

Antti-Ilari Söderholm

**THREATS AND CHALLENGES  
AROUND EUROPEAN CYBER SECURITY  
COOPERATION IN THE CONTEXT OF THE  
EUROPEAN UNION DIRECTIVE ON SECURITY  
OF NETWORK AND INFORMATION SYSTEMS**



UNIVERSITY OF JYVÄSKYLÄ  
FACULTY OF INFORMATION TECHNOLOGY

2018

## ABSTRACT

Söderholm, Antti-Ilari

Threats and Challenges around European Cyber Security Cooperation in the Context of the European Union Directive on Security of Network and Information Systems

Jyväskylä: University of Jyväskylä, 2018, 102 p.

Computer Science (Cyber Security), Master's Thesis

Supervisor: Lehto, Martti

This thesis discusses of the European Union (EU) Directive on Security of Network and Information Systems (NIS Directive), threats of cyber space that the EU embrace or would have to overcome in the future, and challenges around European cyber security cooperation in accordance with the NIS Directive. The research was conducted with qualitative research design, pragmatic worldview, and the desired strategy of inquiry was a case study. Purpose of the research was to provide a view on the current state of European cyber security cooperation. Thereby, the research was focused onto (i) find out what potential threats there are, (ii) what are the EU's objectives of the NIS Directive, and (iii) what challenges are enunciated of the cooperation. Results indicated that threat landscape is broad and evolving where the NIS Directive is required to safeguard European Digital Single Market. Objective of the NIS Directive is to boost and reach a high common level of security of network and information systems across the EU. Critical infrastructure must be secured against threats, both on public and private sector. This concerns Operators of Essential Services (OES) and Digital Service Providers (DSPs). There are challenges around the cooperation, such as varying approaches, different maturity level, lack of trust, incident reporting is not clear enough, OES and DSPs are differently identified across the EU, compliance and sanctions vary, and some elements are left out of scope of the NIS Directive. Despite the challenges, the NIS Directive is needed in defending Member States against future threats.

Keywords: NIS Directive, European Union, cyber security, cooperation, challenges, critical infrastructure, operators of essential services, digital service providers

## TIIVISTELMÄ

Söderholm, Antti-Ilari

Uhkat ja haasteet Euroopan kyberturvallisuusyhteistyön ympärillä Euroopan Unionin verkko- ja tietojärjestelmien turvallisuudirektiivin kontekstissa

Jyväskylä: Jyväskylän yliopisto, 2018, 102 s.

Tietojenkäsittelytiede (Kyberturvallisuus), pro gradu -tutkielma

Ohjaaja: Lehto, Martti

Tämä tutkielma käsittelee Euroopan Unionin (EU) verkko- ja tietojärjestelmien turvallisuudirektiiviä (NIS-direktiivi), EU:n tällä hetkellä tai tulevaisuudessa kohtaamia uhkia sekä haasteita, joita eurooppalaiseen, NIS-direktiiviin pohjautuvaan kyberturvallisuusyhteistyöhön liittyy. Tämä tutkimus tehtiin kvalitatiivisena tutkimuksena, pragmaattisella maailmankuvalla ja tapaustutkimuksena. Tutkimuksen tarkoituksena oli selvittää tämän hetken eurooppalaisen kyberturvallisuusyhteistyön kuvaa. Näin ollen, tutkimus keskittyi (i) löytämään potentiaaliset uhkat, (ii) selvittää EU:n tavoitteet direktiiville sekä (iii) käsitellä esiintuotuja yhteistyön haasteita. Tutkimuksen tulokset osoittivat, että uhkakuva on alati laajentuva ja kehittyvä, johon NIS-direktiiviä tarvitaan turvaamaan eurooppalainen digitaalinen markkinapaikka (Digital Single Market). EU:n tavoitteena on varmistaa yhteinen korkeatasoinen verkko- ja tietojärjestelmien turvallisuus koko unionissa. Kriittinen infrastruktuuri täytyy suojata niin julkisella kuin yksityisellä puolella. Tämä koskettaa keskeisten palvelujen tarjoajia (KPT) ja digitaalisten palvelujen tarjoajia (DPT). Yhteistyön ympärillä on haasteita, kuten vaihtelevat lähestymistavat, erilainen maturiteettitaso, luottamuksen puute, poikkeamien raportointi ei ole riittävän selkeää, KPT:t ja DPT:t määritellään eri tavoin koko unionissa, direktiivin noudattamisen velvoitteet ja siitä seuraavat sanktiot vaihtelevat sekä joitakin tietoturvan kannalta merkittäviä puolia on jätetty direktiivin ulkopuolelle. Haasteista huolimatta direktiivi on tarpeellinen, jotta tulevaisuuden uhkia vastaan voidaan jäsenmaita puolustaa.

Asiasanat: NIS-direktiivi, Euroopan Unioni, kyberturvallisuus, yhteistyö, haasteet, kriittinen infrastruktuuri, keskeisten palvelujen tarjoajat, digitaalisten palvelujen tarjoajat

## ACKNOWLEDGEMENTS

This project has been both challenging and rewarding at the same time. There was only limited time available when written besides daily work. It certainly raised the level of complexity. 2018 will remain as the year to be remembered.

I want to thank friends and family for understanding the demands of the writing process. Many thanks to professor Martti Lehto for his assistance and flexibility. Also, I am thankful for doctor Monica Mookherjee whose tips and hints provided back in the days were considered with this thesis writing process too.

There are plenty of areas to explore regarding to the thesis subject. Unexplored areas are described in the end. My personal wish is that they would provide sparking thoughts for someone to have a further research, to continue from where this thesis was left.

Helsinki, 29 October 2018,

Antti-Ilari Söderholm

## LIST OF ABBREVIATIONS

ACK	Acknowledge
AI	Artificial Intelligence
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information, National Cybersecurity Agency of France
APT	Advanced Persistent Threat
Botnet	Robot Network
CERT	Computer Emergency Response Team
CERT-EU	Computer Emergency Response Team of the European Union
CSIRT	Computer Security Incident Response Team
CSS	Cross-Site Scripting
Cybersecurity Act	Information and Communication Technology Cybersecurity Certification
DDoS	Distributed Denial of Service
DDoSaaS	Distributed Denial of Service-as-a-Service
DNS	Domain Name System
DoS	Denial of Service
DSP	Digital Service Providers
EC3	European Cybercrime Centre
ECFR	European Council on Foreign Relations
ENISA	European Union Agency for Network and Information Security, also known as EU Cybersecurity Agency
EU	The European Union
Europol	European Union Agency for Law Enforcement Cooperation
EP	The European Parliament
GDPR	General Data Protection Regulation
GCSP	Geneva Centre for Security Policy
ICMP	Internet Control Message Protocol
ICS	Industrial Control System
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
IIoT	Industrial Internet of Things
IoT	Internet of Things
ISO	International Organization for Standardization
IT	Information Technology
IXP	Internet Exchange Point
Malware	Malicious Software
MBR	Master Boot Record
NATO	The North Atlantic Treaty Organization
NIS	Network and Information Systems

NISD	The NIS Directive, see NIS Directive
NIS Directive	The Directive on Security of Network and Information Systems
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OCG	Organised Crime Group
OES	Operators of Essential Services
PC	Personal Computer
PPP	Public-Private Partnership
PSD 2	Second Payment Services Directive
RC4	Rivest Cipher 4 encryption algorithm
RSA	Rivest-Shamir-Adleman encryption algorithm
SCADA	Supervisory Control and Data Acquisition
SMB	Microsoft Windows Server Message Block
Spam	Spiced ham, see UBE and UCE
SPoC	Single Point of Contact
SUPO	Suojelupoliisi, Finnish Security Intelligence Service
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SYN	Synchronise
TCP	Transmission Control Protocol
The Union	The European Union
UBE	Unsolicited Bulk Email
UCE	Unsolicited Commercial Email
U.S.	The United States of America

## LIST OF FIGURES

FIGURE 1. Exploit kit workability example .....	35
FIGURE 2. Threat actors divided into six categories.....	37
FIGURE 3. A small selection of cyber incidents throughout the world in 2016 .	38
FIGURE 4. Screenshot of WannaCry infected device.....	39
FIGURE 5. Notable targets of WannaCry in the EU.....	40
FIGURE 6. Screenshot of NotPetya infected device.....	41
FIGURE 7. The main areas and sectors of the NIS Directive requirements.....	58
FIGURE 8. Cyber cooperation structure with related articles .....	60
FIGURE 9. Organisational cooperation levels of the NIS Directive.....	62
FIGURE 10. Perceptions of the EU as a security actor .....	65
FIGURE 11. Perceived vulnerability to cyber-attacks .....	69
FIGURE 12. Interdependencies of each Critical Infrastructure.....	74

## LIST OF TABLES

TABLE 1. Top threats in 2016 and 2017 with annual change indicator .....	26
TABLE 2. State-of-play of the transposition of the NIS Directive .....	67

# TABLE OF CONTENTS

ABSTRACT .....	2
TIIVISTELMÄ .....	3
ACKNOWLEDGEMENTS .....	4
LIST OF ABBREVIATIONS.....	5
LIST OF FIGURES .....	6
LIST OF TABLES .....	7
TABLE OF CONTENTS.....	8
1 INTRODUCTION .....	11
1.1 Background.....	11
1.2 Problem Statement.....	12
1.3 Literature Review .....	13
1.4 Significance of the Research.....	14
1.5 Research Questions & Objectives .....	15
1.6 Scope of the Research.....	16
1.7 Hypothesis .....	17
1.8 Terminology and Clearance .....	18
1.9 Overview of the Chapters.....	18
1.10 Summary of the Chapter .....	20
2 RESEARCH METHODS.....	21
2.1 Introduction.....	21
2.2 Research Setting .....	21
2.3 Approach & Design.....	22
2.4 Strategy of Inquiry.....	22
2.5 Evidence Gathering .....	23
2.6 Conclusion .....	23
3 CYBER THREATS .....	24
3.1 Introduction.....	24
3.2 Top Cyber Threats .....	25
3.2.1 Malware .....	27
3.2.2 Web-Based Attacks .....	27
3.2.3 Web Application Attacks .....	28
3.2.4 Phishing .....	28
3.2.5 Spam.....	29
3.2.6 Denial of Service .....	29



3.2.7	Ransomware.....	30
3.2.8	Botnets.....	31
3.2.9	Insider Threat.....	31
3.2.10	Physical Manipulation / Damage / Theft / Loss .....	32
3.2.11	Data Breaches.....	32
3.2.12	Identity Theft .....	33
3.2.13	Information Leakage.....	34
3.2.14	Exploit Kits.....	34
3.2.15	Cyber Espionage .....	35
3.3	Recent Major Cyber Incidents.....	36
3.3.1	Threat Landscape Overview and Threat Actor Motives .....	36
3.3.2	WannaCry Ransomware .....	38
3.3.3	NotPetya Malware .....	40
3.3.4	Equifax Data Breach.....	41
3.3.5	Future Threats and Developments .....	42
3.4	Conclusions.....	43
4	REQUIREMENTS AND ELABORATION OF THE NIS DIRECTIVE.....	45
4.1	Introduction.....	45
4.2	Requirements of the NIS Directive.....	45
4.2.1	General Provisions .....	45
4.2.2	National Frameworks on the Security of Network and Information Systems .....	47
4.2.3	Cooperation.....	49
4.2.4	Security of the Network and Information Systems of Operators of Essential Services .....	52
4.2.5	Security of the Network and Information Systems of Digital Service Providers.....	53
4.2.6	Standardisation and Voluntary Notification.....	55
4.2.7	Final Provisions .....	55
4.2.8	Annexes I-III.....	56
4.3	Elaboration of the NIS Directive.....	57
4.3.1	Objectives and Scope .....	57
4.3.2	Cooperation on National and European Level .....	59
4.4	Conclusions.....	63
5	CHALLENGES OF THE COOPERATION.....	64
5.1	Introduction.....	64
5.2	Variety in Approaches .....	64
5.3	Variety in Maturity and Resources .....	68
5.4	Trust and Language.....	70
5.5	Reporting and Confidentiality .....	72
5.6	Identification of Entities.....	73
5.7	Compliance and Sanctions .....	75
5.8	Out of Scope.....	76
5.9	Conclusions.....	77

6	DISCUSSION .....	79
6.1	Concerns.....	79
6.2	Opportunities .....	81
6.3	Future Research.....	82
7	CONCLUSIONS.....	83
	REFERENCES.....	86
	APPENDIX I: THE NIS DIRECTIVE ANNEX I: REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTS) .....	96
	APPENDIX II: THE NIS DIRECTIVE ANNEX II: DEFINITIONS OF OPERATORS OF ESSENTIAL SERVICES .....	97
	APPENDIX III: THE NIS DIRECTIVE ANNEX III: DEFINITIONS OF DIGITAL SERVICE PROVIDERS.....	100
	APPENDIX IV: THE NIS DIRECTIVE ARTICLE 4: TERM DEFINITIONS.....	101

# 1 INTRODUCTION

## 1.1 Background

There are billions of information systems and devices connected to the internet. They interact on a new scale and level never seen before. These information systems and devices can improve lives of citizens and economies, but individuals, companies and countries are also dependable of their workability as they have become indistinguishable part of our lives. (Niebler, 2018)

Simultaneously, information systems and devices have become attractive targets for attackers when they consist loads of valuable information, such as transfer of money and personal information. Disturbance of them can also create risks to international peace and security (United Nations, 2015). Probabilities for perpetrators of getting caught are relatively low due to complexity of the cyber space. (Europol, 2018)

A combination of great usage and threats require coherent cyber security, which level of maturity vary across Europe and beyond. These together have evoked governments to guard their societies, citizens, business, and fundamentally whole existence. As technologies and cyber security are becoming more complex phenomenon, it has become harder for business, military and governments to struggle against threats on their own. (European Political Strategy Centre, 2017)

Therefore, cooperation is needed on all levels. The European Union (EU) with its Member States have realised this demand. To improve cooperation, in 2016, the EU published *The Directive on Security of Network and Information Systems* (European Union, 2016a), better known and later referred as “the NIS Directive” in this thesis. Although, the EU forms of 28 Member States, there are approximately 500 million people in the area, and plenty of different cultures (European Commission, 2014). Therefore, implementation of the NIS Directive and execution of cooperation are not an easy task to solve. (Surguy, 2017)

This paper is a result of research that has focused on European cyber security cooperation in accordance with the NIS Directive. Three main focus

areas consist threats, the Directive and challenges. To understand different viewpoints of challenges, there must be an understanding of multiple types of threats that Europe is facing now and most likely in the future, as technology is infiltrating evermore to cyber space and European life in general. Equally important is to comprehend what the NIS Directive is fundamentally about, what it demands from public and private sector in increasing and maintaining cooperation between Member States. Based on these two fundamentals, we may better understand challenges that are exposed around the NIS Directive.

The research presented in this paper is a pro gradu thesis for a Master of Science program in Cyber Security at the University of Jyväskylä. The thesis belongs to Faculty of Information Technology, more specifically onto research environment of Computer Science.

This Introduction chapter introduces to the topic. It explains the subject in a problem statement form, provides a literature review, underlines significance of the research, presents research questions and objectives for the research, defines scope and restrictions of the research, discuss about hypothesis briefly, provides terminology and clearance, overview of following chapters, and in the last section this introduction chapter is summarised.

