the implementation of the NIS Directive. Moreover, MS in collaboration with ENISA can assist MS in building capacity to guarantee the security of network and information systems.

The previously mentioned articles give MS the room to implement measures to stimulate CVD in the EU. It provides options for the EU and its MS to give substance to the international voluntary norms it agreed upon in the UN GGE and the OSCE. Under the command framework of the NIS Directive, implementing acts and guidelines could be used to harmonize the implementation of the NIS Directive and introduce the following measures:

MANDATORY IMPLEMENTATION OF A CVD POLICY FOR ESSENTIAL SERVICE PROVIDERS

MS or the EC could propose a norm in the Cooperation Group stating that all essential services providers are required (or recommended) to have a CVD policy in place, giving substance to the requirement of essential services providers to take appropriate security measures. This would be underpinned by the coercive sanctions for non-compliance of the NIS Directive. The international agreed standards on vulnerability disclosure from the International Standards Organization (ISO) could be advocated for this, which will be further discussed later.

MANDATORY IMPLEMENTATION OF A CVD POLICY FOR NATIONAL CSIRTS

Another option would be an agreement in the Cooperation Group, and perhaps the CSIRT Network, to make it mandatory (or recommended) for national CSIRTs to implement a CVD policy and take a coordinating role in their MS to support ethical hackers and vendors in CVD and mediate if necessary. This could be one of the measures to ensure that all national CSIRTs have the same security baseline in light of the requirements of the NIS Directive. If every national CSIRT would have a CVD policy, this would increase transparency, decrease vulnerabilities in information systems, reduce the chance of negative consequences of public disclosure, and make it clearer for ethical hackers which rules they need to follow when reporting vulnerabilities. Looking at Annex 1 of the NIS Directive specifying the tasks of national CSIRTs, CVD has not directly been named. Although, cooperation with the private sector and promotion of the adoption of standardized practices for incident and risk-handling procedures are mentioned. Moreover, the CSIRT Network has the power to issue guidelines to converge the services of national CSIRTs across Europe. Growing cooperation between CSIRTs and a mandatory clause for CVD could also increase the position of an ethical hacker in cross-border cases. This coordinating role of CSIRTs will be examined later.

6.1.2. REGULATORY OPTIONS UNDER GDPR

Vulnerabilities in information systems can unwittingly make vendors and their customers vulnerable to data breaches (Fimin, 2016). If companies can be fined for data breaches, this will provide a strong financial incentive for them to make sure as little as possible vulnerabilities are in their information systems. The GDPR could thus indirectly stimulate the implementation of CVD because if done responsibly, this can prevent a vulnerability being exploited or a data breach from taking place, and consequently saving the company a huge amount of money. The GDPR with its focus on consistency, transparency and accountability can become a game changer for CVD, which according to Fimin (2016), has until now has been based on a random mix of goodwill and expedience to keep systems secure.

6.1.3. OTHER INSTRUMENTS

INCLUDE CONCRETE ACTIVIES ON CVD IN THE NEW EU CYBERSTATEGY

There are also other options for the EU to comply with its agreement to international norms and CBMs to stimulate CVD. The new EU Cybersecurity Strategy, which is expected to be published in September 2017, could also be a place to underline the importance of CVD. A task could be included for the EC or ENISA to research further how CVD could be better facilitated in the EU or other mentioned, more concrete, instruments discussed in this Chapter could be included in the strategy. It should be noted that the introduced measures do not change the fact that it is illegal, but could make it more transparent for ethical hackers in what cases governments or companies would seek prosecution. CVD policy should therefore include a statement that in principle the government or company will not start prosecution when the conditions are met.

USE INSIGHTS FROM EU REGULATION ON REPORTING OF OCCURENCES IN CIVIL AVIATION

To stimulate CVD, the EU could also use insights from the EU Regulation on preventing negative consequences for reports of vulnerabilities in the aviation sector (EU, 2014b). One of the essential elements of this Regulation is that it provides stricter protection for reporters and aims to encourage reporting. There are clauses in the Regulation that prevent using the information against the reporter but no immunity is given to the reporter in case of gross negligence, willful violations and destructive acts. Besides that, in Table 7 it is stated that national authorities should find a balance between the proper administration of justice and the necessity of stimulating the reporting of safety risks.

Table 7

EU Regulation on reporting of occurrences in civil aviation:
Article 15: Confidentiality and appropriate use of information

"2) Without prejudice to the provisions relating to the protection of safety information in Articles 12, 14 and 15 of Regulation (EU) No 996/2010, information derived from occurrence reports shall be used only for the purpose for which it has been collected. Member States, the Agency and organisations shall not make available or use the information on occurrences:

(a) in order to attribute blame or liability; or

(b) for any purpose other than the maintenance or improvement of aviation safety.

4) Member States shall ensure that their competent authorities referred to in Article 6(3) and their competent authorities for the administration of justice cooperate with each other through advance administrative arrangements. These advance administrative arrangements shall seek to ensure the correct balance between the need for proper administration of justice, on the one hand, and the necessary continued availability of safety information, on the other."

Note. Adapted from *Regulation (EU) 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation* (p. 35), by the European Parliament & the European Council, 2014, www.eur-lex.europa.eu [2017].

The EU could use this EU Regulation as example to stimulate CVD. This can be combined with insights of the public prosecution guidelines on CVD published in the Netherlands, which will be discussed later. Such Regulation would, however, be depended on the political will of MS to progress CVD. As is the case with most measures introduced in this Chapter. There are, however, hopeful signs because an increasing number of MS are working on national frameworks to stimulate CVD. Besides that, large-scale cyber incidents because of vulnerabilities in information systems such as WannaCry and (Not)Petya will possibly open the debate on this subject again.

6.2. COMPETITION

Competition instruments aim to change behavior by making use of economic incentives and the competitive forces of the market. It is argued that these instruments can overcome many flaws of the traditional instruments of command (Morgan & Yeung, 2007). Nevertheless, the law often provides a vital facilitative role to create the framework for using competition-based instruments (Morgan & Yeung, 2007).

CHARGING EXPLOITATION OF VULNERABILITIES

Charges and taxes use a negative financial incentive not only to change behavior but also to increase government revenues and correct misallocations derivate of externalities (Morgan

& Yeung, 2007; Ogus, 1994). To effectively use this instrument there should be a clear connection between the activity and the harm caused which should be measurable (Morgan & Yeung, 2007). If applied to CVD, this would mean there should be a clear link between the responsibility of a company for an exploited vulnerability to a measurement of the consequences for its users. Most certainly, the industry will perceive charges for failed cybersecurity as unjust – because hackers are the cause – and it will feel like a punishment for something they have only limited control over (Schellekens, 2016). Moreover, charges for the lack of cybersecurity are believed to be counterproductive because it will only increase the cybersecurity costs and costs of doing business, which will probably not lead to better cybersecurity and fewer vulnerabilities (Morgan & Yeung, 2007). Hence, charges are not seen as particularly useful for stimulating CVD.

SUBSIDIES FOR CYBERSECURITY INNOVATION

A subsidy is a positive financial incentive to reward desired behavior decided on by the EU and its MS (Ogus, 1994). Subsidies to increase the cybersecurity of information systems will be welcomed with open arms by businesses because it can decrease the costs of cybersecurity. Nevertheless, it will be difficult to make a distinction between companies based on the security harms prevented (Schellekens, 2016). If a company shows good results, it could indicate that sufficient security measures have been implemented or it is a consequence of no interest of hackers to target the information systems of this company (Schellekens, 2016). Providing a direct EU subsidy for the implementation of CVD will thus not be a very realistic option.

There are, however, more indirect subsidies available stimulating innovative research under Horizon 2020 (EU, 2014b) for companies to perform innovative research on "the opportunities and risks of information security markets (e.g. bug bounties, vulnerability discovery & disclosure" (EC, 2017c) in the context of new business models and the economics of cybersecurity. This could possibly lead to innovative ways to stimulate CVD.

MAKE PRODUCT LIABILITY RULES APPLICABLE TO THE PRIVATE SECTOR

Governments can implement liability rules based on the idea that in the ideal situation users know exactly how much harm they risk from using a product and what the costs are of making the product safer (Breyer, 1982). The latter would enable them to bargain with producers with as result the production of goods with the right amount of safety included (Calabresi & Melamud, 1972). Users ordinarily do not have this information or are unable to understand it (Morgan & Yeung, 2007). Cybersecurity liability rules can be difficult to design because who is to blame: the hacker or the company with lacking protection?

The EU product liability rules stemming from 1985 are unfortunately not going to answer this question. In Article 1 it is stated thay: “the producer shall be liable for damage caused by a defect in his product” (European Council, 1985, p. 1). In Article 6 it is stipulated that: “a product is defective when it does not provide the safety which a person is entitled to expect” (European Council, 1985, p. 2). Safety does not have the same meaning as security, but they are closely related. A security vulnerability can evolve into a safety issue (Schellekens, 2016). The application of product liability concerning cybersecurity raises many questions, which go beyond the scope of this thesis.

Nevertheless, some important remarks can be made. EU product liability rules are largely outdated and do not cover the risks derivative of new technologies (European Council, 1985). Therefore, the EC published a roadmap for the evaluation of this Directive and to assess whether it is still ‘fit for purpose’ and decide whether the digital industry should fall under these rules (EC, 2016c). This is important because liability rules would entail an increase in the costs of vendors, which could provide a strong incentive for the vendor to patch vulnerabilities (Cavusoglu et al., 2005).

In the current situation, it is questionable whether the Directive applies to information systems and digital technologies (BEUC, 2017). Product liability rules could thus be another instrument which could indirectly encourage vendors to patch vulnerabilities and stimulate CVD policies, in any case until liability rules apply to information systems (Cavusoglu et al. 2005). However, the private sector has, in general, be reluctant to accept liability when referred to national security. Private companies assess cybersecurity from a cost-benefit perspective rather than from a public good perspective (Carr, 2016).

6.3. CONSENSUS

Consensus-based instruments cover a wide variety or regulatory instruments with the same denominator: they all influence behavior by the consent of its participants. The consensual base can be derivative of laws through which control is exerted or based on social consensus in a community. Law is mainly facilitating consensus-based instruments (Morgan & Yeung, 2007). All forms in this Chapter combine two consensus-based instruments: public-private partnerships (PPP) and self-regulation, which can both be a good step to build trust and give companies some control and influence. For the government, this could provide valuable first-hand information which can be used for new policies and regulations (Morgan & Yeung; Schellekens, 2016). There is, however, the risk of regulatory capture by industry. An excellent stimulus to counter this, would be a warning of the government that if they do not self-regulate, the government will (Schellekens, 2016).