## 1.2 Problem Statement

Our societies are gradually more dependent on technologies, networks and their functionality, including those devices, networks, systems and services that are essential for Member States of the EU. Simultaneously, threats in cyber space are increasing, including cybercrimes, cyber vandalism, cyber intelligence and espionage, cyber terrorism and even state sponsored cyber warfare. (Lehto, 2015)

To have more reliable infrastructure in the EU and to safeguard its Digital Single Market - which is a core element of business in the EU - collaboration in cyber security was seen required. Since Member States can confront issues better together than individually, the EU published new cyber security legislation: the NIS Directive. Objective of the NIS Directive is to boost and achieve a high overall level of security of network and information systems (NIS) across the EU, both public and private sector. As the first EU-wide cyber security legislation, it offers legal measures for achievement of the objective. (European Commission, 2018a)

Fundamentally, the NIS Directive originates from the 2013 EU Cybersecurity Strategy (European Commission, 2013). It was adopted by the European Parliament (EP) on 6 July 2016 and entered into force in August 2016. After that, Member States of the EU had to transpose the NIS Directive into their national laws by 9 May 2018. During following six months, by 9 November 2018, they must have identified identify Operators of Essential Services (OES) and Digital Service Providers (DSPs). The Directive obligates Member States to consider not only their national cyber security capabilities but

also private sector companies operating in their area. There is demand to have more effective EU-level cyber security cooperation. (European Commission, 2018a)

Implementation of the NIS Directive, cooperation between Member States and largely emphasised Public-Private Partnership (PPP) are easier said than done, especially since the NIS Directive is a directive not a regulation<sup>1</sup> (Carrapico and Barrinha, 2017). To understand these challenges, we must understand two basic elements that have driven the EU towards the NIS Directive. First, ever evolving and expanding threat landscape *id est* what kind of threats Europe is facing and aiming to defend against. Second, it is hard to discuss about challenges of the NIS Directive if the Directive itself is unfamiliar. Hence, there must be an understanding of what the NIS Directive is fundamentally about, and what it means for Member States, including public and private sector entities. By then, we may essentially discuss and understand all probable and likable challenges that the NIS Directive and vast cooperation requirements cause. These topics and their features this research was focused on to explore.

### 1.3 Literature Review

When literature regarding to the NIS Directive was evaluated, it became obvious that there was no research made with the exact approach as this thesis. Even the NIS Directive is relatively new, published in 2016, quite surprisingly not much previous research around the Directive in general was made. The result underlines significance of this research which will be elaborated more on section 1.4. However, some articles have discussed around the NIS Directive, but from different perspectives or with alternating depths.

Based on the literature review, articles and researches handling the NIS Directive are published close to the topic. The closest ones considering this research are a journal article by Holzleitner and Reich (2017), “European Provisions for Cyber Security in the Smart Grid - an Overview of the NIS-directive”, providing an overview on the Directive and its influences on energy sector; and a conference paper by Hellwig et. al. (2016), “Major Challenges in Structuring and Institutionalizing CERT-communication”, which discuss of formal CERT communication challenges.

Also, three researches are worth to mention. First, a pro gradu thesis by Rantala (2017<sup>2</sup>), “Two sides of NIS Directive - Risks and Risk Management<sup>3</sup>”,

---

<sup>1</sup> The difference between a directive and a regulation is that regulations come into force as such, whereas directives are to be transposed into national laws of Member States. Directives leave more options for Member States to adjust them which means that approaches onto directives and outcomes usually vary on country by country basis. (ENHESA, 2014)

<sup>2</sup> University of Jyväskylä. (Rantala, 2017)

<sup>3</sup> Original topic in Finnish: *NIS-direktiivin kahdet kasvot - riskit ja riskienhallinta*. (Rantala, 2017)

discussing of risks and their management in accordance with the Directive which slightly overlaps with this research. Second, a master's thesis by Eltzholtz (2017<sup>4</sup>), "Cooperation in European Cyber Security: An International Relations Perspective on Collective Cyber Security in the European Union", which discuss around European cyber security strategies from perspectives of international relations, providing theory and framework-based viewpoint on challenges. Third, a university of applied sciences higher degree thesis by Pollari (2017<sup>5</sup>), "Security Management Governance Development<sup>6</sup>", discussing around security management standards, also relating to the NIS Directive.

When evaluating literature around the NIS Directive, it became obvious that there is a major gap in research of the NIS Directive. Especially, this was seen around cyber security cooperation in accordance with the Directive. When aiming to fill the mentioned gap, there has been APA (American Psychological Association) referencing in use throughout the thesis.

## 1.4 Significance of the Research

Like mentioned in the literature review, the NIS Directive is relatively new regulative document and there is a gap in research regarding to the thesis topic. To exemplify this, the following provides a very illustrative view: When comparing a search engine hits between the NIS Directive and the (EU's) General Data Protection Regulation (GDPR, European Union, 2016b) which also was published in 2016 and entered into force on 25 May 2018, we notice a great difference in number of research hits regarding to these two regulative documents. On 26 September 2018, with an entry "General Data Protection Regulation" made on Google Scholar indicated 23 100 results, whereas "NIS Directive" indicated 559 results, which is only 2,4 % of those compared to the GDPR. So, there seemed to be relevantly more research done of the GDPR than of the NIS Directive, which had gotten less focus.

Certainly, when there was not as much NIS Directive material available, it was one challenging point during the research process. The research gap of the EU cyber security and policy field is also underlined by Carrapico and Barrinha (2018)<sup>7</sup>. Consequently, lack of research underlines significance of the research evermore.

Not only the lack of research, during the research process it became obvious that it is vital to understand why there are complications and challenges around the implementation and cooperation. Research of this kind is important to understand the founding documents and their affections on

---

<sup>4</sup> Aalborg University. (Eltzholtz, 2017)

<sup>5</sup> Savonia University of Applied Sciences (Pollari, 2017)

<sup>6</sup> Original topic in Finnish: *Tietoturvallisuuden hallintamallin kehittäminen*. (Pollari, 2017)

<sup>7</sup> Article title: European Union cyber security as an emerging research and policy field. (Carrapico and Barrinha, 2018)

European cyber security scheme. At least, they need to be understood to overcome implementation and cooperation challenges, or any other relevant future object that may be confronted. The more explored, the more subject itself was found fascinating.

Finally, as the topic is neither much explored nor ubiquitously understood, more importantly as an outcome, this research may provide some new viewpoints for the scientific community of Information Technology and Computer Science. In chapter six, this thesis discusses of future research probabilities that the research could not focus on as there is still loads to explore in the research area.

## 1.5 Research Questions & Objectives

The structure of this thesis is fundamentally based on research questions. There are totally seven chapters which of three are answering on sub-questions, four are supportive chapters and these seven altogether answer to the main question. Outline of the thesis is: two supportive chapters in the beginning (introduction, research methods), two in the end (discussion, conclusions), and three body chapters in the middle answering on sub-questions.

The main question of the research was: **What threats and challenges there are in European cyber security cooperation in the context of the NIS Directive?** Objective of the main question is to find an overall answer into the issue. The “overall answer” considers not only challenges themselves but also phenomenon around them. This means understanding background and requirements of the NIS Directive. When surrounding phenomenon is explored and explained, challenges themselves can be better understood.

Therefore, to answer to the main question thoroughly, there are three sub-questions supporting the objective of the main question. Each sub-question and their objectives focus on certain area, which are:

1. **What potential threats there are?** – Objective of this sub-question has been to find answers on what forces *id est* what cyber and information threats there are that have driven the EU forming the NIS Directive and towards cooperation. This is a fundamental element of the research because by understanding surrounding threat landscape we may better understand why the Directive is needed and analyse effectiveness of it, including its core element, cooperation, against such threats. Answer on this sub-question discuss and elaborate the current and probable emerging threats against the EU.
2. **What are the EU’s objectives of the NIS Directive?** – Objective of this sub-question has been to elaborate what the NIS Directive consists and what implementation of the Directive means for Member States of the EU. Answer to this sub-question aim to explain what the NIS Directive fundamentally is about by exploring the NIS Directive requirements. The

purpose has been to understand what the Directive requirements mean and demand for implementation by Member States and relative entities.

3. **What challenges are enunciated of the cooperation?** – Objective of this sub-question has been to dig into presented challenges that implementation of the NIS Directive and cooperation cause. These include challenges around the EU bodies, Member States, private companies and relationships among them. Answer considers direct and in-direct challenges of the NIS Directive. Basically, answer for this question focus on raised problems regarding to the EU cyber security cooperation.

As briefly presented in the beginning of this section, there are three body chapters where the sub-questions are being answered. The main question is answered partially based on the sub-question results and partially in reflective discussion chapter. Finally, an answer to the main question is presented in conclusive chapter in the end.

## 1.6 Scope of the Research

Resource of time and conducting the research process beside daily work were limiting this research which means that not all available material were explored, and limitations thereby had to be set. Scope of this research was limited to the NIS Directive itself, some chosen supporting documents around the topic and all relevant implementation and cooperation articles and releases were taken into scope. The thesis discusses around the NIS Directive itself and what has been written about it rather than exploring plenty of surrounding documents, including neither specific member state approaches nor relative regulations mentioned in and around the NIS Directive which, for sure, would have given more in-depth analysis. Supporting material are significant part of the research where some examples of relative documents, or of Member States were used but, due to time limit and scope of the research (a master's thesis, not a doctoral research), not each document was thoroughly and, in some cases, sufficiently analysed.

Plenty of processes regarding to the application of the Directive were progressing whilst this thesis was being written. The thesis was conducted during the time of application phase in 2018, before Member States had nominated their OES. Thus, no nominated OES are handled within the research. Also, unlike the author expected, not that many solutions for challenges were enunciated which made to limit the scope and made to drop down one sub-question regarding to probable solutions<sup>8</sup>.

---

<sup>8</sup> Due to not finding enough convincing results, sub-question “What would be probable solutions to improve the cooperation?” was dropped off.



Other notable limitations are that the research was taking stand neither on civil-military cooperation nor much on EU-NATO<sup>9</sup> companionship which would have been interesting areas to research and could have given wider perspectives on the European cooperation as well.

The author does not have substantial legal education background, aside from some separate legal courses regarding to international relations and cyber security, and work projects around the GDPR, so interpretations of the NIS Directive or member state laws were not that professional manner evaluated from a legal perspective.

During planning phase, interviews were kept as an option. They would have provided more in-depth, professional viewpoint onto the research but were intentionally out-scoped. This research was decided to be based only on available public resources.

## 1.7 Hypothesis

Around the EU cyber security cooperation, there seemed to be practical, political and cyber security related challenges. These became obvious when the author attended to two events in 2017: Cyber 9/12 Student Challenge (GCSP, 2017) and the EU Cyber Security Conference (EU2017EE, 2017). Thereby, hypothesis of the research has been not if, but rather *what* and *how many* issues there are.

Cyber 9/12 Student Challenge (GCSP, 2017), held in Geneva, 20-21 April 2017, is a competition where students around the world gather in teams of four to solve and respond on major, evolving cyberattacks by developing policy recommendations for “political leaders”. Even the competition deals with fictional cases, the incidents could realise in the real world. In fact, similar types of crises occurred after the competition: WannaCry and notPetya in 2017 which are further discussed subsections 3.3.2 and 3.3.3. The challenge showed how much effort cyber security cooperation and politics may demand to have effective response on tricky incidents, especially when cyber occasions in the real world may evolve exponentially in time and space. Responding to them can be difficult if exercises are not arranged and processes are not tested.

The EU Cyber Security Conference (EU2017EE, 2017), held in Tallinn, 14-15 September 2017, was an EU-level event where cyber security issues were discussed on many panels and speeches, including those related to cooperation. In the conference, it was brought out by many experts that the main issue for more profound cooperation relays on trust. It is about trust whom to share information and who are reliable enough not to leak anything. Other issues were discussed around what cyber security incident information should be shared as we are having more and more information, how they should be shared, on what level they should be shared, and what are the sanctions of not

---

<sup>9</sup> North Atlantic Treaty Organization.

sharing or should there be any, as well as what should be considered as essential services.

Therefore, the hypothesis of this research was that there are plenty of issues to solve to have a workable cyber security cooperation. The issues may require regulations and standardisation, but if working appropriately they may form a crucial tool for securing the digital single market, OES and DSPs of the EU.

## 1.8 Terminology and Clearance

This thesis includes plenty of basic cyber security terms and abbreviations. The list of abbreviations can be found from the beginning of the thesis. Also, the NIS Directive's own description of terms are in use. It can be found on appendix IV. Other relevant ones are explained and elaborated in this section.

The main terms of the research concern cyber security theme in high, strategic and governmental level. The main terms are (a) *essential services / critical infrastructure* that can be both public or private organisations as they are vital for European citizens, governments and companies to continue daily lives despite the security status. Not so often used but important term is (b) *Public-Private Partnership (PPP)* that correlates strongly with the NIS Directive requirements and is significant in improving European cyber security cooperation. The term (c) *European cooperation* used in this document concerns mainly public and private cooperation in the EU, which is found challenging as the EU (and the NIS Directive) consist of many different entities, various opinions and wills, where crucial cyber security information would need to be shared to have prosperous European cyber security cooperation. Additionally, (d) *cybersecurity* is a fundamental core term of the NIS Directive and the research as a whole.

Often used term, (e) *Member States*, throughout the thesis concerns the 28 member states of the EU. (f) *Competent authorities* are authorities that deal with cyber incidents and provide assistance. (g) *CSIRT* stands for Computer Security Incident Response Team, and (h) *CERT* for Computer Emergency Response Team. (i) *CSIRT network*, on the other hand, is a collaboratively discussing network formed of national CSIRTs, CERT-EU, ENISA and the Commission. (j) *Single point of contact* is a contact point nominated by a member state where contacts elsewhere can be provided, and it may provide the relevant information onwards.

## 1.9 Overview of the Chapters

This pro gradu thesis is divided into seven chapters: introduction, research methods, three body chapters, discussion and conclusions. A guideline

throughout the thesis is that the first chapter will introduce into the subject and scope of the research, second discusses of methods used in research process, the following three body chapters will answer individually to each sub-question, which will be followed by discursive chapter around the results, and finally the last chapter, conclusions, will compose the whole thesis answering to the main research question.

First, *introduction* initiates into the research topic. Introduction chapter presents the subject with its background, problem, short literature review and relevance in Computer Science scheme. It introduces the research questions and objectives, scope and hypothesis of the research. It also describes the main terminology of the research and clarifies what the terms are meant in this thesis, with addition of the structure of the whole thesis as what this section currently represents.

Second chapter, *research methods*, provides overview on research setting, used approach and design, strategy of inquiry, and evidence gathering process. In general, it discusses about how the research was conducted.

Third chapter elaborates *threats* and creates basis for the thesis guideline. Regarding to the chapter topic, it is important to understand what threats Member States of the EU are currently struggling against and what they might encounter in the future. It discusses around various attack types, for example from malwares, web-based attacks and spam to cyber espionage. Also, it explains with near history case examples of outcomes that may occur if cyber security is not considered thoroughly and prepared properly. Overall, after reading the second chapter there should be not a thorough but a basic picture of probable attack types and their consequences, and what the EU need to defend against currently and most likely in the future.

Fourth chapter discusses around *the NIS Directive*. The chapter explores the requirements of the Directive overall. The fundamental purpose of the chapter is to provide understanding of what the NIS Directive is essentially about and how the NIS Directive ought to improve European cyber security. Section 4.2 refers solely to the NIS Directive, without any other references. Section 4.3 provides elaboration of the NIS Directive. Consequently, the chapter explains what Member States have needed to prepare and build for in accordance with the Directive. It elaborates the demands and objectives of the Directive.

Fifth chapter enunciates already raised and probable *challenges* regarding to the EU cyber security cooperation in accordance with the NIS Directive. At the moment, there are 28 Member States in the EU (after Brexit in 2019, the number could lower down to 27 Member States) which means that there are different approaches onto the Directive. Cooperation is not an easy task to fulfil in wide, multi-cultural Europe where is as many currents as there are Member States, not forgetting private companies' approaches either. The chapter elaborates topics, such as trust, reporting, confidentiality and so forth. Chapter five provides a view on many challenges that there are in cooperation.