6.3.1. STANDARDIZATION IN THE EU

According to the EC Communication on ICT Standardisation Priorities for the DSM: “ICT standardisation will continue to be primarily industry-led, voluntary and consensus-driven” (EC, 2016b, p. 4). One of the five priorities areas identified is cybersecurity. This Communication and the proposed actions give room for the EU to issue standards, developed in the PPP spirit, to facilitate CVD.

STIMULATING THE USE OF ISO STANDARDS FOR VULNERABILITY DISCLOSURE

Internationally, there are several widely used and recommended norms relating to CVD, most notably the ISO/IEC standards (2013, 2014) and the US National Institute of Standards and Technology (NIST) Cybersecurity Framework (NIST, 2014). These standards could be endorsed by the EU to give substance to its voluntary commitment in international fora to stimulate CVD, or can be transformed to the EU context. As discussed before, these standards can become mandatory or recommended as part of the implementing acts or guidelines decided on by the Cooperation Group aimed at harmonization of the security requirements for essential services providers or national CSIRTs. This would give MS and operators of essential services grip on how they could shape vulnerability handling and implement a CVD policy.

ISO and the International Electrotechnical Commission (IEC) make up the specialized system for worldwide standardization. All national standardization bodies are also members of ISO or IEC and contribute to a wide variety of standards through technical committees. These organizations are non-profit and open for technical expertise from governments and companies to support the development of standards (www.iso.org). Due to the Vienna Agreement between the ISO/IEC and the European Committee for Standardization (CEN), ISO/IEC standards can be transposed to CEN standards and the other way around to avoid duplication of standards in the world (www.cen.eu). There are two relevant ISO standards relating to CVD and handling endorsed by CEN as shown in Figure 2.

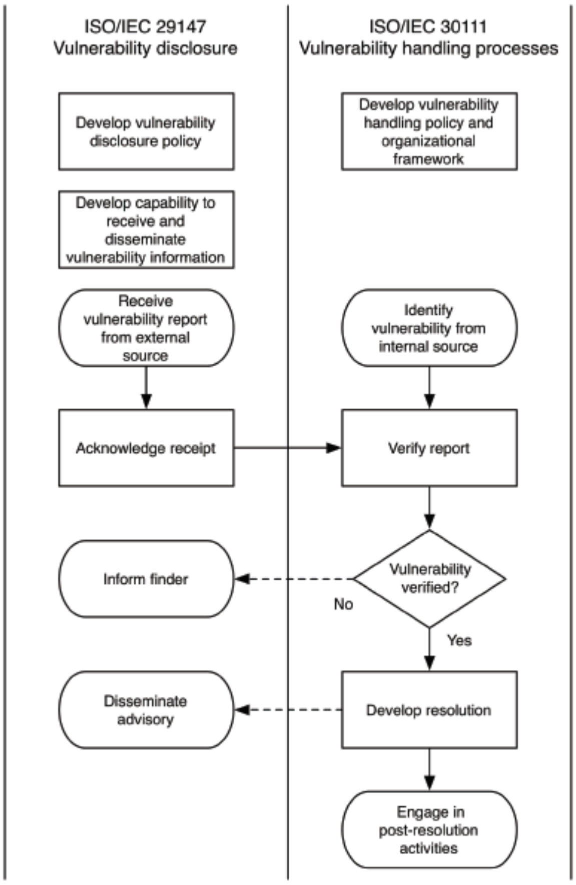

ISO/IEC 29147
Vulnerability disclosure
ISO/IEC 30111
Vulnerability handling processes
Develop vulnerability disclosure policy
Develop vulnerability handling policy and organizational framework
Develop capability to receive and disseminate vulnerability information
Receive vulnerability report from external source
Identify vulnerability from internal source
Acknowledge receipt
Verify report
Inform finder
Vulnerability verified?
No
Yes
Disseminate advisory
Develop resolution
Engage in post-resolution activities

Figure 2. Mapping of ISO/IEC 29147 and ISO/IEC 30111. Reprinted from *ISO/IEC 29147 Information Technology – Security Techniques – Vulnerability Disclosure*, by ISO/IEC, 2014, www.standards.iso.org [2017].

ISO 30111 (ISO, 2013) is about the investigation, triage and resolving of vulnerabilities, independently of whether the report comes from an external party or the own security testing teams. ISO 29147 is about implementing a CVD policy (ISO, 2014).

There is no need to reinvent the wheel. The EU could promote the existing industry guidelines. The above-mentioned ISO standards are useful guidelines on how to do handle vulnerabilities and implement a CVD policy (Fimin, 2016; NTIA, 2016). According to Fimin (2016), it is essential that key stakeholders know these documents, and simultaneously, governments and parts of the industry itself, need to put pressure on the industry to comply with these documents to improve CVD (Fimin, 2016). However, currently only ISO 29147 is freely available, while 30111 is being updated. It remains to be seen whether this standard would become freely accessible, which would be recommendable to stimulate CVD. The ISO standards are complex, so for the EU, it could also be advantageous to create a simplified overview of the ISO standards to make it clearer for governments and businesses what the critical points are for implementing a CVD policy (NTIA, 2016).

The update of the European ICT Security Certification Framework by September 2017 provides the EU with an opportunity to form or implement global standards which would help the EU to achieve cyber resilience (EPSC, 2017). If the EU would choose to recommend international agreed standards for national CSIRTs or operators of essential services, it should start with recommendation of ISO 30111 which is about organizing the internal process to handle and resolve vulnerabilities. The next step would be to stimulate the use of ISO 29147 which concerns how to implement a CVD policy and process external reports of ethical hackers but before this can be implemented the internal process needs to be in place.

USE THE NIST-FRAMEWORK TO STIMULATE VULNERABILITY DISCLOSURE

Another framework the EU should consider is the NIST-Framework, which has in 2014 been developed to reduce cyber risks to critical infrastructures in the US as a response to the Executive Order 13636 'Improving Critical Infrastructure Cybersecurity' (The White House, 2013). The NIST-Framework is a voluntary, risk-based cybersecurity standard that was created by consensus among thousands of stakeholders from government, the private sector and academia. Its main aim is to increase the cybersecurity and resilience of the US, but it has been developed considering the global interest for more standardization and is thus also applicable outside the US for public and private organizations (NIST, 2014; Wolff et al., 2016). The NIST-Framework is useful because it creates a common security baseline which can be tailored to the needs of various stakeholders; is drawn up by a multi-stakeholder effort; and is a living document which constantly evolves to keep up with the changing landscape. There is currently a draft update of the NIST-Framework under discussion which would incorporate CVD into the Framework (NIST, 2017). This would help organizations to evaluate their readiness to respond to reports of vulnerabilities and explain how to communicate with internal and external stakeholders (NIST, 2017). The NIST-Framework can offer some guidance for the EU's activities relating to CVD. Another positive point of using insights of the NIST-Framework would be that it would be applauded by industry. The industry would be in favor of international standards rather than EU standards because they want to avoid the costly compliance with hundreds of varying national requirements across the world (Wolff et al., 2016). International harmonization is thus key.

6.3.2. INDUSTRY SELF-REGULATION

SELF-REGULATION BY THE INDUSTRY: AGREEING ON NORMS

Companies themselves are also active in promoting CVD. Microsoft, for example, is for some time now calling for norms for CVD to mitigate risks of exploitation of vulnerabilities in information systems (Charney et al., 2016). In Table 8 and 9 the norms that Charney et al. (2016) introduced are displayed which could give some directions for norms the EU could adopt.

Table 8
Vulnerability disclosure norm for nations

"States should have a clear, principle-based policy for handling product and service vulnerabilities that reflects a strong mandate to report them to vendors, rather than to stockpile, buy, sell, or exploit them for nation states."

Note. Adapted from *From Articulation to Implementation: Enabling progress on cybersecurity norms* (p. 7), by S. Charney et al., 2016, Microsoft, www.microsoft.com [2017].

Table 9
Vulnerability disclosure norm for the global ICT industry

"Global ICT companies should adhere to coordinated disclosure practices for handling of ICT product and service vulnerabilities."

Note. Adapted from *From Articulation to Implementation: Enabling progress on cybersecurity norms* (p. 7), by S. Charney et al., 2016, Microsoft, www.microsoft.com [2017].

Microsoft calls upon the private sector to implement policies to facilitate CVD and increase transparency about how companies deal with this (Charney et al., 2016). They should motivate governments to do the same (Nicholas et al., 2014). If properly done, all players will in the end profit when security and resilience increase due to the handling of vulnerability reporting in a coordinated way (Nicholas et al., 2014).

SELF-REGULATION BY THE INDUSTRY: ETHICAL CODES

Self-regulation through ethical codes could also create an ecosystem wherein ethical hackers can responsibly disclose vulnerabilities to strengthen information systems. Ethical codes can help with clearly differentiating the activities of ethical hackers and black hats and could increase the trust of government and companies in ethical hackers. There is much literature about ethical codes for ethical hackers[19]. Although, there is no accepted European or international ethical code which is widely used (Kirwan & Power, 2012; Matwyshyn et al.,

[19] See ethics.acm.org for an industry best practice; Matwyshyn et al. (2010) for a historical overview of ethical codes; and Kirwan & Power (2012) for an overview of the current debate about ethical codes.

2010). Besides that, there are no empirical studies that analyzed whether ethical hackers subscribe to the ethics of such codes (Kirwan & Power, 2012).

According to Matwyshyn et al. (2010), the most essential and basic ethic is the duty not to harm (Matwyshyn et al., 2010). However, critics state that vulnerability research is in its core unethical because it includes testing systems of someone other than the ethical hacker (Schneier & Ranum, 2008). On the contrary, a strong argument can be made that at least a part of vulnerability research is ethical and, even ethically desirable. Provided that systems will not be disrupted, nothing will be damaged or in any other way harm third parties, it seems the duty not to harm is achieved (Matwyshyn et al., 2010). On top of that, the aim of CVD is not to harm someone but to prevent people from being harmed by an exploited vulnerability (Matwyshyn et al., 2010). As an example, the Hacker's Aegis suggest the following rules ethical hackers should comply with not to be prosecuted (Baumbauer & Day, 2010):

Table 10
Ethical code for ethical hackers

1) **Tell the vendor first** before publishing when discovering a vulnerability and postpone reporting to give the vendor the time to review the information, contact the ethical hacker, and create a patch if necessary;
2) **Do not sell** or offer the vulnerability information for sale to third parties;
3) **Test on your own system** if possible**,** if it is not reasonable possible, for example with cloud computing, it would be allowed to make use of others' systems lightly**;**
4) **Do not weaponize**. The discoverer should not publish, without the vendor's authorization, an exploit or proof of concept code that makes it possible to attack against the vulnerability. This would weaponize vulnerabilities and increase the amount of potential attacks.
5) **Create a trail** for the vulnerability by giving inter alia a detailed description of the vulnerability, how it can be exploited.

Note. Based on information from "Hacker's Aegis" (p. 34 – 40), D. E. Baumbauer & O. Day, 2010, *Emory Law Journal, 60, pp. 1-51.*

If ethical hackers follow these rules, their activities should be lawful, according to Baumbauer & Day (201). Not complying with these rules will remove the possibility for immunity and the vendor should use facts to show that the ethical hacker has broken one of these rules (Baumbauer & Day, 2010). Ethical hackers could register to such ethical codes of among others, associations or these codes could be used as input for the conditions for responsible behavior in CVD policies.

6.3.3. BEST PRACTICES

STIMULATE CSIRTS TO BECOME VULNERABILITY DISCLOSURE COORDINATING CENTERS

Many actors are not able to resolve cybersecurity threats alone. Simultaneously, there is a public interest to share information about vulnerabilities. New exploits and vulnerabilities found by ethical hackers or companies need to be shared with other relevant stakeholders as quickly as possible (ENISA, 2015; Schellekens, 2016). The problem with information sharing is that for most companies this information is commercially sensitive: it entails information on attempted or succeeded hacks or exploits. Organizations will only share this information if there is a stable base of trust among stakeholders and clear conditions for sharing are in place (Schellekens, 2016). Furthermore, knowledge of vulnerabilities and way to solve them need to be communicated quickly and adequately among the relevant stakeholders (ENISA, 2015). Therefore, a coordinating authority for CVD would be recommendable because it can (ENISA, 2015; Schellekens, 2016):

- Distribute vulnerability information and solutions across borders and sectors preventing harm and unnecessary exposure to risks;
- Mediate between vendors and ethical hackers in case of misunderstandings or problems in the communication preventing uncontrolled publication of vulnerabilities (see Figure 3);
- Overcome the significant difference in power between big vendors and a single ethical hacker to ensure the prospects of a timely reaction of a vendor;
- Limit the legal exposure of the ethical hacker.

A well-placed organization to take up this neutral third party coordinating role is a national CSIRT (Schellekens, 2016). The EU could learn from CSIRTs with much experience with CVD already, notably CERT-CC in the US, JP-CERT in Japan, CERT-FI in Finland and the NCSC in the Netherlands (ENISA, 2015). ENISA, the EU, and its MS could stimulate the use of CVD policies and national CSIRTs to take up roles in a coordinating role in the CVD process.

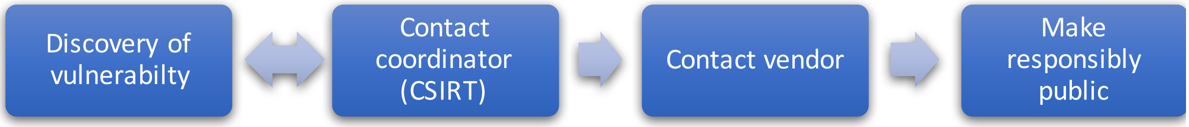


Figure 3. Responsible disclosure / coordinated vulnerability disclosure process including mediation by coordinator.

It could furthermore be recommended to look at the multi-stakeholder process of the NTIA and the Forum of Incident Response and Security Teams (FIRST) which discuss and issue CVD policies, handling practices and best practices (NTIA, 2016; FIRST, 2016). In both initiatives, EU MS were also involved, and these best practices can provide input for EU action to stimulate CVD.

6.4. COMMUNICATION

Communication instruments try to effect behavior by enriching the information available to those whose behavior should change (e.g. governments, vendors, ethical hackers). Communication can be built upon law or be of a non-coercive nature (Morgan & Yeung, 2007).

CREATING BUG BOUNTY PLATFORMS AND PROGRAMS

Communication is of vital importance to better inform users. Next to mandatory reporting, the private sector can also communicate voluntarily about cybersecurity to underline the quality and security of their products (Morgan & Yeung, 2007). A legal option can be through so-called bug bounty platforms where a cash reward is offered by a vendor in exchange for vulnerability information (Maurushat, 2014; McGraw, 2017; Sutton & Nagle, 2006). Especially zero-days[20] are very profitable.

Most vendors or governments do not compensate ethical hackers with money if they find vulnerabilities in their products. In the case of CVD, the rewards are often smaller such as acknowledgment in a hall of fame, 'hacker's t-shirts', or vouchers. The underlying idea of a bug bounty program is not to display that hackers cannot enter the system. It is grounded in the belief that the most secure systems are those that have been exposed to much testing (Schellekens, 2016). In general, bug bounty programs make vulnerability disclosure more transparent and structured. It also gives both parties a reward instead of one, which is a positive incentive for more effective cooperation. There is, however, still some reluctance in accepting bug bounty platforms and giving financial rewards for vulnerabilities. Particularly from a government perspective because they are afraid of possible blackmail, do not support the idea of competition for vulnerability information or have the altruistic believe that this information should be free (ENISA, 2015; Sutton & Nagle, 2006).

[20] "A zero-day vulnerability is a vulnerability for which no patch is available yet because the developer of the vulnerable software has not yet had time to make a patch" (NCSC, 2016).

Furthermore, some governments are in the business of buying vulnerabilities, mainly intelligence agencies, for defensive and offensive actions to protect the national security (Ellis, 2015). This is a worrisome development from the perspective of a resilient EU in cyberspace because vulnerability information is kept secret by various parties, which leaves vulnerabilities unsolved and other actors vulnerable (ENISA, 2015; Sutton & Nagle, 2006). This debate is however to extensive and outside the scope of this thesis.

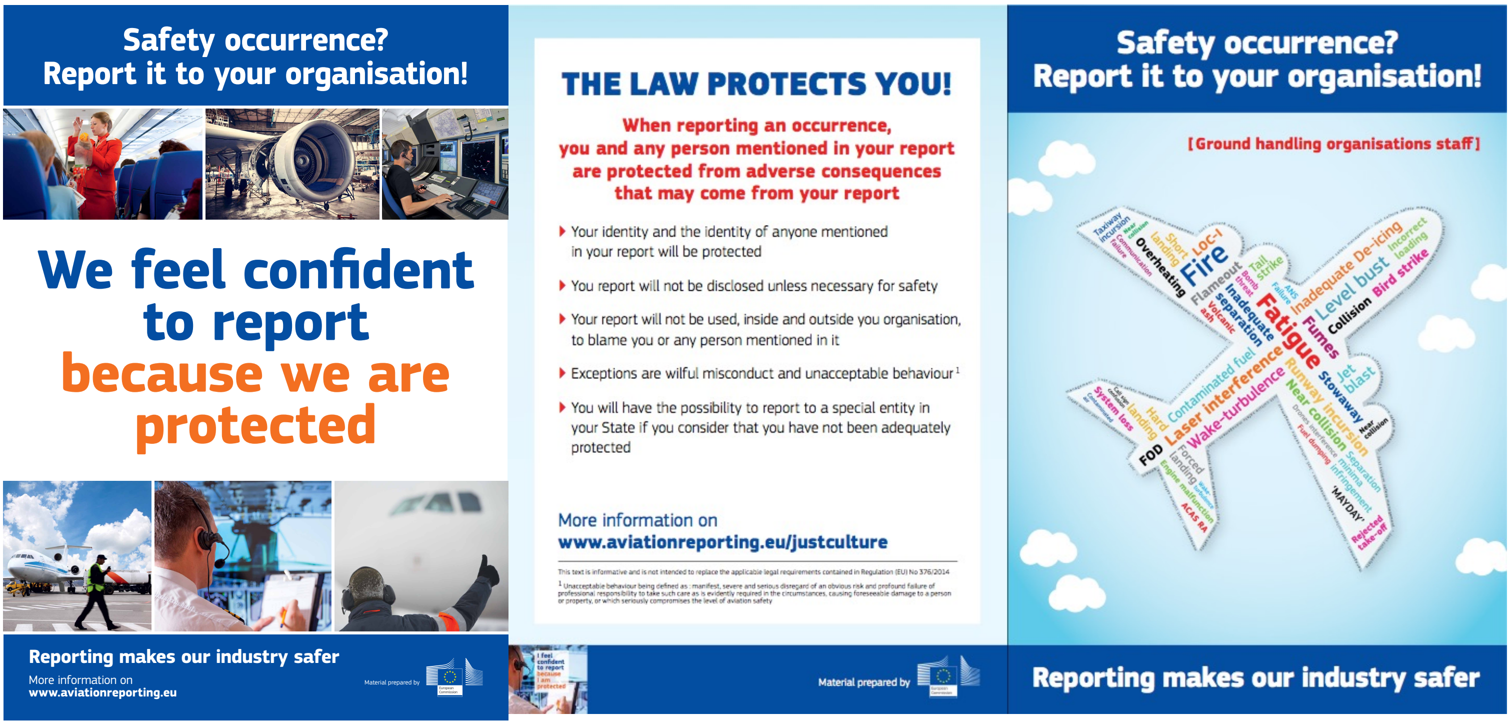
The EU and it MS should nevertheless closely follow the results of the EP program approved in December 2016 on open software which introduces a bug bounty program to stimulate the search for vulnerabilities in free software of the EU institutions to prevent compromise of EU institutions systems (Schaake, 2016). It could also be interesting to keep a close eye on a bug bounty pilot program in the US, which is agreed on with the 'Hack DHS Act' to increase cybersecurity of the systems of the Department of Homeland Security (DHS). According to the Act, the DHS Secretary needs to cooperate with the Attorney General to guarantee that these ethical hackers do not face prosecutions for activities falling within the scope of the program (Hassan, 2017). Besides that, there are also lessons the EU can learn from the concluded initiative 'Hack the Pentagon', wherein ethical hackers were invited to find vulnerabilities in systems of the Pentagon (Collins, 2016).