Chapter six, *discussion*, is the first part of two enclosing chapters. The chapter discusses of outcomes and provides thoughts by the author focusing on perspectives on the topic. It provides analysis of the current situation and probable outcomes for the future. It includes own views and “what-if” situations of the cyber security cooperation. Additionally, one section elaborates future research possibilities that this research could not take a stand on, or otherwise they were observed as notable areas to explore further.

Finally, chapter seven, *conclusions*, will enclose the thesis by providing main results of the whole research. Its purpose is to terminate the research with final thoughts. Basically, the last chapter summarise the thesis by answering to the main question.

## **1.10 Summary of the Chapter**

This chapter has provided an insight to the subject. It explained background of the research and stated the problem behind it. Literature review discussed of researches found closest to the topic, which was followed by an underline of the research significance. These formed a basic understanding for the research purpose.

Thereby, questions and objectives of the research were presented to provide understanding on what questions the research has aimed to look for answers. Scope of the research was described, including limitations that this research could have not taken into count. Before the research was begun, there was the certain type of hypothesis on background when conducting the research. Terminology and clearance were briefly clarified, which was followed by summary of the thesis chapters.

Next chapter explains how the research was executed. Research methods discuss of used techniques during the research, literally indicating what, when, where, how and why the research was done.

## 2 RESEARCH METHODS

### 2.1 Introduction

In this chapter, research methods used in the research are described. The chapter explains the research setting, approach and design, worldview, strategy of inquiry and evidence gathering process briefly. Basically, the chapter provides information on *what, when, where, how* and *why* the research was done as it was done to get research results presented later in this thesis.

### 2.2 Research Setting

As explained in the previous chapter, the main objective of this research was to fill the located gap in Computer Science regarding to cooperation in accordance with the NIS Directive. This means to understand what challenges there are around European cyber security cooperation, PPP and implementation of the NIS Directive. Based on them, the following sections will explain how the research was conducted and what methods were used to reach the set objectives. Before explanation of them, in this section we discuss how and when the research was begun.

Before beginning the research, the author had a certain hypothesis based on the events described in section 1.7. This was also supported by perception of other European pros and cons observed during previous politics and international relations studies. Obviously, the research aimed to look for whether this hypothesis would be accurate or not.

The research idea begun to form during 2017 with evidence gathering process. The process was continued in winter and spring 2018 where, simultaneously, a mini gradu thesis was written at late spring for a master seminar course required by the Faculty of Information Technology. The mini gradu formed a basis for chapter three of pro gradu thesis. Then, during

summer and autumn 2018 the thesis was written alongside daily work with some exception of vacation days sacrificed for academic purpose. A physical location throughout the process was in Helsinki, Finland.

### 2.3 Approach & Design

The research was approached and executed with a qualitative research design. The cyber security cooperation seemed complicated issue. Therefore, qualitative research design was chosen to serve the research objective. Also, there were documents of Member States, OES, DSPs, PPPs *et cetera* involved, so it seemed that qualitative design would ease to understand these occasions most appropriately:

The process of research involves emerging question and procedures, data typically collected in the participant's setting, data analysis inductively building from particulars to general themes, and the researcher making interpretations of the meaning of the data. ... Those who engage in this form of inquiry support a way of looking at research that honors an inductive style, a focus on individual meaning, and the importance of rendering the complexity of a situation. (Creswell, 2009, 4)

Some quantitative elements were involved when interesting, significant numbers were found useful but represent only minimal part of the research. However, qualitative research design was seen the most suitable from perspective of research conducting, research questions and expected results. (Creswell, 2009)

Chosen worldview for the research was a pragmatic worldview. When existing and intended cyber security cooperation is relatively complicated issue and the research questions were focused on 'what', rather than 'how many', pragmatic worldview was seen the most suitable. To achieve the best results within the research, pragmatism left space for researcher to freely choose what technique, procedure or method were used in each research situation. Pragmatism allowed to approach and analyse different subjects with multiple assumptions, with appropriate method for each case, not forgetting quantitative aspects either (Braun & Clarke, 2013). (Creswell, 2009)

### 2.4 Strategy of Inquiry

Strategy of inquiry for the thesis was a case study. When the research was focusing on different aspects of cyber security cooperation in the EU at the current state and probably in the future, case study was seen as the correct description. Also, a case study served the research objectives. Unlike other research strategies, a case study does not really offer a clear path to follow during the research execution which was a bit problematic to some extent (Yin,

2009). However, the desired strategy of inquiry was a case study in terms of the current environment of European cyber security cooperation. (Bell, 2010)

On purpose, there was no specific methodology chosen. Any fundamental theory was seen rather disturbing than assisting the research. Based on the research and its results, the most important part was, however, to provide new evidence and discussion to Computer Science.

## **2.5 Evidence Gathering**

Evidence gathering process was partly based on primary but mostly on secondary data. The primary data forms of statistical, table observations and represents only minority in this research. For example, expert interviews could have been a vital addition to have more in-depth analysis for the research results, but they were excluded due to time and resources. (Bryman, 2011)

The secondary data forms clear majority of the evidence. They consist of official documents provided by the EU, Cooperation Group and Member States, official documents offered by other organisations (for instance centres of excellence, cyber security companies, OES), mass-media outputs and magazines, including academic articles and online newspapers discussing about the cooperation or any other relevant regarding to the topic. Also, conferences, virtual documents, such as social media by experts were involved. Discussion forums and private websites were considered as option if they would have provided feasible and suitable evidence for scientific analysis, but they were excluded in the end. (Bryman, 2011)

## **2.6 Conclusion**

This chapter has explained what, when, where, how and why the research was executed. It provided research setting, research approach and design, strategy of inquiry, and evidence gathering process. Next chapter is the first body chapter of this thesis, presenting threats that Europe need to encounter in the comprehensive and alleged cyber space.

## 3 CYBER THREATS

### 3.1 Introduction

This chapter is divided into four sections: Introduction, top cyber-threats, recent major cyber incidents, and finally conclusions. Introduction elaborates the threat subject and shortly this chapter itself. The purpose of this chapter is to answer onto the first sub-question (What potential threats there are?) by providing overall view of threat landscape in Europe based on the recent results, especially during 2016 and 2017.

Section of top-cyber threats discuss around the current and emerging cyber-threats in Europe and beyond where discussion is based on 'ENISA (2018) threat landscape report 2017 - EU Law and Publications'. The ENISA report presents top 15 cyber threats that are mainly used as a guideline for introducing the threats. Sources used in exploring them are not only the report itself, but references are taken from other relevant origins as well.

Section of recent major cyber incidents discuss around recent threat landscape by providing examples of how security management has failed. The section aims to explore what drives various agents to conduct harmful cyber-attacks and what are their motives in doing so. Based on the examples of WannaCry, NotPetya and Equifax we aim to have understanding what threats the EU defend against currently and which threats could emerge in the future.














































Finally, conclusions wrap together this chapter. By reading the whole chapter, one should understand threats against the EU in general and objectives of the attacking side. As this chapter serves as a core element of the thesis, it provides a view on growing demand of abilities required in efficient European cyber security cooperation.



## 3.2 Top Cyber Threats

Cyber-space is ever increasing and modifying. Simultaneously, threat landscape is broadening in the same scale. This section discusses of top cyber-threats and its landscape. Fundamental document used to categorise the subsections and individual threat types is ENISA threat landscape report 2017 - EU Law and Publications (ENISA, 2018). When considering the EU and the NIS Directive especially, this arrangement has found the most appropriate when discussing of the NIS Directive more deeply in the next chapter. (ENISA, 2018)

The ENISA (2018) report discusses of 15 major threats that Member States are facing now and most likely in the future with indicative trend indicators. Also, other reports were considered during the thesis writing process to be used as a guideline, such as Internet Organised Crime Threat Assessment (Europol, 2018), Security Scorecard: The Nightmare of the Dark (Dennison et. al., 2018) on behalf of European Council on Foreign Relations, and The Cyber Threat to UK Business (NCSC & NCA, 2018). It appeared that generally rather similar topics were discussed in other reports, or their viewpoint was not suitable considering the thesis approach. However, the report by ENISA was seen the most suitable. The following table 1 illustrates the top 15 cyber-threats in the ENISA (2018) threat landscape report 2017.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware		1. Malware		
2. Web based attacks		2. Web based attacks		
3. Web application attacks		3. Web application attacks		
4. Denial of service		4. Phishing		
5. Botnets		5. Spam		
6. Phishing		6. Denial of service		
7. Spam		7. Ransomware		
8. Ransomware		8. Botnets		
9. Insider threat		9. Insider threat		
10. Physical manipulation/damage/theft/loss		10. Physical manipulation/damage/theft/loss		
11. Exploit kits		11. Data breaches		
12. Data breaches		12. Identity theft		
13. Identity theft		13. Information leakage		
14. Information leakage		14. Exploit kits		
15. Cyber espionage		15. Cyber espionage		







Legend: Trends:  Declining,  Stable,  Increasing  
Ranking:  Going up,  Same,  Going down

TABLE 1. Top threats in 2016 and 2017 with annual change indicator. (ENISA, 2018)

The following subsections introduce the above mentioned (table 1) top cyber-threats individually. The purpose of the subsections is neither to provide a full explanation of their usage nor include further technical details. Each topic could easily cover one pro gradu thesis on their own.

Therefore, the purpose of subsections underneath is to provide overall understanding and vital basic background information of the vast and evolving threat landscape. As the nature of this research (a pro gradu thesis instead of a broader PhD or similar), **the explanations hereinafter are rather superficial** compared to full analysis. Basically, they aim to explain briefly how they are used and why they form a threat to Europeans. The background information is vital for understanding discussions in further chapters around the NIS Directive requirements and difficulties in European cooperation.

### 3.2.1 Malware

Malware, which is a word combination of malicious software<sup>10</sup>, is any software that is designed with malicious intent. It includes a backdoor which allows access on software information without permission of the software user. Anything that the software does that it was not intended to do can be considered as a malware but, basically, malwares are often used, for example, on theft of private information, such as passwords or credit cards. (Fisher, 2018)

To infect a computer or other device with a malware, there are number of ways. Usually, a malware is installed by accident as an action of downloading and, without hesitation, installing a software which actual actions are overlooked by a user. Some infect a device with a safe-looking document, such as picture, audio or video, which could be, for instance, an email attachment and contains an executable program that installs and thereby harms the device. Others may take an advantage of security vulnerabilities, such as outdated versions of operating systems, browsers or their additional parts. Typical malware types are virus, worm, trojan horse, spyware, rootkit, malvertising and browser hijacker. (Fisher, 2018)

What comes to affecting on Europeans, the number of threats of malwares is the most frequent. Anti-Virus vendors have detected over four million samples per day in 2017 which of 0,2 % are detected as a mobile malware. Mobile malwares have shown a descending trend compared to results in 2016 but, simultaneously, their sophistication is on rise. Notably, there has been detections of diversification regarding to infection vectors. Top-known malwares in 2017 were WannaCry and NotPetya which were allegedly developed by a state intelligence agency. Malware had the most detections compared to other threats. Based on detections in 2017, ENISA classifies their trend as **stable** with slight decline. (ENISA, 2018)

### 3.2.2 Web-Based Attacks

Web based attacks are on second place in top cyber-threats list by ENISA (2018). A web-based attack is fundamentally based on a malicious code on a website that is visited by an oblivious user. Basically, there are three phases in a web-based attack anatomy. First, an attacker breaks into a legitimate website and infects it with a malicious code. Then, an unsuspecting user visits the website and the code is automatically downloaded on a user's computer without user even noticing it. Finally, once downloaded, a malicious code (for instance a virus) allows its author to remotely take control of the device and use it for infecting other devices or simply steal information. (Symantec, 2009)

Web based attacks can be part of websites but also within social media and mobile applications, and mostly they are well hidden. According to Verizon's 2016 Data Breach Investigation Report, number of web-based attacks

---

<sup>10</sup> Also known as *badware* or *computer contamination* in legal documents. (Fisher, 2018)

represented 50 % of data breaches during the year. Web based attacks were seen as **increasing** in 2017 (ENISA, 2018). (Sears, 2017)

### 3.2.3 Web Application Attacks

Web applications, such as mobile applications, web applications and other web services, are widely used due to their advantages for daily lives. Since their use is broad and plenty personal and financial details are handled in them, they have become a seductive target for hackers. Simultaneously, from security perspective, they include improper coding which, thereby, rise security concerns. These significant vulnerabilities are being exploited as web application attacks. (Acunetix, 2018)

Attackers may try to utilise databases because of the valuable information they hold. Vulnerabilities in web applications, sometimes due to human error or negligence, makes it relatively easy for hackers to gain access on residing data. It may need creativity and sometimes luck for a hacker but since security is not on appropriate level this is a relative threat. (Acunetix, 2018)

Famous technique in web application attacks is cross-site scripting (CSS) where hackers inject malicious code into a vulnerable web application and redirect users onto phishing sites. This technique is useful when database or web server themselves would not vulnerable. According to ENISA, web application attacks were seen **increasing** in 2017 (ENISA, 2018). (Acunetix, 2018)

### 3.2.4 Phishing

According to ENISA threat landscape report 2017, phishing is on fourth place with a rising trend compared to 2016 results with sixth place (ENISA, 2018). Basically, phishing is a cybercrime that targets genuine persons or services by luring them to provide valuable, confidential information or to click on something that will allow access for an attacker without a target knowing it. Usually, phishing is conducted through an email, but can also be a phone call or a text message, asking for certain details that may benefit an attacker. An email may include an attachment, which upon opening, installs a malicious code without knowledge of a user, or a link directing a user to a familiar looking website where login details or financial information, such as credit card information, are asked to input. (CERT-UK, 2015)

More sophisticated version of this type of an attack is called spear phishing. Spear phishing targets specific persons or organisations that may trick employees to believe that information is received from known sources. For example, a common type of spear phishing is an email sent by a resembling high-ranking member of a targeted organisation requesting a rapid payment to a particular bank account. Attackers may also be interested into information that organisations process. It may be valuable for stealing and selling or simply having access for spying on it. The trend of phishing is reported as **increasing** in 2017 (ENISA, 2018). (CERT-UK, 2015)

### 3.2.5 Spam

The definition of spam<sup>11</sup> is, according to Kaspersky Lab (2018), is anonymous unsolicited bulk email which of word anonymous they describe as following: “real spam is sent with spoofed or harvested sender addresses to conceal the actual sender”. The word bulk considers that mails are sent in enormous amounts, mass mailing, where larger the number is more responses may be received because statistically only small percentage of receivers actually respond on spam mails. Mails can be both legitimate or spam depending on whether a receiver has opted to receive the mail or not, so unsolicited refers to newsletters, mailing lists and other materiel sent to receivers that can be wanted or unwanted, which of unwanted often is the case when discussing about spam.

Spam can be divided into unsolicited commercial email (UCE) consisting commercial content and unsolicited bulk email (UBE) without any commercial information. Some of spam messages are advertising, include commercial services or goods but not all. They do not define spam as such only as commercial messages. Kaspersky Lab (2018) state that there are typically five categories that non-commercial UBEs may drift into. These are political mails, chain letters, fake spam spreading malwares, quasi-charity appeals or financial scams. The trend of spam is seen **increasing** in 2017 (ENISA, 2018). (Kaspersky Lab, 2018)

### 3.2.6 Denial of Service

A denial of service (DoS) attack, or Distributed Denial of Service (DDoS) attack if done from multiple computers, aims to make a service, network or machine inaccessible to its intended users. Victims of DoS attacks are typically media, banks, commerce services, governmental or trading organisations. When their web servers are being targeted the regular users, such as customers, employees, or other account holders may not access daily services which, in the comprehensive world, are evermore significant for functionality of societies and business. The DoS attacks usually do not result to loss of information or other assets. Instead, victim organisations of the DoS attacks embrace great harm, especially in terms of time and money, to overcome the situation. (Palo Alto Networks, 2018)

---

<sup>11</sup> Spam is an acronym, originating from the combination of words ‘spiced’ and ‘ham’, first used in 1937 of out-of-date minced sausage sold unsuccessfully by Hormel Food Corporation in the USA which, after a major campaign, resulted to a tinned meat product contract with Army and Navy (and are still on sale). Later in 1970, spam was used in Monty Python’s Flying Circus sketch and in George Orwell’s book ‘1984’ spam was described as disgusting but inevitable. With a first reference to undesired bulk messages spam was used in 1993 when Richard Dephew accidentally spread dozens of recursive messages in early internet communication system, Usenet. In 1994, spam was stabilised as a term when Canter & Siegel law firm posted the first large scale commercial spam in Usenet. (Kaspersky Lab, 2018)

Palo Alto Networks (2018) name two general methods for a DoS attack: flooding and crashing services. Basically, flooding causes too much traffic for a receiving server to buffer. When the attack continues, it first slower down the intended service and, eventually, the requests cannot be handled anymore and the server crash down. Thereby, it becomes unavailable for its users. There are three types of favoured flood attacks. (1) Buffer overflow attack is based on sending too much traffic on a network address for it to process. (2) Leveraging misconfigured network with ICMP (Internet Control Message Protocol) flood<sup>12</sup> that overloads not only one computer but the whole targeted network with spoofed data packets. (3) SYN (synchronise) flood which uses TCP (Transmission Control Protocol) three-way-handshake by sending constantly connecting requests to a server. The server responds with ACK (acknowledge) but the attacker never completes the handshake with ACK and thus floods the server. Other DoS attacks exploit vulnerabilities. They cause the target service or system to crash. “In these attacks, input is sent that takes advantage of bugs in the target that subsequently crash or severely destabilize the system” (Palo Alto Networks, 2018) Thereby, it cannot be used or accessed. In 2017, the overall trend of denial of service was **increasing** (ENISA, 2018).

### 3.2.7 Ransomware

Basically, a ransomware is a malware that encrypts files and folders, prevents users from accessing their system or the files and then begin to demand for ransoms to regain access. Typically, payment is expected to be conducted via a cryptocurrency or with credit card. (Malwarebytes, 2018) Ideally, as an exchange for the payment the victim is supposed to receive a decryption key to unlock encrypted system or files, but this is not always the case. It is up to cybercriminals whether they decide to share the decryption key or not. (Levin & Simpson, 2018a)

Most ransoms begin with two typical types. A common one is an email attachment that attempts to install a ransomware. Other usual type is exploit kits hosted by certain websites: To install a ransomware, exploit kits endeavour to utilise vulnerabilities of internet browsers and other software. After ransomware has infected a computer or other device, it begins to encrypt system or parts of it, such as individual files, folders, or even entire partitions of hard drive depending on the type of ransomware. Algorithms used for encryption may be, for instance, RSA<sup>13</sup> or RC4<sup>14</sup>. (Levin & Simpson, 2018a)

There are three main types of ransomware. The type mentioned in the previous paragraph is encrypting ransomware which, as explained, encrypt files or system. To gain decryption key and redeliver encrypted part, one must pay. This type is dangerous since there is no such system restore or security software that could recalculate the encryption to return encrypted part. Other

---

<sup>12</sup> Also known as ping flood. (Palo Alto Networks, 2018)

<sup>13</sup> Rivest-Shamir-Adleman.

<sup>14</sup> Rivest Cipher 4.

two are scareware and screen lockers. Scareware aims to scare user with a rogue software and technical support scams but is basically harmless. One may notice a pop-up message claiming of malware existence and resolving it with payment. Though, files are essentially safe. Screen lockers, on the other hand, locks a PC entirely. They will show a full-size window upon starting up computer and often claim with official looking national authority statement that the user has done some illegal activities of which fine must be paid. Authorities in such cases use appropriate legal channels, not locking anyone's computer. (Malwarebytes, 2018)

For cybercriminals, ransomware is one of the most profitable revenue channels. It is very likely that we see increasingly sophisticated ransoms that target enterprises. This trend will put older and not updated platforms susceptible to ransomware attacks, which of WannaCry and NotPetya during 2017 are worth to mention (discussed further in section 3.3). When this has become so lucrative it has created a new business model, ransomware-as-a-service, which may involve many sharing parties from creators to operators. No wonder if ENISA has observed the trend of ransoms **increasing** in 2017 (ENISA, 2018). All these are occurring at the expense of citizens of the EU and Digital Single Market. (Levin & Simpson, 2018a)

### 3.2.8 Botnets

Botnet (a shortened version of robot network) is a network of compromised computers. Compromised botnet computers are infected with malicious code that can be remotely controlled and used for multiple, often dubious purposes. These purposes may vary: Botnet can be used for concomitant DDoS attacks to block internet traffic at victim servers, gather of information, spread malicious code, such as viruses, or for distributing spam. As not all criminals are experts in computing, cyber-space enables renting botnets for the described purposes also for the DDoSaaS mentioned sub-section 2.2.6. Consequently, botnets are used for criminal purposes in terms of deception, disturbance and extortion. The activity of botnets was observed as **increasing** in 2017 (ENISA, 2018). (Alexander, 2012)

### 3.2.9 Insider Threat

Insider threat is not a new issue which of governments and companies around the globe have suffered for a long time. (ENISA, 2018) Insider threat means that an individual or group of an organisation allow, unwittingly or in purpose, unauthorized access into confidential information by leaking valuable business or national security information. Thereby, the action may cause major damage in terms of economic, capability, resource or reputational losses, unauthorized disclosure, espionage, or terrorism. (ODNI, 2013)

According 2016 Cyber Security Intelligence Index by IBM, 60 % of all attacks were carried out by insiders and within that number three-quarter

involved malicious intent (van Zadelhoff, 2016). During the current age of easily accessible, ever growing amount of information, insiders remain a constant threat as the activity is hard to distinguish from benign activity. No wonder when some organisations form guidelines to deal with insider threats, such as the U.S. Insider Threat Security Classification Guide (ODNI, 2013). However, the overall trend of insider threat remained **stable** in 2017. (ENISA, 2018)

### 3.2.10 Physical Manipulation / Damage / Theft / Loss

Even though physical manipulation / damage / theft / loss is not always a technical or cyber threat *per se* it still may have major impact on various types of digital assets and is therefore relevant to be included into the list. (ENISA, 2018)

According to Trend-Micro (2017), in 2015, “the likeliest breach method was through device loss or theft” (Trend-Micro, 2017, 16). Though, it has lowered down in statistics ever since. Malwares and hacking have overcome as the top cause of data breaches in early 2017.

Also results of Verizon (2018) supports this view. Companies losing devices remain considerably high positioned, as Verizon remind that not all data theft occur via online sources. Equally important is to predict criminals from stealing sensitive material or tampering systems by having appropriate entry controlling systems and surveillance cameras for restricted areas. According to ENISA the trend of physical manipulation / damage / theft / loss was observed as **stable** with a slight increase in 2017 (ENISA,2018).

### 3.2.11 Data Breaches

A data breach is not a cyber threat itself. Instead, it could be considered as a collective term of successfully triggered cyberthreats where data has been either accessed or stolen by unauthorised attacker. Defending against data breaches is becoming harder when they are formed of ever more complex phenomena. Besides current, there are new and evolving threats where constant vigilance in regards of incident response plans updating is required. (Olavsrud, 2017)

According to Experian (2017) there are five major topics within data breaches. Experian state that (1) passwords are getting nearer to extinction when, despite years old data breaches, same stolen usernames and passwords are still sold in dark web. This occurs because people tend to use the same login details in different environments.

Experian (2017) predicted that (2) nation-state cyber-attacks escalate from cyber-attack level to cyber-warfare, from espionage to war. These are due to when attacks involve into politics as state-sponsored cyber-attacks on the U.S. presidential campaign in 2016. Thus, critical infrastructure, business world and large number of customers are left as a collateral damage.

According to Experian (2017) (3) new, sophisticated attacks on healthcare were predicted on rise when personal healthcare information, especially



electronic healthcare records, are great value for attackers. Experian state that most likely these were about to be combined with ransomware when they are safe and easy way to cash out as many organisations are willing to pay the ransom. Also, (4) payment-based attacks, such as ransom attacks, are not the one to ignore either when there have been indications that cyber criminals may turn towards them.

Additionally, Experian (2017) have stated that (5) international data breaches will cause major difficulties for multinational companies if their incident response plans are not well in place. New regulations, such as the GDPR (or similar new laws in other countries), require informing of data breaches to data subjects and to supervisory authorities within 72 hours which may be relatively hard to comply.

Conclusively, we may state that the forecast by Experian (2017) for year 2017 actualised dramatically well. For example, Equifax (Gressin, 2017) data breach occurred as discussed further in subsections 3.2.12 and 3.3.4, as well as access preventing ransomwares WannaCry (Sherr, 2017; discussed further in subsection 3.3.2) and notPetya (Newman, 2017; discussed further in subsection 3.3.3) actualised. Therefore, it is not surprising that in 2017, the overall trend of data breaches was **increasing** (ENISA, 2018).

### 3.2.12 Identity Theft

Identity theft usually involves identity fraud. They are referred to crimes where stolen personal data are wrongfully used for deception or fraud. Identity theft is not a new issue, but cyber space has enabled identity thefts in new means. Typically, identity theft unfolds for such purpose where the obtained data can be economically gained. Such cases could be fraudulent bank account withdrawals, false loan or credit card applications, use of online accounts or telephone cards, acquiring goods, or obtaining such privileges that the criminal himself would be denied by using real name. (U.S. Department of Justice, 2018)

Many types of confidential information may be abused to impersonate the original owner of the data. The information could consist contact data, including identifiable names or addresses; credentials, financial data, health data or even computer system data, including logs. Identity theft is strongly related to data breaches, as discussed in subsection 3.2.11, but it is a special case of data breaches, targeting identity information. (ENISA, 2018)

There are number of ways for fraudsters to acquire personal information. Achievable means are hacking, social engineering, exploiting from social media, shopping from dark web, and so forth. (Samee, 2017) For example, credit card information on dark web is probable to acquire from 10-20 dollars. Other highly detailed personal data range from 10 dollars. (ENISA, 2018)

Identity theft can be profitable for attackers and this will likely guarantee continuous attempts of identity thefts in the future. Simultaneously, there are companies that do not take care of their networks properly. The worst data breach of personal information of all time has been the breach of consumer

credit reporting agency, Equifax, as discussed further in subsection 3.3.4 (Gressin, 2017). Additionally, there are users around Europe that are not aware enough of the threats that identity theft could cause. Due high activity, the trend of identity theft was observed **increasing** in 2017. (ENISA, 2018)

### 3.2.13 Information Leakage

Information leakage is typically caused by an unwilling action or failure by someone inside the organisation, unlike insider threat with purposely intentions as discussed in subsection 3.2.9. According 2016 Cyber Security Intelligence Index by IBM, one-quarter involved inadvertent actors out of all attacks caused by insiders (van Zadelhoff, 2016). Primary types of information leakage are resulted of trusted but unwitting human error which represent a major factor in leakages; but can also occur based on false identity by cyber criminals. (van Zadelhoff, 2016)

Information leakage can occur on many levels, such as password or document leakage. In application level, on the other hand, this could be caused by one or more of the following: “a failure to scrub out HTML/script comments containing sensitive information; improper application or server configurations; or differences in page responses for valid *versus* invalid data” (White Hat Security, 2018). At the worst, information leakage may cause significant economical, reputational harm or loss of confidential information, such as personal data, depending on number and value of information leaked. (van Zadelhoff, 2016)

Information leakage is a common and often misunderstood risk. It impacts many organisations constantly without their own knowledge of the situation. As number of devices begin to grow it may be difficult for security managers to track all of them. According to ENISA, the trend of information leakage was observed **increasing** in 2017 (ENISA, 2018). (Walker, 2018)

### 3.2.14 Exploit Kits

Exploit kits are a specific type of malware that exploit vulnerabilities and infect a device by bypassing security safeguards of a computer. Exploit kits utilise vulnerabilities in software to gain access to a device. (Levin & Simpson, 2018b)

Exploit kits scan for outdated systems having critical vulnerabilities and to infect devices and infiltrate organisations they aim to deploy targeted malware into the vulnerabilities often with so-called “shellcode” which is a small payload of malware. Exploit kits take advantage of multiple software types, such as Adobe Reader, Adobe Flash Player, Java-based applications, and web browsers. Exploits kits can be distributed with emails, but more frequently they are deployed through web sites as the following figure illustrates. (Levin & Simpson, 2018b)

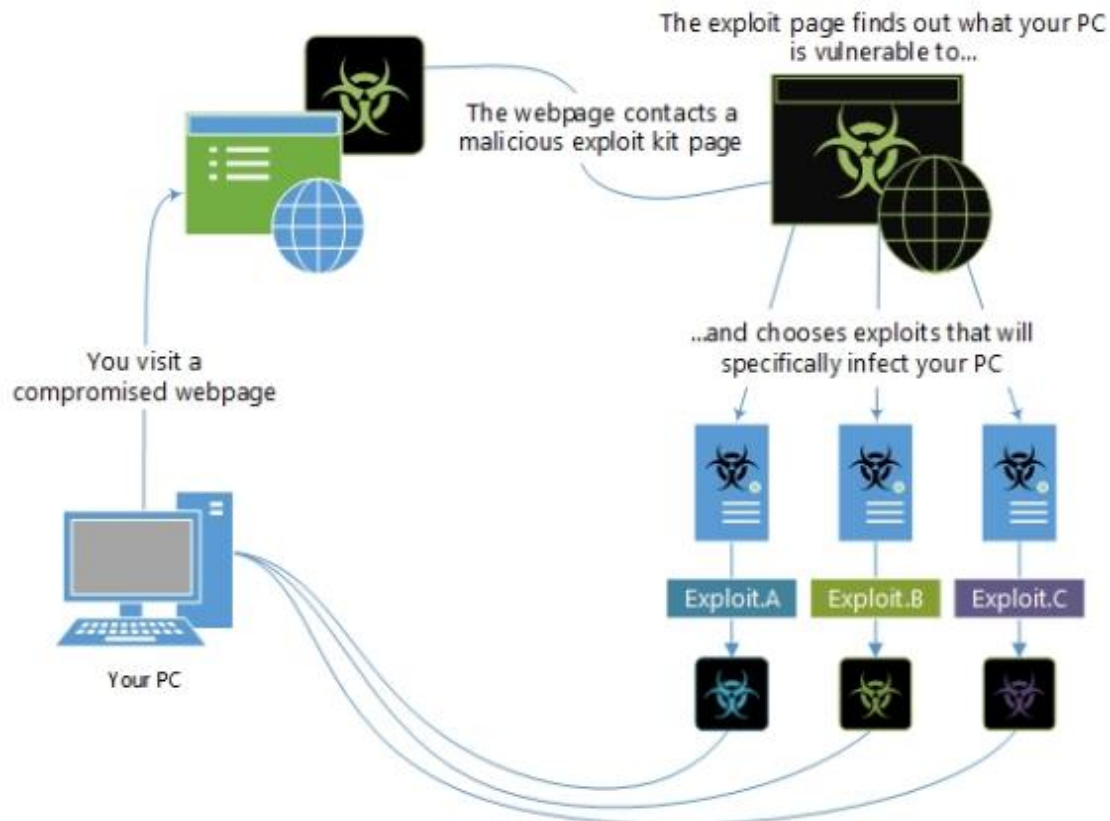


FIGURE 1. Exploit kit workability example. (Levin & Simpson, 2018b)

The above-mentioned type of infiltrating exploit kits is typical. Some web pages host ads containing malicious code and exploits. This may be without knowing and willing of the website owner. (Levin & Simpson, 2018b)

The best way to prevent exploits and defend against exploit kits is to keep software updated as software vendors provide updates for prominent vulnerabilities (Levin & Simpson, 2018b). According to ENISA (2018), it appears that the trend of exploit kits has been **decreasing** in 2017.