USE EXPERIENCES FROM THE JUST CULTURE INITIATIVE AND THE CVD MANIFESTO

On 1 October 2015, the PPP-initiative 'Just Culture' was signed by the European air industry, in cooperation with the EU, to make the aviation sector safer. The signatories commit to creating an environment of trust where staff has the confidence to report safety vulnerabilities, even when they have made honest mistakes (www.aviationreporting.eu). This Just Culture Declaration is comparable with the 'Coordinated Vulnerability Disclosure Manifesto' which was launched during the Netherlands' Presidency of the EU by 29 private organizations in cooperation with the NCSC (CIO Platform, 2016a, 2016b). Signatories of these documents, acknowledge the importance of responsible reporting of safety or security vulnerabilities. In case of the latter, these organizations publicly announced their support for CVD. Both are good examples of combining consensus- and competition-based instruments to stimulate a change of behavior. Moreover, both declarations are non-legally binding and do not intend to overrule judicial rules of MS (www.aviationreporting.eu; CIO Platform, 2016).

START A PUBLIC CAMPAIGN TO STIMULATE CVD

The EU could use the same elements as used in the public campaign to promote a Just Culture in the aviation sector to stimulate CVD (see Figure 4). It is a way of educating both vendors as well as ethical hackers about the criteria they should follow when finding a vulnerability, expressing the boundaries of responsible disclosing vulnerabilities and good conduct.



THE LAW PROTECTS YOU!

When reporting an occurrence, you and any person mentioned in your report are protected from adverse consequences that may come from your report

- Your identity and the identity of anyone mentioned in your report will be protected
- You report will not be disclosed unless necessary for safety
- Your report will not be used, inside and outside you organisation, to blame you or any person mentioned in it
- Exceptions are wilful misconduct and unacceptable behaviour[1]
- You will have the possibility to report to a special entity in your State if you consider that you have not been adequately protected

More information on
www.aviationreporting.eu/justculture

This text is informative and is not intended to replace the applicable legal requirements contained in Regulation (EU) No 376/2014

[1] Unacceptable behaviour being defined as : manifest, severe and serious disregard of an obvious risk and profound failure of professional responsibility to take such care as is evidently required in the circumstances, causing foreseeable damage to a person or property, or which seriously compromises the level of aviation safety

Figure 4. Overview of documents used for the public campaign promoting reporting occurrences in the aviation sector. Reprinted from *www.aviationreporting.eu* [2017].

STIMULATE THE USE OF CVD POLICIES

Another example of using communication as an instrument is the guideline to boost responsible disclosure published by the NCSC in January 2013 drafted up in cooperation with the private sector and academics (NCSC, 2013). It gives organizations several building blocks to construct their CVD policy. Such policy, can by way of communication give the discoverer "sufficient reassurance with regards to legal issues, such as protection from legal actions if the reporting by the discoverer is compliant with the CVD policy" (van der Meulen, 2016, p. 8).

PUBLISH PROSECUTION GUIDELINES AND CREATING AN OVERVIEW OF JURISPRUDENCE

As a reaction to these guidelines, the Dutch Public Prosecutor (DPP) sent a letter to all its departments communicating how a CVD policy should play a role to decide if to proceed with a prosecution of hacking on a case by case base (Openbaar Ministerie, 2013, p. 3).

Table 11

Letter Dutch Public Prosecutor on Responsible Disclosure

> "In short: when assessing the question whether or not criminal acts were committed, the Public Prosecutor will have to take the following circumstances into account:
>
> - Was the conduct of the suspect necessary within the context of a democratic society (i.e. was there an important general interest)?
> - Was the conduct of the suspect proportionate (were his means proportionate in relation to the goal he wanted to achieve)? In other words: how did the hacker get access to the ICT system? If for this purpose he acted disproportionately, e.g. as described in the Guidelines on page 8 under 4.2., one cannot speak of an 'ethical' hack.
> - Did the suspect act alternatively (were there other ways to act)? In other words: was the hack immediately reported to the owner of the ICT system or did the hacker not do so in order to be able to delete traces, to manipulate, copy or delete data? If traces were deleted and data were manipulated, copied or deleted, it was not an ethical hack.
>
> If the answer to the above questions is positive, the Public Prosecutor may refrain from conducting a criminal investigation or from initiating criminal proceedings."

Note. Adapted from *Responsible Disclosure (how to act in cases of 'ethical' hackers?)* (p. 3), by Openbaar Ministerie, 2013, www.om.nl [2017].

In short: if someone finds a vulnerability in the Netherlands and this right away reports to the owner of the information system, this would most likely be seen as ethical hacking. But if this person did go further than this (copy, manipulate or delete data), a criminal investigation can be opened. The guideline of the NCSC does not provide ethical hackers with legal certainty because hacking can always be investigated and prosecuted under the Dutch Penal Code. Nevertheless, the letter of the DPP does show that they have seriously thought about this issue and provides ethical hackers with some directions about how they should responsibly disclose vulnerabilities without risking prosecution.

The annual Cyber Security Assessments of the NCSC show that an increasing number of Dutch companies have implemented CVD policies and the number of reports of ethical hackers is also growing (NCSC, 2015b, 2016). These are hopeful signs that the Dutch approach has given ethical hackers a certain degree of confidence. Until now, the DPP has prosecuted two cases that provide more direction about the boundaries that apply to CVD and ethical hacking[21] (van 't Hof, 2015). According to van der Meulen (2015), this can be seen as a growing trust between the governments, vendors and ethical hackers.

[21] Rechtbank Den Haag (2014) & Rechtbank Oost-Brabant (2013). In both cases, they did not responsibly disclose a vulnerability, although they tried to argue that it was about CVD.

As mentioned before, creating legal certainty in the EU landscape with a wide variety of laws is difficult to accomplish soon. Hence, ENISA already recommended in 2013 after the adoption of the AIS Directive that it would be recommended for MS to publish guidance on "the interpretation and application of the unlawful access provisions, and particularly on the element of intent (i.e. the unlawfulness – without right) in cases where no security measures were breached, if this is permitted under national law" (Muynck, Graux & Robinson, 2013). ENISA reiterated the need for large-scale implementation of CVD in a report of 2015 on CVD. Options would be to create prosecution guidelines that permit CVD under certain conditions or issue overviews of jurisprudence to demonstrate how courts apply the law in practice (Muynck et al., 2013). The collection and distribution of such good practices at the EU level can also support the homogenous application of the law regarding hacking across the EU (Muynck et al., 2013). All these measures will make the process and possible legal consequences more predictable for ethical hackers. As a result, the trust between all actors will increase and, therefore, positively affect CVD and the cyber resilience of the EU (ENISA, 2015; van der Meulen, 2016).

6.5. CONCLUSION

The question whether the EU could leave stimulating CVD to the industry itself is difficult to answer. A combination of instruments that stimulate both governments as the private sector would be recommended.

Command measures are suitable to set the framework, particularly the NIS Directive and the GDPR provide links to take measures to stimulate CVD underpinned by a coercive sanction for non-compliance. Other instruments should be used to build upon the framework's clauses to take appropriate security measures and give substance to the duty of care for essential service providers. Specifically, because close cooperation between public and private organizations is advocated to effectively regulate cybersecurity and stimulate CVD. Competition-based measures such as subsidies and product liabilities could be used to stimulate CVD. Although subsidies can only be used indirectly to stimulate research about how CVD could be better facilitated in the EU. It is not clear what the effects of product liability rules would be on CVD. Moreover, the industry is in general reluctant to accept liability measures from the perspective of national security. Charges and sanctions are not seen as desirable and useful to stimulate CVD.

Furthermore, consensus and communication-based instruments are considered the most suitable instruments to build upon frameworks provided by command instruments. Consensus-based instruments are valuable to unite the public and private interests. The EU could make use of international standards and industry best practices to shape its own guidelines or norms to stimulate CVD, to give substance to the duty of care of the NIS Directive or a new EU Cyberstrategy. Lastly, most introduced instruments are hybrids and to some extent use the power of communication to change behavior. The EU could use insights of the Just Culture initiative in the aviation sector, experiences with bug bounty programs and Dutch best practices such as the guideline on how to implement a CVD policy for companies and the DPP's letter explaining which circumstances the DPP will consider when assessing whether an ethical hacker has committed a crime.

7. CONCLUSIONS & DISCUSSION

This thesis examined how the EU could use regulatory instruments to increase its cyber resilience through stimulating coordinated vulnerability disclosure.

First of all, when hackers or other malicious actors check out the security of information systems, they are looking for any chink in one's armor to infiltrate the system. Security experts say everything can be hacked; it is just a matter of time and resources. For that reason, vulnerabilities have always been the digital Achilles heel of information systems. Not only in the EU, but all over the world, as underlined by ransomware campaigns exploiting vulnerabilities such as WannaCry and (Not)Petya.

Identifying and solving vulnerabilities is therefore critical. A vital measure to do so is stimulating CVD. Currently, ethical hackers risk being sued because searching for vulnerabilities without consent of the system's owners is illegal in all MS. Consequently, ethical hackers can be persuaded to sell vulnerabilities on the black market, exploit the vulnerability themselves or make it public for others to exploit. It is of importance for the EU to come up with measures to stimulate CVD, so ethical hackers, vendors and governments will work together to make information systems more secure, protect the users and prevent negative consequences of vulnerabilities.

The analysis demonstrates that some form of regulation is needed as current legislation does not address this security issue at all. Policymakers in the EU should embrace the services of ethical hackers because of its significant benefits. There is a need to proper facilitate CVD, instead of inappropriately obstruct it.

In the EU, stimulating CVD is also depended on political will. The momentum to address this issue is present. Many MS are currently working on creating national frameworks to stimulate CVD, while at the same time large-scale cyber incidents have become less hypothetical and more tangible due to WannaCry and (Not)Petya. Subsequent statements of the EC and MS point to a realization that vulnerabilities in information systems must be addressed on the EU level. Meanwhile, discussions concerning cybersecurity are ongoing because a new EU Cyberstrategy will be issued in September 2017 and the Cooperation Group and the CSIRT Network are still discussing the implementation of the NIS Directive.