### 3.2.15 Cyber Espionage

Cyber espionage is an ever-growing matter in cyber space. As modern societies are transferring data in networks, including classified and sensitive data, networks have enabled new possibilities for intelligence organisations to gather information with less risks of getting caught (Alton, 2018). Simultaneously, means to gather information have evolved and are getting more advanced, including APTs (Advanced Persistent Threat) which in the threat landscape report (ENISA, 2018, 87) is described as “APTs represent a collection of processes, tools and resources used by certain groups in order to covertly infiltrate specific networks, remain stealthy in the systems over a long period of time, and exfiltrate data or perform other destructive actions.” The problem concerns both, governments and companies. They concern in Europe and beyond, especially in the USA. (ENISA, 2018)

Notably, according to Finnish Security Intelligence Service (SUPO) report released in early 2018, the activity in networks still has not decreased threat of traditional espionage where old ways are equally in use. Foreign intelligence organisations, especially Russia, are trying to recruit local nationals to provide non-public information, and also aiming to gather information about foreign and security policy, cyber security infrastructure, counter-combat abilities of information operations, and drafting of an upcoming intelligence legislation. (YLE, 2018)

Espionage does not end on European borders. They need to be considered also when Europeans travel abroad. Member States have begun to warn their citizens about traveling with mobile devices. For example, Dutch Foreign Ministry is suggesting having 'empty' devices when travelling to China, Iran, Turkey and Russia (Schaake, 2018). Also, French officials are providing guidelines of internet use and traveling abroad (ANSSI, 2014). The trend of cyber espionage was observed as **increasing** in 2017 (ENISA, 2018).

### 3.3 Recent Major Cyber Incidents

#### 3.3.1 Threat Landscape Overview and Threat Actor Motives

According to European Political Strategy Centre (2017) cyber-attacks on critical infrastructure, data breaches, cyber espionage, as well as mass disinformation campaigns are no longer futuristic threats. Cyber events and incidents affect businesses in all sectors, governments across Europe and individual citizens in the present state daily. Cyber aggression, whether conducted by individual script kiddies, insider threat, organised crime or state-sponsored actors, is a major new vector that must be understood to be able to defend the EU. The vector can be activated to "achieve strategic superiority, destabilise states, and cause large-scale economic damage" (European Political Strategy Centre, 2017, 1). Thereby, it is no wonder that year 2016 is claimed as a turning point in offensive use of cyber power as media reported a new record in number of data breaches, and the US formally claimed that Russia had supported interference on US presidential election (Khafir, 2017).

Motives behind the attacks may vary. Though, it is essential to understand them to have proactive defence. According to Recorded Future website (RFSID, 2016), threat actor types can be generally divided into four main categories: cyber criminals, hacktivists, state-sponsored attackers and insider threats. (1) Cyber criminals, whether organised or otherwise, are driven by economical gain. They could have a targeted attack and, usually, they attack if they can profit. Main objective of (2) hacktivists is to undermine reputation or destabilise operations, for instance, with a DDoS. Instead of motivated with money, typically, vandalism is their preferred attack mean. (3) State-sponsored attackers are not usually interested in money and they are far less common than

cybercrime and hacktivism. State-sponsored attacks are especially concentrated on information, they might last a long period of time, and the attackers are hard to identify which require high maturity in security. (4) Insider threat types may vary and they may cause major harm as discussed in subsection 3.2.9. Some are normal employees unwittingly providing information to wrong hands, others malign their organisation, but gradually more insider threats occur because of real user accounts compromised by external attackers. However, this is one way to divide motivators. As illustrated in the following figure, motivators can also be arranged based on their target selection.



FIGURE 2. Threat actors divided into six categories. The order is made based on their usual target selection. (RFSID, 2017)

The main thing is to understand that there are various types of threat actors with different motives in the threat landscape.

When the threat landscape in cyber space continuously evolves and accelerates the threats simply cannot be set aside if the Digital Single Market is desired to be defended and maintained resilient. The EU need to anticipate and plan countermeasures against unimaginable scenarios which desperately require cooperation within the EU. Consequently, the EU must comprehend the latest threats and improve cooperation to prepare against future threats. (European Political Strategy Centre, 2017)

By having a view on recent incidents, we understand why new policies and partnerships are needed. There is neither an industry nor a member state of the EU that could be spared of severity of cyber-attacks. The following figure illustrates a small selection of incidents only in 2016.

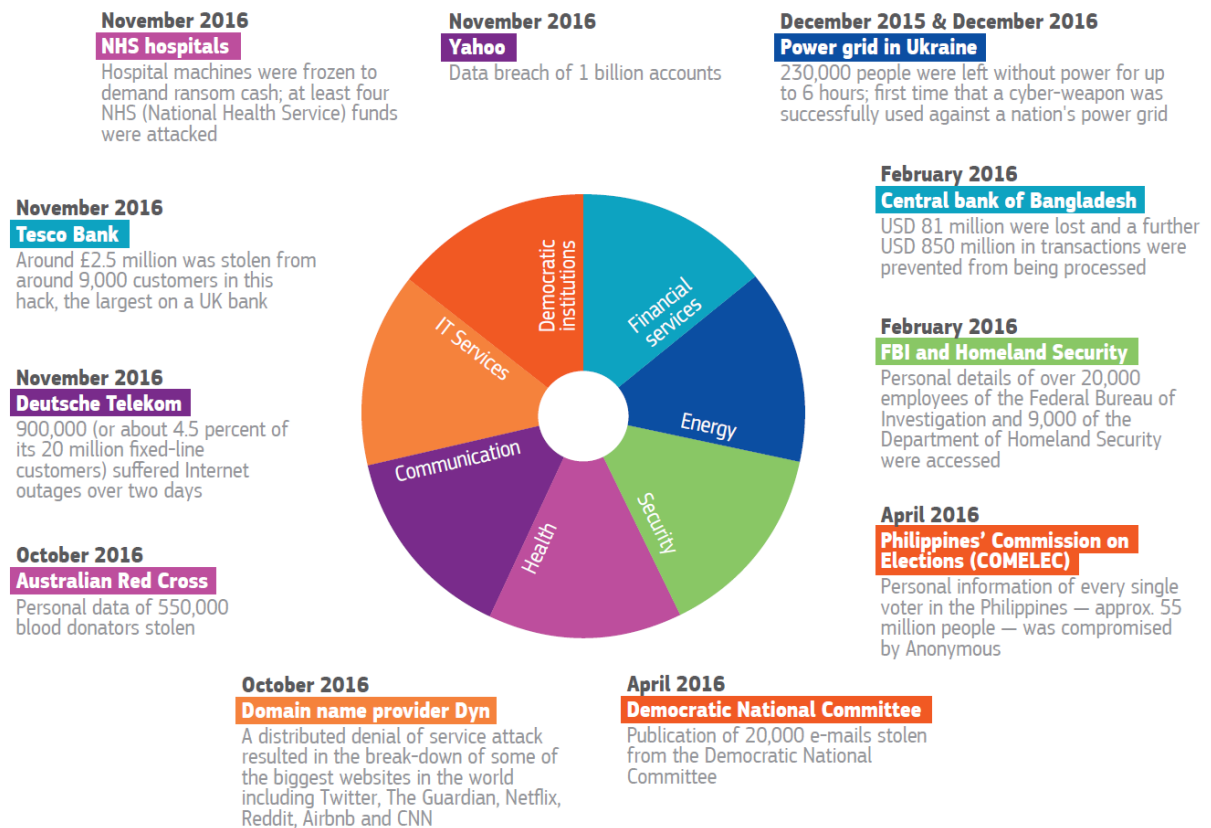


FIGURE 3. A small selection of cyber incidents throughout the world in 2016. As it can be observed of the figure, there are many areas that are hit by cyber attacks. (European Political Strategy Centre, 2017)

To effectively defend against such threats and prepare for the worst, institutional collaboration across the EU is required. Threats are becoming more complex and their intense grows. Not only appropriate policies but practicality to enhance competence sharing, that is driven by the NIS Directive requirements as discussed in chapter four, are unquestionably needed. Member States must have major priority on cyber security. (European Political Strategy Centre, 2017)

Likewise, year 2017 was the time of underpinning the increasing trend. There were very effective and broad incidents that had not observed before. The following subsections provide examples of them.

### 3.3.2 WannaCry Ransomware

WannaCry<sup>15</sup> was a ransomware that hit hard between 12-15 May 2017. It was targeted on outdated Windows XP platforms. In fact, the vulnerability of the system was originally discovered by the American National Security Agency (NSA) which held it as a potential surveillance tool, but ever since the information was stolen from them. In March 2017, when knowing the vulnerability Microsoft released a protective software update, but not many did

<sup>15</sup> Also known as Wcry and WannaCrypt. (Hunt, 2017)



update their computers. Thus, underlining the need for constant updates against such vulnerabilities, as an outcome, many companies and industries where the update was not made became vulnerable on the attack. It spread through standard file sharing technology called Microsoft Windows Server Message Block (SMB). It appeared that there was no way to resolve the situation on encrypted and locked computer of WannaCry. (Sherr, 2017)



FIGURE 4. Screenshot of WannaCry infected device. (Hunt, 2017)

WannaCry was made for financial gain. Though, due to poor implementation attackers were not able to profit as intended: Majority of victims of WannaCry found that even ransoms were paid the ransomware was not decrypted. In successful ransomware campaigns victims are made to believe that by paying ransoms the decryption key will be received. (NCSC & NCA, 2018)

However, WannaCry attack crippled computers in at least 150 countries. (Berr, 2017) The figure underneath illustrates that the EU was not spared by the attack either:

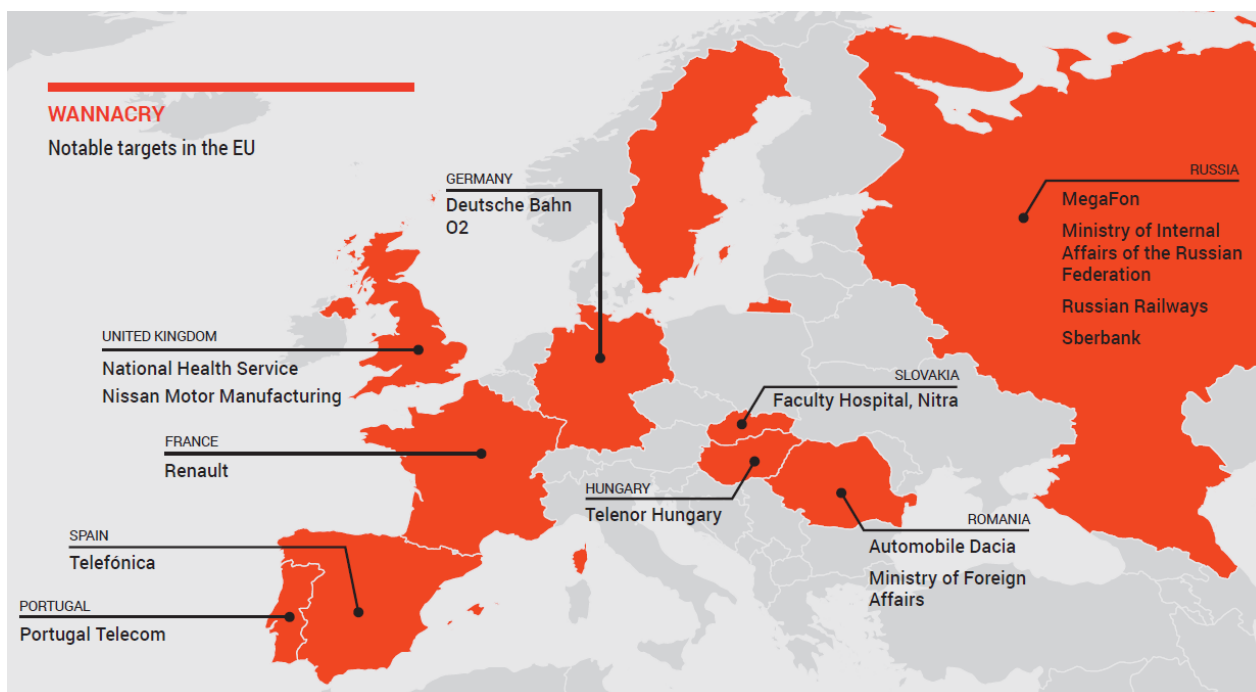


FIGURE 5. Notable targets of WannaCry in the EU. (Europol, 2018)

Cyber risk modelling company, Cyence, has estimated that WannaCry may have caused potential costs up to 4 billion dollars. Other companies have estimated the attack causing hundreds of millions of losses. Certainly, WannaCry is one of the most damaging ransomware based cyber incident by far. (Berr, 2017)

### 3.3.3 NotPetya Malware

NotPetya<sup>16</sup> was followed soon after WannaCry on 27 June 2017. NotPetya utilised the same SMB exploit as in the outbreak of WannaCry. Though, NotPetya was relevantly more advanced than WannaCry but still had some flaws, including inefficient and ineffective payment system (Newman, 2017). NotPetya modified the Master Boot Record (MBR) at a low level: It made a computer to reboot, presented a faux Check Disk operation while it actually was encrypting files. The MBR was overwritten to display the following ransom note:

<sup>16</sup> Variously known as PetrWrap, ExPetr, GoldenEye and NotPetya. (NCSC & NCA, 2018)



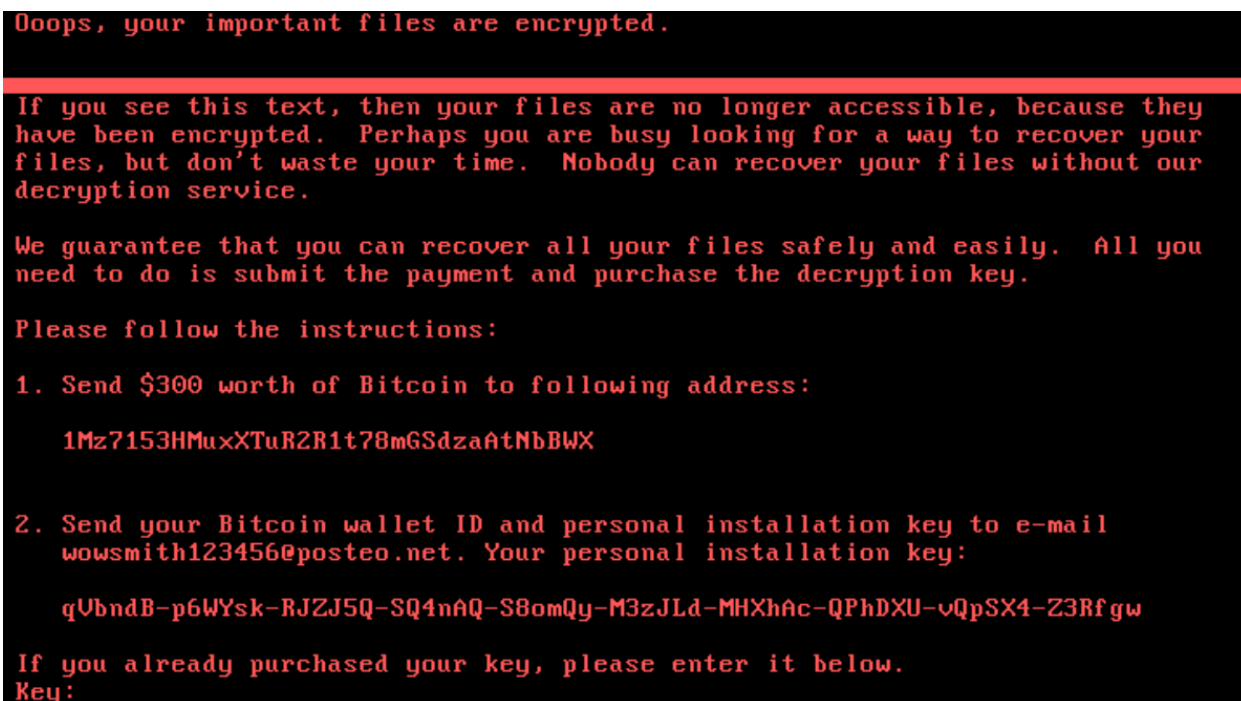


FIGURE 6. Screenshot of NotPetya infected device. (Malwarebytes Labs, 2017a)

It appeared that NotPetya was targeted against businesses and companies specialised in software development. File types being targeted were somewhat that developers use, such as .vbox, .vbs, .ova and so forth. (Malwarebytes Labs, 2017a)

It is commonly believed that NotPetya was targeted against Ukrainian companies and organisations because Ukrainian infrastructure got hit particularly hard. The ransomware disrupted power companies, the central bank, public transit and airports being the latest in a series of cyber-attacks against the country. (Newman, 2017) While NotPetya was spreading around the country, at the same time, international companies doing business with Ukraine got infected, including Danish shipping company Moller-Maersk, US pharmaceutical company Merck, British confectionary company Cadbury, Russian oil company Rosnoft and US courier delivery service FedEx. Because of the attack, Moller-Maersk on their own, reported having loss of revenue worth of 350 million euros. (NCSC & NCA, 2018) All in all, as all the victims indicate, it appears that NotPetya attack was particularly targeted on critical infrastructure, especially in Ukraine but apparently infecting other related countries as well.

### 3.3.4 Equifax Data Breach

Throughout the years, there have been other notable data breaches, but Equifax data breach was exceptionally severe which is the reason why it was chosen here as an example. The data breach of Equifax, a consumer credit reporting agency, was revealed on 7 September 2017. It is the worst data breach of stolen personal information by far impacting on 145,5 million consumers. (Leary, 2018)

Compromised sensitive consumer information may have included: full names, social security numbers, birth dates, addresses and driver's license numbers. Also, it is reported to that credit card numbers of 209 000 people and "dispute documents with personal identifiable information" concerning 182 000 people were compromised (Gressin, 2017).

Most of the Equifax data breach concerned American customers, but also data of approximately 400 000 UK customers were stolen (BBC, 2017). This emphasises that in similar cases in the future, even the company would operate outside the EU they would need to follow the NIS Directive requirements if any Europeans are concerned in the breach. This is more elaborated in section 4.2.

### 3.3.5 Future Threats and Developments

Europol (2018) (together with EC3, European Cybercrime Centre) estimate that ransoms will continue to flourish as they are profitable way for cybercriminals to earn. Ransoms will become more available and accessible in a few years when, for example, as-a-service business models and affiliate programmes will be taken into repertory by all cybercriminals. Europol predicts that crypto mining could gradually overtake ransomware making it a future threat. Risk *versus* reward advantages crypto mining, whereas at the same time crypto currencies are becoming more valuable.

Europol (2018) states that mobile malware may grow. Online banking model seem to be changing towards mobile banking which will form mobile devices more attractive threat targets. In financial sector, trojans will remain a key concern and sophisticated cybercriminals may target more on payment systems, such as SWIFT<sup>17</sup> network. In a five years term, fileless attacks will become a regular part of the crime-as-a-service industry, as well as both cybercriminals and technology advance making them even harder to detect.

Europol (2018) predicts that other financial frauds may rise. When instant payments are becoming more popular they may reduce possibilities for detection intervention by banks. Europol argues that when PSD 2<sup>18</sup> came into force in January 2018, it may allow additional forms and new opportunities for cybercriminals when PSD 2 grants third party access to payments accounts in order to follow the permission of consumers.

It is very likely that terrorist groups will evermore be involved into cyber space when internet is propitious soil for sharing their ideology. Alongside, there is much concern and speculation of terrorist groups launching cyber-attacks against critical infrastructure. A critical infrastructure focused cyber security report by German officials<sup>19</sup> states that well targeted attacks against

---

<sup>17</sup> Society for Worldwide Interbank Financial Telecommunication.

<sup>18</sup> Second Payment Services Directive.

<sup>19</sup> National Cyber Response Centre (Nationales Cyber Abwehrzentrum, NCA), The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI), and The Domestic Intelligence Service of the Federal Republic of Germany (Bundesamt für Verfassungsschutz, BfV), The Federal Intelligence Service

major German electricity providers by hackers could black out electricity network in whole Europe when German companies produce electricity to several EU Member States (Saraste, 2018). Meanwhile tools and techniques of terrorists lack of sufficient expertise, their focus could be on DDoS attacks and crypto mining. Additionally, there are concerns raised of developing West Africa where social engineering scams by organised crime groups (OCG) have steadily been growing. High unemployment rates combined with more technically advanced attackers, and environment where fraudster tactics are openly shared, the growing trend within the OCGs will most likely continue. (Europol, 2018)

### 3.4 Conclusions

There are plenty of threats in cyber space that concern not only Europe but whole globe, especially Western societies. Considerably, the threat list by ENISA is having only 15 main threats and there could be even more threat types to be considered. Threats need to be taken seriously in the modern world and when processing European cyber security cooperation further.

Top three threat types, malwares, web-based attacks and web application attacks form great major threat since they are widely and increasingly more used. DoS and DDoS attacks, botnets and spam, on the other hand, form medium threat. Quite surprisingly, cyber espionage is “only” on fifteenth place.

Whether perpetrators are cyber criminals, hackers, state-sponsored attackers, insider-threats, they all can cause significant harm in cyber space despite motives behind them. Targets may vary but often critical infrastructure or digital service providers are under attack. As Europol state, even though WannaCry, NotPetya and Bad Rabbit<sup>20</sup> attacks in 2017 were not necessarily directly targeted towards critical infrastructure they made many critical infrastructure victims, especially in health, transport and telecommunications sectors (Europol, 2018).

It is very likely that data breaches, such as Equifax, will continue to exist. So do efforts by cybercriminals with ransomware, crypto mining, and attacks on mobile banking or financial services. Terrorist groups and Western Africa OCGs form their own type of attack vectors that must be considered in defending European OES and DSPs, as well as citizens of Europe. Simultaneously, technology and expertise of perpetrators continue to grow. At the worst, attacks could black-out the whole Europe.

---

(Bundesnachrichtendienst, BND). The report made by the officials contains assessments of cyber threats against critical infrastructure, including electricity, gas and water supply, as well as traffic control. (Saraste, 2018)

<sup>20</sup> Ransomware using a fake Flash update and, thus, dropping its payload. Most likely created by the same authors as NotPetya. (Malwarebytes Labs, 2017b)

The threats certainly effect on the Digital Single Market as a whole. Companies and Member States may lose information throughout non-vigilant employees, suffer of leakages and cyber espionage, or have their networks encrypted. Also, individuals are under attack, knowingly or unknowingly. These require constant education and vigilance since they would be the best solution to tackle the issues. It could be considered as an important progress that Member States are warning and enlightening their citizens. Notably, when the attacks do not end on European borders every European citizen should be aware of the threats while being in or outside of Europe.

In conclusion, what is notable that majority of the ENISA (2018) threat trend indicators of 2017 compared to 2016 show increasing appearance. Out of 15 threats described, 11 are reported increasing, 3 stable and only 1 is decreasing. The indicators could enunciate that cyber security threats at least do not ease in the future. Therefore, the NIS Directive and European cooperation in cyber security are more needed than ever. Although, as mentioned, the cooperation may not be easy. In the best-case scenario, it would be extremely valuable for Member States, companies and citizens to confront future issues in cyber space and beyond.

## **4 REQUIREMENTS AND ELABORATION OF THE NIS DIRECTIVE**

### **4.1 Introduction**

This chapter discuss around the NIS Directive itself. The purpose of this chapter is to answer onto the second sub-question (What are the EU's objectives of the NIS Directive?) by providing view on the Directive details and elaborate its requirements from perspective of different entities.

The chapter is divided into four sections. This first section introduces the chapter. In second section, the NIS Directive is explored on article by article basis. Second section is divided into subsections in accordance with the chapters and annexes of the Directive. Third section explains the objectives of the NIS Directive. It also elaborates cooperation on national and European level. Finally, there is a conclusive chapter in the end.

### **4.2 Requirements of the NIS Directive**

This section explores the NIS Directive. The section is divided into subsections by the NIS Directive's chapters and annexes explaining their articles. The purpose of this chapter is to provide a basic knowledge of what the NIS Directive consists. What is notable is that this exploration does not consist some exceptions and limitations referenced in the Directive, and recitals in the beginning of the NIS Directive are left out of scope.

#### **4.2.1 General Provisions**

The NIS Directive (European Union, 2016a) chapter I, articles 1-6, provide general provisions. Topics of articles in chapter I discusses around subject matter and scope, processing of personal data, minimum harmonisation,

definitions, identification of operators of essential services, and significant disruptive effect.

Article 1 (European Union, 2016a), *subject matter and scope*, defines the objective, the scope and the subject for the NIS Directive. Article 1 sets demands for Member States to secure and improve the functioning of the internal market concerning the whole Union. The Directive sets the following general requirements, as stated in point two of article 1 (bolds made by the author):

- (a) “lays down obligations for all Member States to adopt a **national strategy** on the security of network and information systems;
- (b) creates a **Cooperation Group** in order to support and facilitate strategic cooperation and the exchange of information among Member States and to develop trust and confidence amongst them;
- (c) creates a computer security incident response teams network (**‘CSIRTs network’**) in order to contribute to the development of trust and confidence between Member States and to promote swift and effective operational cooperation;
- (d) establishes **security and notification requirements** for operators of essential services and for digital service providers;
- (e) lays down obligations for Member States to **designate national competent authorities, single points of contact and CSIRTs** with tasks related to the security of network and information systems.” (European Union, 2016a, 11-12)

Confidential national and business information are considered exchangeable only in such cases where it is seen necessary for the application of the NIS Directive. Such confidential information exchange needs to protect security and commercial interests of all stakeholders. The Directive allows Member States, without prejudice, to safeguard from disclosure such confidential information that is essential for State functions, national security, or maintaining law and order, including matters regarding to criminal offence.

Article 2 (European Union, 2016a) handles *processing of personal data*. Personal data will need to be carried out in accordance with Directive 95/46/EC as stated in article 2. Though, such directive is no longer in force and is repealed by the GDPR<sup>21</sup> (European Union, 2016b). Article 3 (European Union, 2016a), *minimum harmonisation*, defines that Member States may, without prejudice, achieve higher level of security of network and information systems than the NIS Directive *per se* requires. Article 4 (European Union, 2016a) includes *definitions* for the terms used in the NIS Directive. In this thesis, full list of definitions and their descriptions can be found from Appendix IV.

Article 5 (European Union, 2016a), *identification of operators of essential services*, defines that Member States are required to identify and nominate their OES of each industry sector and their subsectors (details: Appendix II) by 9 November 2018. These lists Member States will need to review and update every two years. Identification criteria for the OES are described in point two of article 5 as:

---

<sup>21</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. (European Union, 2016b)

- (a) “an entity provides a service which is essential for the maintenance of critical societal and/or economic activities;
- (b) the provision of that service depends on network and information systems; and
- (c) an incident would have significant disruptive effects on the provision of that service.” (European Union, 2016a, 14)

This, rather broad identification criteria set a basis for Member States’ lists of nomination. Role for the Cooperation Group has been to support Member States in the process of identification of OES. The arrangement has aimed to have a consistent approach for the process. Additionally, besides creating the list, article 5 obligates Member States to define national measures for the identification of the OES, inform the number of the OES, indicate how important they are in relation to the specific sector, and determine thresholds where they exist.

Article 6 (European Union, 2016a) focus on determining *significant disruptive effect*. It obligates Member States to take into account at least the following cross-sectoral factors as stated in the article point one of article 6 (bolds and footnote made by the author):

- (a) “the **number of users** relying on the service provided by the entity concerned;
- (b) the **dependency of other sectors** referred to in Annex II<sup>22</sup> on the service provided by that entity;
- (c) the **impact** that incidents could have, in terms of degree and duration, on economic and societal activities or public safety;
- (d) the **market share** of that entity;
- (e) the **geographic spread** with regard to the area that could be affected by an incident;
- (f) the **importance of the entity** for maintaining a sufficient level of the service, taking into account the availability of alternative means for the provision of that service.” (European Union, 2016a, 15)

Besides the list above, Member States are obligated to consider sector-specific factors when determining a significant disruptive effect, if appropriate.

#### 4.2.2 National Frameworks on the Security of Network and Information Systems

The NIS Directive (European Union, 2016a) chapter II, articles 7-10, regulate on the security of network and information systems (NIS) regarding to national frameworks. Topics of articles in chapter II discusses around national strategy on the security of NIS, national competent authorities and single point of contact, computer security incident response teams (CSIRT), and cooperation at national level.

Article 7 (European Union, 2016a), *national strategy on the security of network and information systems*, sets requirements for each Member State to

---

<sup>22</sup> Appendix II in this thesis.

adopt a national strategy on the security of NIS. According to article 7, the national strategy on the security of NIS must define “the strategic objectives and appropriate policy and regulatory measures with a view to achieving and maintaining a high level of security of NIS” (European Union, 2016a, 15). At least sectors of OES and DSPs, referred in appendix II and III in this thesis, must be covered in the national NIS security strategy. Point one of article 7 defines that the following issues are to be addressed in the national strategy on the security of NIS (bolds made by the author):

- (a) “the **objectives and priorities** of the national strategy on the security of network and information systems;
- (b) a **governance framework to achieve the objectives and priorities** of the national strategy on the security of network and information systems, including roles and responsibilities of the government bodies and the other relevant actors;
- (c) the identification of measures relating to **preparedness, response and recovery**, including **cooperation between the public and private sectors**;
- (d) an indication of the **education, awareness-raising and training programmes** relating to the national strategy on the security of network and information systems;
- (e) an indication of the **research and development plans** relating to the national strategy on the security of network and information systems;
- (f) a **risk assessment plan** to identify risks;
- (g) a **list** of the various **actors involved in the implementation** of the national strategy on the security of network and information systems.” (European Union, 2016a, 15-16)

For developing such strategy, ENISA is appointed as the first point instance of assistance. Additionally, Member States are required to communicate their national NIS security strategy to the EC within three months of the adoption which of sensitive national security elements may be excluded.

Article 8 (European Union, 2016a), *national competent authorities and single point of contact*, demands Member States to designate one or more competent authorities for monitoring of industries and one single point of contact for liaison purposes. If there is only one competent authority it will also serve as a single point of contact. Nominated competent authority or authorities are required to cover areas of OES and DSPs mentioned in appendix II and III in this thesis. They may be new or already existing ones and their responsibility is to monitor the application of the NIS Directive. The single point of contact, on the other hand, is responsible of ensuring information exchange with (1) other Member State authorities regarding to European wide cross-border cooperation, (2) Cooperation Group and (3) CSIRT network (these are further discussed in subsection 4.3.3). Likewise, a national single point of contact may be new or already existing one. However, all the designated entities are made public. According to article 8, they are regulated to have “adequate resources” (European Union, 2016a, 16) to comply their tasks, not forgetting “effective, efficient and secure cooperation” (European Union, 2016a, 16) in the Cooperation Group, and they must, when appropriate, cooperate with national data protection authorities and other national law enforcement entities. If any of



these change Member States must inform the Commission about new designations.