When looking at the EU's aim to become cyber resilient, it is essential that the EU has the capability to absorb and recover from cyber incidents quickly. Due to the rapid technologic developments, ever-changing threat landscape, the rat-race in cyberspace and the lack of borders, it is important that the EU has flexible mechanisms in place to ensure the security of the EU. To achieve this, the EU should increasingly create flexible and adaptive structures based on self-organization, multi-stakeholderism and public-private cooperation. Regulations should not be developed top-down but rather bottom-up. By doing so, the EU will best be able to counter cyber threats, and will not only deal with the symptoms but also address the root causes.

Consequently, command rules are suitable to set the framework for action but are not sufficiently flexible to quickly adapt to changing circumstances and do not make enough use of the power of partnerships. The NIS and GDPR do in contrast create a framework underpinned by sanctions for non-compliance. Consensus and communication-based measures should be introduced using the expertise of the private sector to extend this legal framework. Until now, it seems the industry has stimulated CVD in dribs and drabs. Therefore, a somewhat stronger direction provided by the EU should be promoted. There is momentum to incorporate stimulating measures for CVD into the implementation of the NIS Directive. For this the EU could use guidelines advocating for (or obligating) national CSIRTs or essential service providers to implement a CVD policy, or in the case of national CSIRTs to also take up a coordinating role in the process. The EU should not come up with everything on its own, but make use of the insights and best practices from international multi-stakeholder processes, industry, MS and other governments.

The EU could prescribe, or use insights from, the internationally agreed ISO-standards, of which the first step would be to recommend ISO 30111 to internally organize vulnerability reporting, followed by ISO 29147 which introduces the external component. Moreover, the EU should seriously consider in what way and to what extent they could use the NIST-Framework. This would be welcomed by the industry and would ensure a favorable business climate for global companies in the EU, as it would prevent companies from having to comply with a wide variety of standards and national requirements in different parts of the world. Moreover, global standards are better suited than ‘regional’ EU standards to address cybersecurity issues because of its borderless nature.

Furthermore, communication instruments are essential to stimulate CVD, particularly to provide all parties involved with more clarity about when behavior is responsible. Therefore, widespread implementation of CVD policies should be supported to come to a common agreement that vulnerability details will not be published before they are solved and when following the rules in the policy legal action will not be taken. For making the legal consequences of ethical hacking clearer, the EU should look at best practices from the Netherlands – the CVD policy guideline and the DPPs letter explaining which criteria it will use in cases of hacking. Moreover, using insights of the Just Culture initiative and the harmonization of regulation in the aviation sector for reporters would be beneficial because it is also about stimulating responsible reporting of security issues.

The EU could use a combination of these measures to stimulate CVD and increase the legal certainty of ethical hackers to strengthen the resilience of the EU's cyber ecosystem. By working together with all actors involved, the EU could develop a culture of cybersecurity at all levels and layers (technical, legal, policy) and among all stakeholders (e.g. governments, vendors, ethical hackers) by using instruments to raise awareness and transparency to ensure learning and clarity for all parties involved. From a cyber resilience perspective, these measures are excellent examples of working in partnerships, making use of the expertise of the private sector and converge amongst stakeholders on a common understanding of norms, laws and standards of security as resilience in the EU.

Unfortunately, this thesis could not extensively elaborate on other important debates that are also relevant if the EU wants to increase its cyber resilience and decrease vulnerabilities in information systems. Important debates wherein technical and non-technical experts should exchange opinions about the desirability of keeping vulnerabilities secret for defensive and offensive purposes by governments and intelligence services; how to develop incentives for companies to make products that are secure by design; and how certification schemes can help with increasing the trust in information systems and ethical hackers.

This thesis has contributed to the limited amount of literature on this subject and has tried to bridge the gap between the technical and non-technical (e.g. policy, legal) worlds by using academic literature and primary documents from both sides. For developing effective and efficient EU policies on cybersecurity this is essential. The highly technical nature of cybersecurity issues and the fast technological developments are reasons why policymakers in the EU need the insights from the technical experts who are at the forefront of increasing cybersecurity to create effective policies. The other way around, the industry and information system experts should critical and engage with policymakers about new policies and regulations. Technical and non-technical experts of public and private parties in the EU should thus bundle their forces to create a secure cyber ecosystem for all.

BIBLIOGRAPHY

ACADEMIC LITERATURE

Algarni, A. M. (2016). *Quantitative economics of security: software vulnerabilities and data breaches.* Colorado, CU: Colorado State University.

Algozzine, B., & Hancock, D. R. (2006). *Doing case study research: A practical guide for beginning researchers*. New York, NY: Teachers College Press.

Arnull, A., & Chalmers, D. (Eds.). (2015). *The Oxford Handbook of European Union Law*. OUP Oxford.

Arora, A., & Telang, R. (2005). Economics of software vulnerability disclosure. *IEEE Security & Privacy*, 3(1), 20-25.

Arora, A., Telang, R., & Xu, H. (2008). Optimal policy for software vulnerability disclosure. *Management Science*, 54(4), 642-656.

Baumbauer, D. E., & Day, O. (2010). The Hacker's aegis. *Emory Legal Journal*, 60, 1051.

Begum, S., & Kumar, S. (2016). A Comprehensive Study on Ethical Hacking*. International Journal of Engineering Sciences & Research Technolog*y, 1(5), 214-219.

Bendrath, R., Eriksson, J., & Giacomello, G. (2007). From 'cyberterrorism' to 'cyberwar', back and forth. *International Relations and Security in the Digital Age*, 57-82.

Bergman, K. M. (2015). Target to the Heart of the First Amendment: Government Endorsement of Responsible Disclosure as Unconstitutional. *Northwestern Journal of Technology and Intellectual Property*, 13.

Berinato, S. (2007). Software Vulnerability Disclosure: The Chilling Effect. *CSO Security and Risk.*

Betz, D., & Stevens, T. (2011*). Cyberspace and the State: Toward a Strategy for Cyber-power*. London, UK: The International Institute for Strategic Studies.

Biancuzzi, F. (2008). The Laws of Full Disclosure. *Security Focus*.

Böhme, R. (2006). *A comparison of market approaches to software vulnerability disclosure.* Retrieved on 25 April 2017, from https://www.is.uni-muenster.de/security/publications/Boehme2006_CompVulnMarkets_ETRICS.pdf

Bossong, R., & Wagner, B. (2016). A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change*, 1-24.

Breyer, S. (1982). *Regulation and its Reform*. Cambridge, MA: Harvard University Press.

Brownsword, R. (2005). Code, control, and choice: why East is East and West is West. *Legal Studies*, 25(1), 1-21.

Calabresi, G., & Melamed, A. D. (1972). Property rules, liability rules, and inalienability: one view of the cathedral. *Harvard law review*, 1089-1128.

Carr, M. (2016). Public–private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43-62.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor? *Journal of Common Market Studies*, 1-19.

Cavoukian, A., & Chanliau, M. (2013). *Privacy and security by design: a convergence of paradigms.* Ontario, Canada: Office of the Privacy Commissioner.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2005). *Emerging Issues in Responsible Vulnerability Disclosure*. Retrieved on 25 April 2017, from http://infosecon.net/workshop/pdf/cavusoglu.pdf

Cencini, A., Yu, K., & Chan, T. (2005). *Software Vulnerabilities: Full-, Responsible-, and Non-Disclosure*. Washington, WA: Washington University.

Christou, G. (2014). *The EU's Approach to Cyber Security,'EU-China Security Cooperation: Performance and Prospects Project*. Jean Monnet Multilateral Research Group. Retrieved on 22 May 2017, from http://eusc.essex.ac.uk/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf

Christou, G. (2016). *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. New York, NY: Palgrave Macmillan.

Clough, J. (2014). A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation. *Monash University Law Review*, *40*, 698.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, 4(10).

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative* (pp. 146-166). Upper Saddle River, NJ: Prentice Hall.

Daintith, T. (1997). Regulation. In R. Buxbaum & F. Madl (Eds.), *International Encyclopedia of Comparative Law*. New York, NY: Oceana.

Denney, A. S., & Tewksbury, R. (2013). How to write a literature review. *Journal of Criminal Justice Education*, 24(2), 218-234.

Dudley, A., Braman, J., & Vincenti, G. (Ed.). (2011). *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: Issues, Impacts and Practices*. IGI Global.

Dunn Cavelty, M. (2007). Cyber-Terror-Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology and Politics*, 4(1), 19-35.

Dunn Cavelty, M. (2008), *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. London, UK: Routledge.

Dunn Cavelty, M. (2013). A resilient Europe for an open, safe and secure cyberspace. *UI Occassional Papers*, 23.

Dunn Cavelty, M. (2014). Breaking the cyber-security dilemma: Aligning security needs and removing vulnerabilities. *Science and Engineering Ethics*, 20(3), 701-715.

Ellis, R. (2015). T*he Vulnerability Economy: Zero-days, cybersecurity, and public policy*. Cambridge, MA: Harvard Kennedy School.

Engebretson, P. (2013). The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. *Elsevier.*

Eriksson, J. (2001). Cyberplagues, IT, and security: Threat politics in the information age. *Journal of Contingencies and Crisis Management*, 9(4), 200-210.

European Institute for Security Studies (EUISS) (eds.) (2017). *After the EU Global Strategy: Building resilience*. Paris, France: European Union Institute for Security Studies.

Falot, N. & Schermer, B.W. (2016). De strafrechtelijke positie van de Nederlandse ethisch hacker. *Computerrecht*, 45, 1-13.

Graves, K. (2010). *CEH certified ethical hacker study guide*. New York, NY: John Wiley & Sons.

Handmer, J. W., & Dovers, S. R. (1996). A typology of resilience: rethinking institutions for sustainable development. *Organization & Environment*, 9(4), 482-511.

Harper, A., Harris, S., Ness, J., Eagle, C., Lenkey, G., & Williams, T. (2011). *Gray Hat Hacking: The Ethical Hackers Handbook.* New York, NY: McGraw-Hill Osborne Media.

Havana, T. (2004). *Communication in the software vulnerability reporting process*. Oulo, Finland: University of Oulo.

Kavalski, E. (2009). Timescapes of security: Clocks, clouds, and the complexity of security governance. *World Futures*, 65(7), 527-551.

Kirchner, E. J., & Sperling, J. (Eds.). (2007). *Global security governance: Competing perceptions of security in the twenty-first century*. London, UK: Routledge.

Kirsch, C. (2014). Grey Hat Hacker: Reconciling Cyberspace Reality and the Law. *The Northern Kentucky University Law Review*, 41, 383.