Article 9 (European Union, 2016a), *computer security incident response teams (CSIRTs)*, regulates about national CSIRTs: Each Member State is required to have one or more CSIRTs that is responsible for risk and incident handling based on a proper process. Requirements for the CSIRTs are more broadly presented in appendix I and related responsible areas in appendix II and III in this thesis. Basically, as stated in article 9, this means that national CSIRTs need to “comply with the requirements” (European Union, 2016a, 17) on point one in appendix I, and have “adequate resources” (European Union, 2016a, 17) presented on point two in appendix I. On national level, Member States must guarantee for their CSIRTs an access to “an appropriate, secure, and resilient communication and information infrastructure” (European Union, 2016a, 17) as CSIRTs are required to cover all relevant NIS sectors and services mentioned in appendix II and III. Regarding to CSIRTs in the European CSIRT network, Member States must ensure “the effective, efficient and secure cooperation<sup>23</sup>” (European Union, 2016a, 17). In developing national CSIRTs, the ENISA is appointed to assist by Member State request basis, and Member States are yet to address CSIRT incident handling processes to the EC. All in all, these leave space for Member States to define their own national approach regarding to the CSIRTs.

Article 10 (European Union, 2016a), *cooperation at national level*, defines basics of how national cooperation in Member States should be arranged to fulfil the obligations of the NIS Directive. Article 10 requires “the competent authority, the single point of contact and the CSIRT” (European Union, 2016a, 10) in an individual Member State to cooperate if they are separated. Incident notifications must be submitted either to competent authorities or to CSIRTs. In a Member State where CSIRT is not a primary receiver of such notifications CSIRT must be granted access to the incident data (provided by OES or DSPs) in order to fulfil its tasks. However, incident notifications must also be informed to the single point of contacts. Additionally, single point of contact is required to submit an annual summary report<sup>24</sup> to the Cooperation Group about “the notifications received, including the number of notifications and the nature of notified incidents, and the actions taken” (European Union, 2016a, 17). Two points of article 10, the CSIRT tasks and summary report, are referred to demands of the OES and DSPs which will be discussed further in subsections 4.3.4 and 4.3.5.

### 4.2.3 Cooperation

Chapter III (European Union, 2016a), articles 11-13, regulate about the Cooperation Group, CSIRT network and international cooperation. As other

---

<sup>23</sup> Cooperation further presented in subsection 4.3.3.

<sup>24</sup> Begun from 9 August 2018. (European Union, 2016a)

subsections in section 4.2 are generally good to recognise, this subsection – and the chapter of the NIS Directive – is rather one of the core parts of this thesis.

The Cooperation Group is for strategic level having biennial terms whereas CSIRT network is set out for operational usage. International cooperation, on the other hand, considers external elements, outside of the EU. Since this thesis focus on challenges of the NIS Directive based European Cooperation, special attention should be given to this subsection.

Article 11 (European Union, 2016a), *Cooperation Group*, deals with European strategic approach on the NIS Directive and execution of its cooperative information sharing element in practise. The article establishes the Cooperation Group and states that it is formed of representatives of Member States, the Commission and ENISA with addition of relevant stakeholders where appropriate. Besides strategic cooperation facilitation and information exchange, its purpose is to achieve EU wide “high common level of security of NIS” (European Union, 2016a, 17) and “develop trust and confidence” (European Union, 2016a, 17) among Member States. Point three of article 11 indicates the following thirteen tasks for the Cooperation Group (bolds made by the author):

- (a) “providing **strategic guidance** for the activities of the CSIRTs network established under Article 12;
- (b) **exchanging best practice** on the exchange of information related to **incident notification** as referred to in Article 14(3) and (5) and Article 16(3) and (6);
- (c) **exchanging best practice** between Member States and, in collaboration with ENISA, assisting Member States in **building capacity** to ensure the security of network and information systems;
- (d) **discussing capabilities and preparedness** of the Member States, and, on a voluntary basis, **evaluating national strategies** on the security of network and information systems and the effectiveness of CSIRTs, and identifying best practice;
- (e) exchanging information and best practice on **awareness-raising and training**;
- (f) exchanging information and best practice on **research and development** relating to the security of network and information systems;
- (g) where relevant, **exchanging experiences** on matters concerning the security of network and information systems with relevant Union institutions, bodies, offices and agencies;
- (h) **discussing the standards and specifications** referred to in Article 19 with representatives from the relevant European standardisation organisations;
- (i) **collecting best practice information on risks and incidents**;
- (j) **examining**, on an annual basis, **the summary reports** referred to in the second subparagraph of Article 10(3);
- (k) **discussing** the work undertaken with regard to **exercises** relating to the security of network and information systems, **education programmes** and **training**, including the work done by ENISA;
- (l) with ENISA's assistance, **exchanging best practice** with regard to the identification of operators of essential services by the Member States, including in relation to **cross-border dependencies**, regarding risks and incidents;
- (m) **discussing modalities** for reporting notifications of incidents as referred to in Articles 14 and 16.” (European Union, 2016a, 18)

Based on the list mentioned above, the Cooperation Group is ought to establish biennial work programme<sup>25</sup> which will include executable objectives and tasks in consistency with objectives of the NIS Directive itself. Also, the functionality and gained experiences of these strategic performs are evaluated every year and a half which of a report will be made. The review of this kind is discussed further in on subsection 4.3.7 (article 23).

Article 12 (European Union, 2016a), *CSIRT network*, focus on determining CSIRT network stipulations. The first point of the article could be considered rather vivid:

“In order to contribute to the development of confidence and trust between the Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is hereby established.” (European Union, 2016a, 19)

This is continued by defining roles within the CSIRT network: The core part is formed by representatives of CSIRTs of Member States and CERT-EU. Additionally, ENISA provides the secretariat and active support for the CSIRT network cooperation whereas the Commission participates as an observer. Rules of procedure of CSIRT network are to be regulated by the CSIRT network themselves. Point three of article 12 underlines the following tasks for the CSIRT network (bolds made by the author):

- (a) “**exchanging information** on CSIRTs' services, operations and cooperation capabilities;
- (b) **at the request** of a representative of a CSIRT from a Member State potentially affected by an incident, **exchanging and discussing non-commercially sensitive information** related to that incident and associated risks; however, any Member State's CSIRT **may refuse** to contribute to that discussion if there is a risk of prejudice to the investigation of the incident;
- (c) **exchanging and making available on a voluntary basis** non-confidential information concerning individual incidents;
- (d) **at the request** of a representative of a Member State's CSIRT, discussing and, where possible, **identifying a coordinated response** to an incident that has been identified within the jurisdiction of that same Member State;
- (e) providing Member States with support in addressing cross-border incidents on the basis of their voluntary mutual assistance;
- (f) **discussing, exploring and identifying** further forms of operational cooperation, including in relation to:
  - (i) categories of risks and incidents;
  - (ii) early warnings;
  - (iii) mutual assistance;
  - (iv) principles and modalities for coordination, when Member States respond to cross-border risks and incidents;
- (g) **informing the Cooperation Group of its activities** and of the further forms of operational cooperation discussed pursuant to point (f), and requesting guidance in that regard;

---

<sup>25</sup> Begun from 9 February 2018. (European Union, 2016a)

- (h) **discussing lessons learnt** from exercises relating to the security of network and information systems, including from those organised by ENISA;
- (i) **at the request** of an individual CSIRT, **discussing the capabilities and preparedness** of that CSIRT;
- (j) **issuing guidelines** in order to facilitate the convergence of operational practices with regard to the application of the provisions of this Article concerning operational cooperation.” (European Union, 2016a, 19)

Likewise, as the Cooperation Group, also CSIRT network is obligated to be reviewed every year and a half their experiences in a form of report. The report must include “conclusions and recommendations” (European Union, 2016a, 19) of the conducts made in accordance with the NIS Directive.

Article 13 (European Union, 2016a), *international cooperation*, is very brief. It enables opportunity for international cooperation by stating that international agreements may be concluded with third countries or international organisations referring to Article 218 of Treaty on the Functioning of the European Union (European Union, 2012). When adequate protection of data is guaranteed external parties may participate in some of the activities conducted by the Cooperation Group.

#### 4.2.4 Security of the Network and Information Systems of Operators of Essential Services

Chapter IV (European Union, 2016a), articles 14-15, are appointed on the OES. It is separated on two articles which establish: security requirements and incident notification, as well as implementation and enforcement. Interestingly, Member States are responsible for the OES security implementations in their area.

Article 14 (European Union, 2016a) discusses around *security requirements and incident notification*. The first two points of the article demands the OES on risk management and proper resilience. Member States must ensure the OES, operating in their country, to have “appropriate and proportionate technical and organisational measures” (European Union, 2016a, 20) on uprising threats and their risk management. Prevention of impacts and minimising them are expected to be appropriately executed with addition of such resilience that continuity of NIS used by the OES is ensured. On third point, Member States are required to overlook that the OES notify the competent authority or CSIRT without undue delay of “incidents having a significant impact on the continuity” (European Union, 2016a, 20) regarding to the service provided by the OES. Evaluation of any cross-border impact of the incident must be included to the notification. Fourth point of article 14 underlines parameters for evaluating significance of an impact (bolds made by the author):

- (a) “the **number of users affected** by the disruption of the essential service;
- (b) the **duration** of the incident;
- (c) the **geographical spread** with regard to the area affected by the incident.” (European Union, 2016a, 20)

Further points in the article concern notifications. When the competent authority or CSIRT has received the notification, it is required to inform other affected Member States, if the impact is significant for their OES. The single point of contact of sending and receiving Member State shall transfer information among each other if requested by the competent authority or CSIRT. Security, confidentiality and commercial interests should be considered in such case. The competent authority or CSIRT should provide any sort of assistance for the OES notifier that could help it to overcome the situation. The competent authority or CSIRT may also release a public announcement of the incident but prior-consulting of the notifier should be conducted and a necessity for public awareness should be evaluated before the announcement.

Article 15 (European Union, 2016a), *implementation and enforcement*, sets obligations to the competent authorities to assess and overlook compliance on security of NIS of OES. Member States must enable that the competent authorities have “the necessary powers and means” (European Union, 2016a, 21) for the assessments and, as stated in point two of article 15, require the OES to provide:

- (a) “the information necessary to assess the security of their network and information systems, including documented security policies;
- (b) evidence of the effective implementation of security policies, such as the results of a security audit carried out by the competent authority or a qualified auditor and, in the latter case, to make the results thereof, including the underlying evidence, available to the competent authority.” (European Union, 2016a, 21)

Hereby, the competent authorities may request specified and justified additional information about the compliance and, thus, conclusively obligate the OES to achieve higher level of security by remedying the identified deficiencies.

#### **4.2.5 Security of the Network and Information Systems of Digital Service Providers**

Chapter V (European Union, 2016a), articles 16-18, are regulating about the DSPs similarly to the OES. There are articles handling security requirements and incident notification, implementation and enforcement, but also jurisdiction and territoriality that is not included on chapter regarding to the OES.

Article 16 (European Union, 2016a), *security requirements and incident notification*, discusses about minimum standards of security and how incidents should be informed throughout the Union. Member States are obligated to ensure that the DSPs, operating in their country, will have “appropriate and proportionate technical and organisational measures” (European Union, 2016a, 21) on uprising threats and risk management of threats. While overlooking the level of security of NIS, the DSPs must also take into consideration the elements listed underneath:

- (a) “the security of systems and facilities;
- (b) incident handling;
- (c) business continuity management;
- (d) monitoring, auditing and testing;
- (e) compliance with international standards.” (European Union, 2016a, 21)

The article is continued by demands of having processes for prevention and minimising of impacts in place as well as guarantee continuity of provided services. Without undue delay, the DSP must inform the competent authority or CSIRT of “any incident having a substantial impact on the provision of a service” (European Union, 2016a, 22) and this notification should include information about evaluation of cross-border impact significance. Member States must monitor these activities to occur. Similarly to the OES, as stated in point four of article 16, DSPs are obligated to evaluate significance of an impact based on (bolds made by author):

- (a) “the **number of users** affected by the incident, in particular users relying on the service for the provision of their own services;
- (b) the **duration** of the incident;
- (c) the **geographical spread** with regard to the area affected by the incident;
- (d) the **extent** of the disruption of the **functioning** of the service;
- (e) the **extent** of the impact on **economic and societal** activities.” (European Union, 2016a, 22)

Notably, the last two of the list are additional compared to the OES. However, if a DSP is providing as a third-party such service that an OES with critical societal or economical activities relies on, the DSP operator must notify about the continuity of the service. Additionally, chapter V articles does not apply to micro and small enterprises.

Article 17 (European Union, 2016a), *implementation and enforcement*, requires that Member States follow up on the competent authorities to act on DSPs that do not meet article 16 requirements. If necessary for such action, it will be conducted through ex post supervisory measure basis and may be done by any Member State competent authority where the DSP operates. For such actions, competent authorities must have the necessary powers and means. As on point two of article 17, competent authorities may require the DSPs to:

- (a) “provide the information necessary to assess the security of their network and information systems, including documented security policies;
- (b) remedy any failure to meet the requirements laid down in Article 16.” (European Union, 2016a, 23)

If above mentioned actions require cross-border collaboration regarding to the main establishment and a representative, concerned competent authorities may be involved and conduct information exchange.

Article 18 (European Union, 2016a), *jurisdiction and territoriality*, defines basis of them in accordance with the NIS Directive. Only the DSPs are having this type of article. Article 18 defines that where the main establishment of an

individual DSP is located, the DSP will be under jurisdiction of that Member State. Where the main office is located, there the main establishment is interpreted to be located. If the DSPs do not have the main establishment in the Union but still offer digital services (see Appendix III) within the EU, the DSP must nominate a representative into one of those countries where the DSP operates and follow their jurisdiction.

#### 4.2.6 Standardisation and Voluntary Notification

Chapter VI (European Union, 2016a), articles 19-20, could be seen as clarifying additional articles for Member States. Article 19, *standardisation*, refers to the first two points of articles 14 and 16 which have defined security requirements and need for incident notifications by the OES and the DSPs. Article 19 encourages Member States to use European or internationally accepted standards and specifications relevant to NIS security. Also, existing standards, such as Member States' own could be used if they are sufficient. In technical definitions and guidelines, ENISA may assist Member States. Also, Member States are obligated not to impose or discriminate in favour any particular type of technology usage.

Article 20 (European Union, 2016a), *voluntary notification*, allows organisations, that are not recognised as an OES or a DSP, to voluntarily provide notifications regarding to their services that are under a significant impact and thus lacks continuity. Member States are obligated to process voluntary notifications in accordance with article 14 process that highlights the number of users, the duration and the geographical spread as well as requires informing other Member States and CSIRTs in worse cases. Interestingly, the last paragraph states that inordinate obligations on the notifying entity shall not be placed if it would have not given the voluntary notification.

#### 4.2.7 Final Provisions

Chapter VII (European Union, 2016a), articles 21-27, include final clarifications for the Directive. Articles determine provisions regarding to penalties, committee procedure, review, transitional measures, transposition, entry into force and addressees. The articles within chapter VII are relatively disambiguate and concise.

Article 21 (European Union, 2016a), *penalties*, requires Member States to ensure the Directive is being implemented and to regulate "the rules on penalties applicable to infringements of national provisions adopted pursuant" (European Union, 2016a, 24) to the NIS Directive. The penalties must be "effective, proportionate and dissuasive" (European Union, 2016a, 24) and must had been notified to the Commission by 9 May 2018. Article 22 (European Union, 2016a), *committee procedure*, defines that the Commission will be assisted by the Network and Information Systems Security Committee.