Kirwan, G. & Power, A. (2012). Hacking: Legal and Ethical Aspects of an Ambiguous Activity. In A. Dudley, J. Braman & G. Vincenti (Ed.), *Investigating Cyber Law and Cyber Ethics: Issues, Impacts and Practices: Issues, Impacts and Practices*. IGI Global.

Klimburg, A. (2011). Mobilising cyber power*. Survival*, 53(1), 41-60.

Klimburg, A., & Tiirmaa-Klaar, H. (2011). *Cybersecurity and cyberpower: Concepts, conditions and capabilities for cooperation for action within the EU*. Retrieved on 30 March 2017, from http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf

Kronsell, A. & Manners, I. (2015). Single policy study: Three variations in design. In K. Lynggaard, I. Manners & K. Löfgren (Eds.), *Research methods in European Union studies*. New York, NY: Springer.

Lessig, L. (1999). *Code and other Laws of Cyberspace*. New York, NY: Basic Books.

Lessig, L. (2006). *Code: Version 2.0*. New York, NY: Basic Books.

Mason, S. (2012). *Electronic Evidence*. London, UK: LexisNexis Butterworths.

Matwyshyn, A. M., Cui, A., Keromytis, A. D., & Stolfo, S. J. (2010). Ethics in security vulnerability research. *IEEE Security & Privacy*, 8(2), 67-72.

Maurushat, A. (2014). *Disclosure of Security Vulnerabilities: Legal and Ethical Issues*. Springer Science & Business Media.

McGraw, G. (2015). Silver Bullet Talks with Katie Moussouris. *IEEE Security & Privacy*, *13*(4), 7-9.

Miller, G. J., & Yang, K. (Eds.). (2007). *Handbook of research methods in public administration*. CRC press.

Morgan, B., & Yeung, K. (2007). *An introduction to law and regulation: Text and materials*. Cambridge, MA: Cambridge University Press.

Moumoutzis, K. (2011). Still fashionable yet useless? Addressing problems with research on the Europeanization of foreign policy. *Journal of Common Market Studies*, 49(3), 607-629.

Nye Jr, J. S. (2010). *Cyber Power*. Harvard Kennedy School Belfer Center for Science and International Affairs.

Ogus, A. I. (1994). Standard Setting for Environmental Protection: Principles and Processes. *Environmental Standards in the European Union*, 25-37.

Ogus, A. (1995). Rethinking self-regulation. *Oxford Journal of Legal Studies*, 15(1), 97-108.

Osula, A.M, & Rõigas, H. (2016). *International Cyber Norms - Legal, Policy & Industry Perspectives*. Tallinn, Estonia: NATO CCD COE.

Parker, T., Sachs, M., Shaw, E., & Stroz, E. (2004). *Cyber adversary characterization: Auditing the hacker mind*. Rockland, MA: Syngress.

Pawlak, P. (2016). *Resilience in the EU's foreign and security policy*. Retrieved on 20 March 2017, from http://www.europarl.europa.eu/thinktank/nl/document.html?reference=EPRS_BRI(2016)583828

Pawlak, P. (2017). Horiziontal Issues. In European Institute for Security Studies (eds.), *After the EU Global Strategy: Building resilience*. Paris, France: European Union Institute for Security Studies.

Pfleeger, C. P., & Pfleeger, S. L. (2006). *Security in computing*. New Jersey, NJ: Prentice Hall Professional Technical Reference.

Preston, E., & Lofton, J. (2002). Computer security publications: Information economics, shifting liability and the first amendment. *Whittier Law Review*, 24, 71.

Ranum, M. J. (2008). *The Vulnerability Disclosure Game: Are We More Secure*? Retrieved on 15 June 2017, from http://www.csoonline.com/article/2122977/application-security/the-vulnerability-disclosure-game--are-we-more-secure-.html

Ryan, D. J., & Heckman, C. (2003). Two views on security software liability. Let the legal system decide. *IEEE Security & Privacy*, 99(1), 70-72.

Samuel, A. W. (2004). *Hacktivism and the future of political participation*. Cambridge, MA: Harvard University Cambridge.

Schwartz, A., & Knake, R. (2016). *Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process*. Cyber Security Project, Belfer Center for Science and International Affairs, Harvard Kennedy School.

Schellekens, M. (2016). Car hacking: navigating the regulatory landscape. *Computer Law & Security Review*, 32(2), 307-315.

Schiller, J. (2002). Responsible vulnerability disclosure: a hard problem. *Secure Business Quarterly*, *2*(1-5).

Schneier, B. (2000). *Full disclosure and the window of exposure*. Retrieved on 15 April 2017, from https://www.schneier.com/crypto-gram/archives/2000/0915.html.

Schneier, B., & Ranum, M. (2008). Face-off: Is security market consolidation a plague or progress. *Information Security*.

Schuster, S., van den Berg, M., Larrucea, X., Slewe, T., & Ide-Kostic, P. (2017). Mass surveillance and technological policy options: Improving security of private communications. *Computer Standards & Interfaces*, 50, 76-82.

Sliwinski, K. F. (2014). Moving beyond the European Union's weakness as a cyber-security agent. *Contemporary Security Policy*, 35(3), 468-486.

Stone, A. (2003). Software flaws, to tell or not to tell?. *IEEE Software*, *20*(1), 70-73.

Summers, S. (2015). EU Criminal Law and the Regulation of Information and Communication Technology. *Bergen Journal of Criminal Law & Criminal Justice*, *3*(1), 48-60.

Sutton, M., & Nagle, F. (2006). Emerging Economic Models for Vulnerability Research. *WEIS*.

Tai, E. T. T., & Koops, B. J. (2015). Zorgplichten tegen cybercrime. *Nederlands Juristenblad*, 231-261.

Takanen, A., Vuorijärvi, P., Laakso, M., & Röning, J. (2004). Agents of responsibility in software vulnerability processes. *Ethics and Information Technology*, 6(2), 93-110.

Tauwhare, R. (2016). Improving cybersecurity in the European Union: the Network and Information Security Directive*. Journal of Internet Law*, 19(2), 1-12.

Tavani, H. (2007). *The conceptual and moral landscape of computer security*. Sudbury, MA: Jones & Bartlett.

Timmerman, M.A.P. (2013). Goedwillende hackers, responsible disclosure en strafrecht. *Nederlands Juristenblad*, 87(8), pp. 483-484.

Trachtenberg, M. (2009). *The craft of international history: A guide to method*. Princeton University Press.

Trimintzios, P. Chatzichristos, G., Portesi, S., Drogkaris, P., Palkmets, L., Liveri, D., & Dufkova, A. (2017). *Cybersecurity in the EU Common Security and Defense Policy: Challenges and risks for the EU*. European Parliamentary Research Centre.

Van Evera, S. (1997). *Guide to methods for students of political science*. Cornell University Press.

Van der Meulen, N., Jo, E., & Soesanto, S. (2015). *Cybersecurity in the European Union and Beyond*. Retrieved on 22 May 2017, from http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU%282015%29536470_EN.pdf

Van der Meulen, S. (2016). Vulnerability disclosure: ENISA's guide and the Dutch approach. *Cyber Security Law & Practice*, 8-9.

van der Vleuten, A. (2012). Gendering the Institutions and Actors of the EU. In G. Abels, and J.M. Mushaben (eds.), *Gendering the European Union*: *New Approaches to Old Democratic Deficits*. Basingstoke: Palgrave.

Van ’t Hof, C. (2016). *Helpful Hackers: how the Dutch do Responsible Disclosure*. Tek Tok Uitgeverij.

Wagnsson, C., Sperling, J., & Hallenberg, J. (Eds.). (2009). *European security governance: the European Union in a Westphalian world*. London, UK: Routledge.

Waltz, E. (1998). *Information warfare: Principles and operations*. Boston, MA: Artech House.

Webber, M., Croft, S., Howorth, J., Terriff, T., & Krahmann, E. (2004). The governance of European security. *Review of international studies*, 30(1), 3-26.

Wolf, M. J., & Fresco, N. (2016). Ethics of the software vulnerabilities and exploits market. *The Information Society*, 32(4), 269-279.

Wolff, E.D., Oringher Lerner, M., Miller, P.B., Welling, M.B., & Hoff, C. (2016). The global uptake of the NIST Cybersecurity Framework. Retrieved on 20 June 2017, from https://www.crowell.com/files/20160215-The-Global-Uptake-of-the-NIST-Cybersecurity-Framework-Wolff-Lerner-Miller-Welling-Hoff.pdf

Yeung, K. (2005). Government by publicity management: Sunlight or spin. *Public Law*, 2, 360-383.

Yin, R. K. (2013). *Case study research: Design and methods*. Thousand Oaks, CA: Sage Publications.

Zina, A. (2009). *Debate on full, responsible and no disclosure as it applies to security vulnerability.* British Colombia Institute for Technology. Retrieved on 10 June 2017, from https://www.scribd.com/document/13745573/Vulnerability-Disclosure-Debate

GOVERNMENTAL DOCUMENTS

Council of Europe (2001). *Convention on Cybercrime*. Retrieved on 6 November 2016, from https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

ENISA (2006). *CSIRT Setting Up Guide in English*. Retrieved on 6 November 2016, from https://www.enisa.europa.eu/publications/csirt-setting-up-guide

ENISA (2015). *Good practice guide on Vulnerability Disclosure*: From challenges to recommendations. Retrieved on 6 November 2016, from https://www.enisa.europa.eu/publications/vulnerability-disclosure.

ENISA (2017a, May 15). *WannaCry Ransomware Outburst*. Retrieved on 20 May 2017, from https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst

ENISA (2017b, May 15). *WannaCry ransomware: First ever case of cyber cooperation at the EU-leve*l. Retrieved on 23 May 2017, from https://www.enisa.europa.eu/news/enisa-news/wannacry-ransomware-first-ever-case-of-cyber-cooperation-at-eu-level

European Commission (2013). *Cybersecurity Strategy of the European Union: An open safe and secure cyberspace* (no. 01/2013). Retrieved on 3 November 2016, from https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

European Commission (2015a). *Communication on the European Agenda on Security* (no. 185/2015). Retrieved on 1 June 2017, from https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf

European Commission (2015b). *Communication on a Digital Single Market Strategy for Europe* (no. 192/2015). Retrieved on 1 June 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52015DC0192

European Commission (2016a). *Communication on a Joint Framework on countering hybrid threats: a European Union response* (no. 18/2016). Retrieved on 1 June 2017, from http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016JC0018

European Commission (2016b). *Communication on ICT standardization priorities for the Digital Single Market* (no. 176/2016). Retrieved on 14 June 2017, from https://ec.europa.eu/digital-single-market/en/news/communication-ict-standardisation-priorities-digital-single-market

European Commission (2016c). *Evaluation of the Directive 85/374/EEC concerning liability for defective products.* Retrieved on 20 June 2017, from http://ec.europa.eu/smart-regulation/roadmaps/docs/2016_grow_027_evaluation_defective_products_en.pdf

European Commission (2016d). *Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry* (no. 410/2016). Retrieved on 6 November 2016, from https://ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and

European Commission (2017a). *EU cybersecurity initiatives: Working towards a more secure online environment*. Retrieved on 1 May 2017, from http://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf

European Commission (2017b). *Implementing Decision laying down procedural arrangements necessary for the functioning of the Cooperation Group* (no. 179/2017). Retrieved on 1 June 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017D0179&from=EN

European Commission (2017c). Horizon 2020 work programme 2016-2017: Secure societies – protecting freedom and security of Europe and its citizens (no. 2468/2017). Retrieved on 1 June 2017, from https://ec.europa.eu/research/participants/data/ref/h2020/wp/2016_2017/main/h2020-wp1617-security_en.pdf

European Commission (2017d). *Mid-Term Review on the implementation of the Digital Single Market Strategy: A Connected Digital Single Market for All* (no. 228/2017). Retrieved on 25 May 2017, from https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-228-F1-EN-MAIN-PART-1.PDF

European Commission (2017e). *Seventh progress report towards an effective and genuine Security Union* (no. 261/2017). Retrieved on 25 May 2017, from https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20170516_seventh_progress_report_towards_an_effective_and_genuine_security_union_en.pdf

European Council (1985). Directive *on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products (no. 85/374/EEC)***.** Retrieved on 5 April 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31985L0374&from=EN.

European Council (2015). *Council Conclusions on Cyber Diplomacy* (no. 6122/15). Retrieved on 15 May 2017, from http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf

European Council (2017). *Council Conclusions on a Cyber Diplomacy Toolbox* (no. 9916/17). Retrieved on 15 May 2017, from http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

European External Action Service (2016*). A global strategy for the European Union's Foreign and Security Policy: Shared vision, common action, a stronger Europe*. Retrieved on 5 November, from https://eeas.europa.eu/top_stories/pdf/eugs_review_web.

European Union (2005). *Council Framework Decision on Attacks Against Information Systems* (no. 222/2005). Retrieved on 20 May 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN

European Union (2013). *Directive on attacks against information systems* (no. 40/2013). Retrieved on 5 November 2016, from http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=URISERV%3Al33193

European Union (2014a). *Regulation on the reporting, analysis and follow-up of occurences in civil aviation* (no. 376/2014). Retrieved on 20 May 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0376&from=EN

European Union (2014b). *Horizon 2020 in brief*. Retrieved on 1 June 2017, from http://ec.europa.eu/programmes/horizon2020/en/news/horizon-2020-brief-eu-framework-programme-research-innovation

European Union (2016a). *General Data Protection Regulation* (no. 119/2016). Retrieved on 1 May 2017, from http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

European Union (2016b). *Directive concerning measures for a high common level of security of network and information systems across the Union* (no. 1148/2016). Retrieved on 1 May 2017, from http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

EUROPOL (2016). *The Internet Organised Crime Threat Assessment 2016*. Retrieved on 1 June 2017, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

National Cyber Security Centre the Netherlands (2013). *Responsible Disclosure Guideline*. Retrieved on 5 November 2016, from https://www.ncsc.nl/english/current-topics/responsible-disclosure-guideline.html

National Cyber Security Centre the Netherlands (2015a). *Introducing Responsible Disclosure, experiences in the Netherlands: A Best Practice Guide*. Retrieved on 5 November 2016, from https://www.gccs2015.com/sites/default/files/documents/BestPracticeRD-20150409_0.pdf

National Cyber Security the Netherlands (2015b). *Cyber Security Assessment the Netherlands 2015*. Retrieved on 5 November 2016, from https://www.ncsc.nl/english/current-topics/news/cyber-security-assessment-netherlands-2015.html

National Cyber Security the Netherlands (2016). *Cyber Security Assessment the Netherlands 2016*. Retrieved on 5 November 2016, from https://www.ncsc.nl/english/current-topics/Cyber+Security+Assessment+Netherlands

Openbaar Ministerie (2013). *Policy Letter Responsible Disclosure*. Retrieved on 1 June 2017, from https://www.om.nl/vaste-onderdelen/zoeken/?mode=zoek&zoeken_tab=site&zoeken_term=responsible+disclosure&zoeken_sortering=Num&zoeken_daterange_start=&zoeken_daterange_end=&Zoeken_button=

Organisation for Security and Cooperation in Europe (2013). *Confidence Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies* (no. 1106). Retrieved on 10 June 2017, from http://www.osce.org/pc/109168?download=true

Organisation for Security and Cooperation in Europe (2016). *Confidence Building Measures to reduce the risks of conflict stemming from the use of information and communication technologies* (no. 1202). Retrieved on 10 June 2017, from http://www.osce.org/pc/227281?download=true

The White House (2013, 12 February). *Executive Order: Improving Critical Infrastructure Cybersecurity* (no. 13636). Retrieved on 1 June 2017, from https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

UN GGE (2010). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (no. A/65/201). Retrieved on 15 June 2017, from http://www.unidir.org/files/medias/pdfs/final-report-eng-0-189.pdf

UN GGE (2013). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (no. A/68/98). Retrieved on 15 June 2017, from http://www.unidir.org/files/medias/pdfs/developments-in-the-field-of-information-and-telecommunications-in-the-context-of-international-security-2012-2013-a-68-98-eng-0-518.pdf

UN GGE (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (no. A/70/174). Retrieved on 15 June 2017, from http://undocs.org/A/70/174

REPORTS, NEWSPAPER ARTICLES AND OTHER LITERATURE

Bajo, G. & Varisco, G. (2016, 23 December). *Why information security is not simply a matter of black and white. Digital Team Italia*. Retrieved on 1 February 2017, from https://medium.com/team-per-la-trasformazione-digitale/cybersecurity-policy-responsible-disclosure-ethical-hacker-290918f58858

BEUC (2017). *Review of Product Liability Rules: BEUC Position Paper*. Retrieved on 10 June 2017, from http://www.beuc.eu/publications/beuc-x-2017-039_csc_review_of_product_liability_rules.pdf

Charney, S., English, E., Kleiner, A., Malisevic, N., McKay, A., Neutze, J., & Nicholas, P. (2016). *From Articulation to Implementation: Enabling progress on cybersecurity norms*. Microsoft. Retrieved on 1 June 2017, from https://mscorpmedia.azureedge.net/mscorpmedia/2016/06/Microsoft-Cybersecurity-Norms_vFinal.pdf

CIO Platform (2016a). *Coordinated Vulnerability Disclosure: Implementation Guide*. Retrieved on 1 June 2017, from https://www.cio-platform.nl/k/nl/n255/news/view/1871/4145/coordinated-vulnerability-disclosure-responsible-disclosure-available.html

CIO Platform (2016b). Coo*rdinated Vulnerability Disclosure: Model Policy and Procedure*. Retrieved on 1 June 2017, from https://www.cio-platform.nl/k/nl/n255/news/view/1871/4145/coordinated-vulnerability-disclosure-responsible-disclosure-available.html

Cisco (2017). *Cisco Annual Cybersecurity report 2017*. Retrieved on 20 April 2017, from https://www.cisco.com/c/dam/m/digital/en_us/Cisco_Annual_Cybersecurity_Report_2017.pdf

Collins, S. (2016, 20 October). *DoD announces 'Hack the Pentagon' Follow-Up initative*. US Department of Defense. Retrieved on 1 May 2017, from https://www.defense.gov/News/Article/Article/981160/dod-announces-hack-the-pentagon-follow-up-initiative/

European Corporate Just Culture Declaration (2015, 1 October). Retrieved on 1 May 2017, from https://ec.europa.eu/transport/sites/transport/files/modes/air/events/doc/2015-10-01-just-culture/declaration.pdf

European Policy Strategy Centre (2017). *Building an effective European cyber shield: Taking EU cooperation to the next level.* Retrieved on 1 June 2017, from https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf

Electronic Frontier Foundation (2008). *A gray hat guide*. Retrieved on 1 May 2017, from https://www.eff.org/pages/grey-hat-guide

Fimin, M. (2016, 3 May). *Meeting the new vulnerability disclosure challenge*. *SC Magazine.* Retrieved on 15 June 2017, from https://www.scmagazineuk.com/meeting-the-new-vulnerability-disclosure-challenge/article/531534

Forum of Incident Response and Security Teams (FIRST) (2016). *Guidelines and practices for multi-party vulnerability coordination*. Retrieved on 1 May 2017, from https://www.first.org/_assets/downloads/FIRST-Multiparty-Vulnerability-Coordination-draft.pdf

Frenkel, S., Scott, M., & Mozur, P. (2017, 28 June). Mystery of motive for a ransomware attack: Money, mayhem or message? *New York Times*. Retrieved on 29 June 2017, from https://www.nytimes.com/2017/06/28/business/ramsonware-hackers-cybersecurity-petya-impact.html?mcubz=0&_r=1

Gayle, D., Topping, A., Sample, I., Marsh, S., & Dodd, V. (2017, 13 May). NHS seek to recover from global cyberattack as security concerns resurface. *The Guardian.* Retrieved on 22 May 2017, from https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20

Hassan, M. (2017, 26 May). *Senators Hassan, Portman introduce bipartisan bill to strengthen cyber defenses at Department of Homeland Security*. Retrieved on 1 June 2017, from https://www.hassan.senate.gov/news/press-releases/senators-hassan-portman-introduce-bipartisan-bill-to-strengthen-cyber-defenses-at-department-of-homeland-security

Herns, A. & Gibbs, S. (2017, 12 May). What is Wannacry Ransomware and why is it attacking global computers. *The Guardian*. Retrieved on 22 May 2017, from https://www.theguardian.com/technology/2017/may/12/nhs-ransomware-cyber-attack-what-is-wanacrypt0r-20

International Organization for Standardization (2013). *ISO Standard vulnerability handling process standard (ISO/IEC 3011)*. Retrieved on 7 November 2016, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=53231

International Organization for Standardization (2014). *ISO Standard vulnerability disclosure (ISO/IEC 29147)*. Retrieved on 7 November 2016, from http://www.iso.org/iso/catalogue_detail.htm?csnumber=45170

Kleiner, A. Nicholas, P., & Sullivan, K. (2013). L*inking cybersecurity policy and performance.* Microsoft. Retrieved on 15 June 2017, from http://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Tecnologie/2013/02/SIR-Special-Edition-Security-Atlas-whitepaper.pdf

Laakso, M., Takanen, A., & Röning, J. (1999). *The Vulnerability Process: a tiger team approach to resolving vulnerability cases*. Retrieved on 20 May 2017, from https://www.ee.oulu.fi/research/ouspg/PROTOS_FIRST1999-process

Lemos, R. (2002, September 23). *A Thin Gray Line*. CNET. Retrieved on 8 November 2016, from http://news.cnet.com/2009-1001_3-958129.html

Leyden, J. (2011). *EU Parliament Suspends Webmail After Cyber-Attack*. *The Register*. Retrieved on 3 November 2016, from: http://www.theregister.co.uk/2011/03/31/eu_parliament_hack/

Microsoft (2016). *Microsoft Security Intelligence Report 2016.* Retrieved on 20 April 2017, from https://www.microsoft.com/security/sir/default.aspx

Muynck, J., Graux, H. & Robinson, N. (2013). *The Directive on attacks against information systems: A Good Practice Collection for CERTs on the Directive on attacks against information systems*. ENISA. Retrieved on 10 June 2017, from https://www.enisa.europa.eu/publications/the-directive-on-attacks-against-information-systems

National Institute of Standards and Technology (NIST) (2014, 12 February). *Framework for improving critical infrastructure cybersecurity.* Retrieved on 1 May 2017, from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

National Institute of Standards and Technology (NIST) (2017, 10 April). *Joint Comments on "Framework for Improving Critical Infrastructure Cybersecurity" version 1.1.* Retrieved on 1 May 2017, from https://www.nist.gov/sites/default/files/documents/2017/05/12/2017-04-10-consortium.pdf

National Telecommunications and Information Administration (2016). *Vulnerability Disclosure Attitudes and Actions*. Retrieved on 19 December 2016, from https://www.ntia.doc.gov

Nicholas, P., McKay, A., Neutze, J., & Sullivan, K. (2014). *International Cybersecurity Norms: Reducing conflict in an Internet-depended world.* Retrieved on 1 June 2017, from https://blogs.microsoft.com/microsoftsecure/2014/12/03/proposed-cybersecurity-norms/

Organisation for Economic Cooperation and Development (OECD) (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy.* Retrieved on 10 June 2017, from https://www.oecd.org/sti/ieconomy/cybersecurity%20policy%20making.pdf

Rechtbank Den Haag (2014, 18 December). *09/748019-12*. Retrieved on 15 June 2017, from https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2014:15611&show button=true&keyword=hack+groene+hart

Rechtbank Oost-Brabant (2013, 19 February). *01/820892-12*. Retrieved on 15 June 2017, from https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBOBR:2013:BZ1157&keyword=820892-12

Schaake, M. (2016, 1 December). *EU budget creates bug bounty program to improve cybersecurity*. Retrieved on 1 May 2017, from https://marietjeschaake.eu/en/eu-budget-creates-bug-bounty-programme-to-improve-cybersecurity

Segal, A. (2017, 29 June). The development of cyber norms at the United Nations ends in deadlock. Now what? *Council on Foreign Relations*. Retrieved on 30 June 2017, from https://www.cfr.org/blog-post/development-cyber-norms-united-nations-ends-deadlock-now-what

Shepherd, S. A. (2003). V*ulnerability Disclosure: How do we define Responsbile Disclosure*? Retrieved on 3 November 2016, from https://www.sans.org/reading-room/whitepapers/threats/define-responsible-disclosure-932

Symantec (2016). *Internet Security Threat Report 2016*. Retrieved on 20 April 2017, from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

T. (2017, 17 March). *Vulnerability co-ordination pilot*. Retrieved on 15 May 2017, from https://www.ncsc.gov.uk/blog-post/vulnerability-co-ordination-pilot

Techopedia (2017). *What is a white hat*?. Retrieved on 1 May 2017, from https://www.techopedia.com/definition/10349/white-hat-hacker

Techopedia (2017). *What is an information system*?. Retrieved on 1 May 2017, from https://www.techopedia.com/definition/24142/information-system-is

Van Leemputten, P. (2016, 8 December). *Ethish hacken bijna legaal in Belgie: Want alles zit vol lekken*. *KNACK*. Retrieved on 1 February 2017, from http://datanews.knack.be/ict/nieuws/ethisch-hacken-bijna-legaal-in-belgie-want-alles-zit-vol-lekken/article-normal-787153.html

ANNEX 1: EXAMPLE OF A GOVERNMENTAL CVD POLICY

Retrieved from www.ncsc.nl/english

"The National Cyber Security Centre (NCSC) contributes to jointly enhancing the resilience of the Dutch society in the digital domain and, in doing so, realises a safe, open and stable information society by providing insight and offering a perspective for action. Therefore it is essential that the ICT systems of the NCSC are safe. The NCSC strives towards providing a high level of security for its systemn. However, it can occur that one of these systems has a vulnerability.

Vulnerabilities in ICT systems of the NCSC

If you have found a weak spot in one of the ICT systems of the NCSC, the NCSC would like to hear about this from you, so the necessary measures can be taken as quickly as possible to rectify the vulnerability. To deal with the vulnerabilities in the NCSC ICT systems responsibly, we propose several agreements. You may hold the NCSC to this when you discover a weak spot in one of our systems.

The NCSC asks you:

- *To e-mail your findings to cert@ncsc.nl. Encrypt your findings if possible with the PGP Key of the NCSC to prevent the information falling into the wrong hands.*
- *Provide sufficient information to reproduce the problem so that the NCSC can solve the problem as quickly as possible. The IP address or the URL of the system affected and a description of the vulnerability is usually sufficient, but more may be needed for more complex vulnerabilities.*
- *Leave your contact details so that the NCSC can contact you to cooperate on a safe result. At least, leave an e-mail address or a telephone number.*
- *Report the vulnerability as quickly as possible after its discovery.*
- *Do not share the information on the security problem with others until the problem has been solved.*
- *Handle the knowledge on the security problem with care by not performing any acts other than those necessary to reveal the security problem.*

Avoid in any case the following acts:

- *installing malware.*
- *copying, changing or deleting data in a system (an alternative to this is making a directory listing of a system).*
- *making changes to a system.*
- *repeatedly accessing the system or sharing access with others.*
- *using so-called "brute force" to access systems.*
- *using denial-of-service or social engineering.*

What you can expect:

- *If you comply with the conditions above when reporting the observed vulnerability in an ICT system of the NCSC, the NCSC will not attach any legal consequences to this report.*
- *The NCSC handles a report confidentially and does not share personal details with third parties without permission from the reporter, unless this is mandatory by virtue of a judicial decision.*
- *In mutual consultation, the NCSC can, if you desire, mention your name as the discoverer of the reported vulnerability.*
- *The NCSC will send you a confirmation of receipt within one working day.*
- *The NCSC responds within three working days to a report with an assessment of the report and an expected date for a solution.*
- *The NCSC keeps the reporter up-to-date on the progress made with solving the problem.*
- *The NCSC solves the security problems observed by you in a system as quickly as possible, but no later than within 60 days. In mutual consultation, whether and in what way the problem will be published, after it has been solved, is determined.*
- *The NCSC offers a reward as thanks for help. Depending on the seriousness of the security problem and the quality of the report, the reward can vary from a T-shirt to maximum EUR 300 in gift vouchers. It must concern a serious problem that is unknown to NCSC.*

Vulnerabilities in ICT systems of third parties:

The NCSC would like to hear if you find a weak spot in a system of the Dutch government or in a system with a vital role. For systems of other owners/administrators and/or suppliers, in the first instance you must approach the organisation yourself. If the organisation does not or inadequately responds, you can inform the NCSC. In this regard, the NCSC will play a role as intermediary to achieve result together.

For reports on systems of third parties:

- *The NCSC will respond to a report within three working days by contacting the owner and giving you a response.*
- *The owner is primarily responsible for keeping the reporter informed about the progress made in solving the problem.*
- *The NCSC will help the owner with advice so that the security problem can be solved as quickly as possible.*
- *The NCSC asks you to give us information on whether and how there has already been contact with the organisation.”*

ANNEX 2: EXAMPLE OF A COMPANY'S CVD POLICY

Retrieved from www.responsibledisclosure.nl/en

"At the … Corporation, we consider the security of our systems a top priority. But no matter how much effort we put into system security, there can still be vulnerabilities present.

If you discover a vulnerability, we would like to know about it so we can take steps to address it as quickly as possible. We would like to ask you to help us better protect our clients and our systems.

Please do the following:

- *E-mail your findings to cert@example.com. Encrypt your findings using our PGP key to prevent this critical information from falling into the wrong hands,*
- *Do not take advantage of the vulnerability or problem you have discovered, for example by downloading more data than necessary to demonstrate the vulnerability or deleting or modifying other people's data,*
- *Do not reveal the problem to others until it has been resolved,*
- *Do not use attacks on physical security, social engineering, distributed denial of service, spam or applications of third parties, and*
- *Do provide sufficient information to reproduce the problem, so we will be able to resolve it as quickly as possible. Usually, the IP address or the URL of the affected system and a description of the vulnerability will be sufficient, but complex vulnerabilities may require further explanation.*

What we promise:

- *We will respond to your report within 3 business days with our evaluation of the report and an expected resolution date,*
- *If you have followed the instructions above, we will not take any legal action against you in regard to the report,*
- *We will handle your report with strict confidentiality, and not pass on your personal details to third parties without your permission,*
- *We will keep you informed of the progress towards resolving the problem,*
- *In the public information concerning the problem reported, we will give your name as the discoverer of the problem (unless you desire otherwise), and*
- *As a token of our gratitude for your assistance, we offer a reward for every report of a security problem that was not yet known to us. The amount of the reward will be determined based on the severity of the leak and the quality of the report. The minimum reward will be a €50 gift certificate.*

We strive to resolve all problems as quickly as possible, and we would like to play an active role in the ultimate publication on the problem after it is resolved."