Article 23 (European Union, 2016a), *review*, sets two deadlines for the NIS Directive and its implementation. The Commission must deliver a report about Member States' consistency in the identification of the OES to the EP and to the Council by 9 May 2019. Second deadline is set on 9 May 2021 when the Commission must deliver, to the same recipients, the first verse of periodical review of functioning of the NIS Directive. Reports by the Cooperation Group and the CSIRT network at strategic and operational level must be considered.

Article 24 (European Union, 2016a), *transitional measures*, defines cooperative and supportive elements regarding to the NIS Directive transition. By 9 February 2018, the Cooperation Group and the CSIRTs network had to begin their tasks, including prior-nomination of Member States onto the regarded positions. From that day to 9 November 2018, the Cooperation Group has been obligated to follow the consistency of identification of the OES throughout the EU with addition of assisting Member States in national measures if they request.

Article 25 (European Union, 2016a), *transposition*, required Member States to adopt and publish nationally the laws, regulations and administrative provisions set in the NIS Directive by 9 May 2018 which thereby applied from 10 May 2018 and should have been communicated to the Commission.

The last two articles are one sentence long. Article 26 (European Union, 2016a), *entry into force*, simply states that the Directive was entered into force on the twentieth day since its publication in the Official Journal of the EU. Article 27 (European Union, 2016a), *addressees*, appoints the Directive to Member States. Finally, the Directive ends on signatures by president Martin Schulz on behalf of the European Parliament and president Ivan Korčok on behalf of Council of the European Union, dated in Strasbourg, 6 July 2016.

#### **4.2.8 Annexes I-III**

The last part of the NIS Directive (European Union, 2016a) consists of its three annexes (appendix I-III in this thesis). Annex I (European Union, 2016a) handle CSIRT requirements, titled as "Requirements and Tasks of Computer Security Incident Response Teams (CSIRTs)".

Annex II (European Union, 2016a) defines Operators of Essential Services by sector and subsector basis, titled as "Types of Entities for the Purposes of Point (4) Of Article 4". Annex III (European Union, 2016a) defines types of Digital Service Provides with three short bullets, titled as "Types of Digital Services for the Purposes of Point (5) of Article 4". For further information of the NIS Directive Annexes I-III, see appendix I-III in this thesis.



### **4.3 Elaboration of the NIS Directive**

This section generally elaborates the articles and requirements of the NIS Directive that were presented in the previous section. The objective of this section is to make the overall picture clearer with illustrative figures. Thus, one should have better understanding the demands and probable difficulties that several institutions and their interdependencies could create regarding cooperation.

#### **4.3.1 Objectives and Scope**

The NIS Directive is the main piece of legislation of the EU Cyber Security Strategy (European Commission, 2013). The main objective of the NIS Directive is to ensure a high common level NIS security across the EU. It particularly requires OES and DSPs to have appropriate abilities to manage security as well as they are required to report serious incidents. The incident reporting is to be done to the national competent authorities. (Bickerstaff et. al., 2016)

The high common level of security is ought to find out with collaborative cooperation and information sharing (further discussed in subsection 4.3.3). The key behind all of this is that each Member State must have a national strategy that guidelines to coherent cyber security. Each Member State must safeguard their main NIS and have an overall view on NIS resilience improvements. Member States observe and insist minimum level of security in their area. They do not have to have all system operators in their scope but those providing essential services and a limited number of DSPs. Member States must also observe those that are either based in their country or the ones that have business in one or more Member States. The above-mentioned elements under the NIS Directive must cooperate both nationally and across borders (see figure 7 underneath). Fundamentally, the idea is to prevent any major disaster scenario. The NIS Directive requirements aim to avoid such to occur, or at least contain and minimise consequences. (Surguy, 2017)

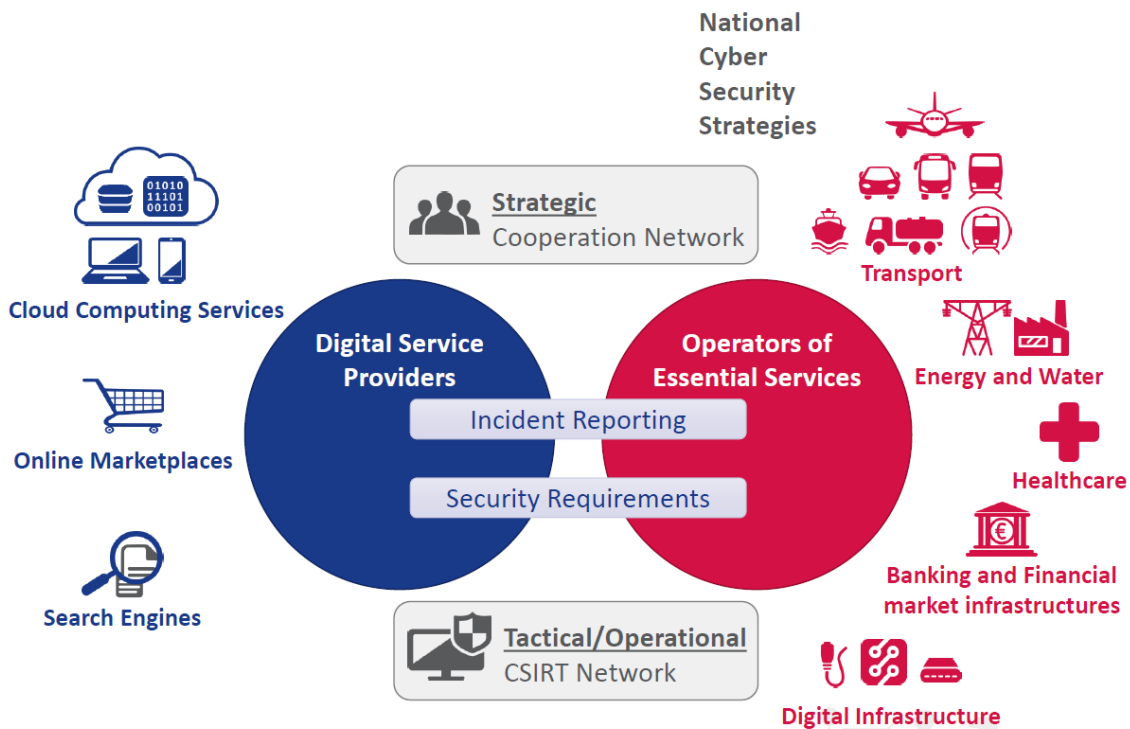


FIGURE 7. The main areas and sectors of the NIS Directive requirements. (Purser, 2016)

The OES are those operators that are nominated by Member States by 9 November 2018 in the OES sectors. As indicated in figure 7 and in appendix II, the OES sectors and their subsectors are

- energy: electricity, oil, gas,
- transport: air transport, rail transport, water transport, road transport,
- banking,
- financial market infrastructures,
- health sector: healthcare settings, including hospitals and private clinics,
- drinking water supply and distributions, and
- digital infrastructure,

which must take steps to minimise and prevent incident impacts on their NIS. They should put efforts on guaranteeing continuity of the services to avoid major loss, any significant disruption to supply chains or significant economic damage. (European Union, 2016a)

DSPs are having similar but less onerous requirements. In fact, at one stage during development process of the NIS Directive, DSPs were about to be excluded from the scope when risk degree for DSP could be less. They were taken into scope when it was realised that DSPs are significant to some businesses, and some OES may rely on DSPs. (Surguy, 2017) Though, like discussed in subsection 4.2.5, micro and small enterprises are out scoped of the DSP definition. As indicated in figure 7 and in appendix III, the DSPs include

- online marketplace,
- online search engine, and
- cloud computing service,

which must minimise and prevent incident impacts on their services. (European Union, 2016a) There are same kind of “high-level parameters for determining whether an incident is ‘substantial’ and setting out issues that digital service providers should consider when considering what security measures to implement” (Evans & White, 2016). Although, instead of Member States imposing any other notification or security requirements on their own, for harmonisation purposes, the Commission expands the criteria and definitions. (Evans & White, 2016)

Regarding to figure 7, when it appears that an incident will cross borders of Member States, the incident details are required to be shared to other Member States. CSIRTs and competent authorities are the entities to conduct such information sharing. CSIRT network operates on tactical and operational level, whereas Cooperation Network is for strategic purposes (Purser, 2016). (Evans & White, 2016)

#### 4.3.2 Cooperation on National and European Level

Information sharing and cooperation are to be considered as the core parts of the NIS Directive. To have effective cooperation, it must work on all levels and sectors. Practically, this means having efficient PPP, coherent work between OES, DSPs and national authorities as well as to other Member States and the EU institutions. (European Union, 2016a)

Cooperation on national level is executed between the following entities: OES, DSPs, voluntary notifiers, law enforcement agencies, CSIRT(s), national competent authorities, and single point of contact. Both, OES<sup>26</sup> and DSPs<sup>27</sup>, are responsible for their risk management and incident reporting. Others, not belonging to either of the categories, may report voluntarily<sup>28</sup>. For reporting, OES must evaluate above mentioned<sup>29</sup> impact significance parameters: (1) the number of users affected, (2) the duration of the incident, and (3) the geographical spread. DSPs must also evaluate<sup>30</sup>: (4) the extent of the disruption of the service, and (5) the impact on economic and societal activities. Based on the NIS Directive, there is no exact time limit for incident reporting. They must be made without undue delay. Though, it is recommended that CSIRT network exchange detailed technical information and analysis about anomalies, such as IP addresses and indicators of compromise, and they should be delivered to ENISA within 24 hours of notifying the anomaly activity (European

---

<sup>26</sup> NISD article 14, subsection 4.2.4. (European Union, 2016a)

<sup>27</sup> NISD article 16, subsection 4.2.5. (European Union, 2016a)

<sup>28</sup> NSID article 20, subsection 4.2.6. (European Union, 2016a)

<sup>29</sup> NSID article 14, subsection 4.2.4. (European Union, 2016a)

<sup>30</sup> NISD article 16, subsection 4.2.5. (European Union, 2016a)

Commission, 2017b). However, the limit of 72 hours by the GDPR must be considered regarding to personal data (European Union, 2016b). As the following figure 8 (and related NISD articles) indicate, incident notifications are submitted either to competent authorities or CSIRTs, depending on how the notification process in a Member State has been defined:

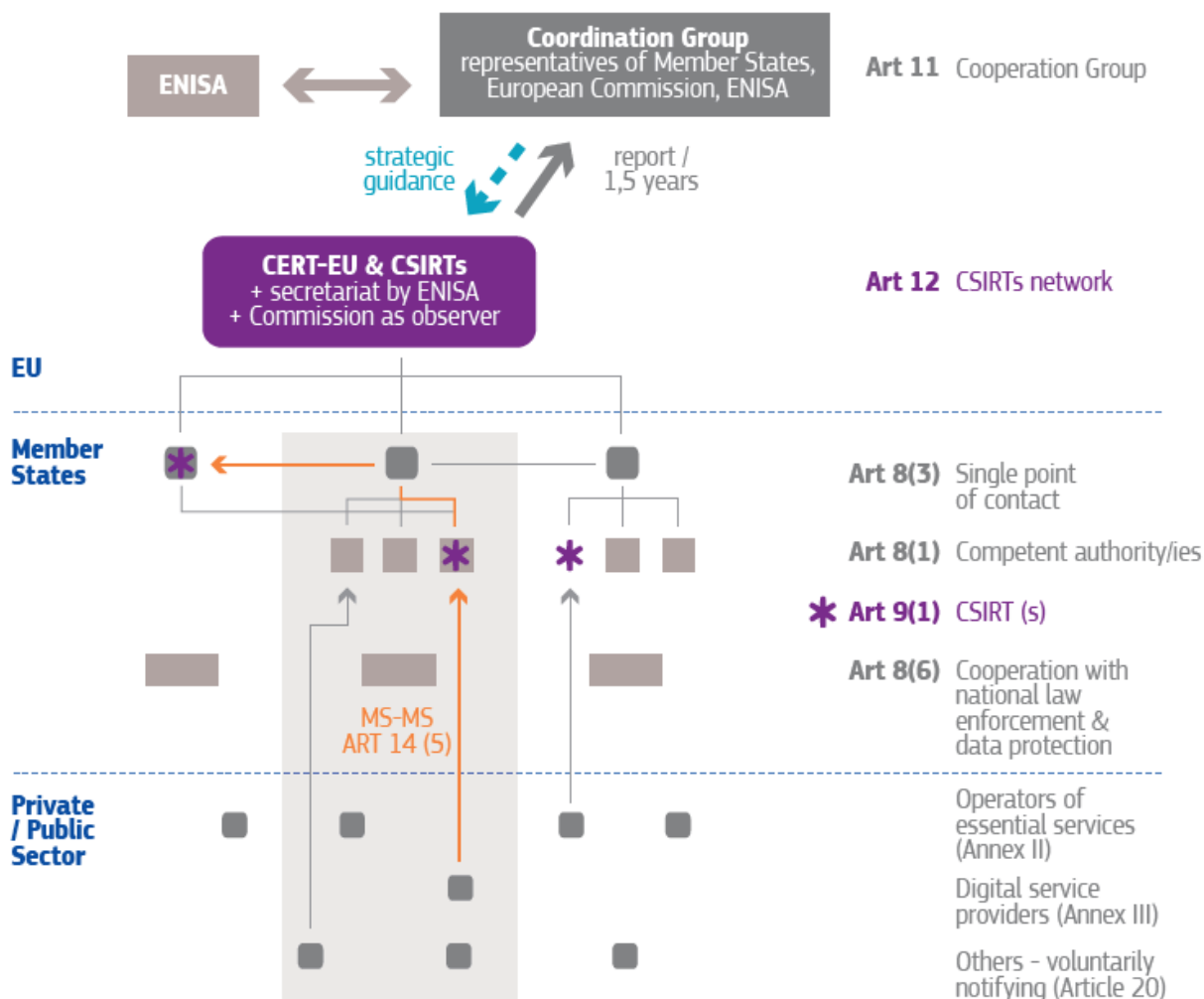


FIGURE 8. Cyber cooperation structure with related articles. (European Political Strategy Centre, 2017)

Each Member State must have designated one or more competent authorities that receive these incident notifications (and oversee application of the NIS Directive). In case where only one competent authority is designated, the same authority will serve as a single point of contact, as well. In plural case where (a) one or more competent authorities, (b) one or more CSIRTs, and (c) single point of contact are separated, they must cooperate between each other for the sake of cooperation efficiency. If CSIRT is not the primary receiver CSIRT must have access to the incident data. CSIRTs are responsible for monitoring incidents, assisting and responding to them, cooperating with private sector, providing early threat warnings and public notifications, if necessary. All cooperation must be executed in respect of the data without exposing sensitive material that

could harm the notifier(s). Conclusively, incident notification must be informed to the single point of contact which is responsible of passing information onwards to other relevant Member States. (European Union, 2016a)

Cooperation on European level involves cooperation across Member States and international cooperation with external parties of the EU. The European cooperation consists national single point of contact, CSIRT network and Cooperation Group, whereas international cooperation may involve any relevant stakeholders outside the EU. The single point of contact is some sort of a first-liner in European cooperation. They are responsible of ensuring information exchange<sup>31</sup> with authorities of other Member States, Cooperation Group, and CSIRT network. It could be argued that single point of contact of each Member State act a central role regarding to European cooperation, while their focus is to receive and deliver information. Likewise, CSIRT network is having a central role but in operational means<sup>32</sup>. CSIRT network is ought to exchange information, coordinate responses, develop further forms of operational cooperation and issue guidelines. The following figure 9 (and related NISD articles) show overall cooperation relations between different levels, though, it contradicts with the previous figure 8 regarding to European level of cooperation:

---

<sup>31</sup> NISD article 8, subsection 4.2.2. (European Union, 2016a)

<sup>32</sup> NISD article 12, subsection 4.2.3. (European Union, 2016a)

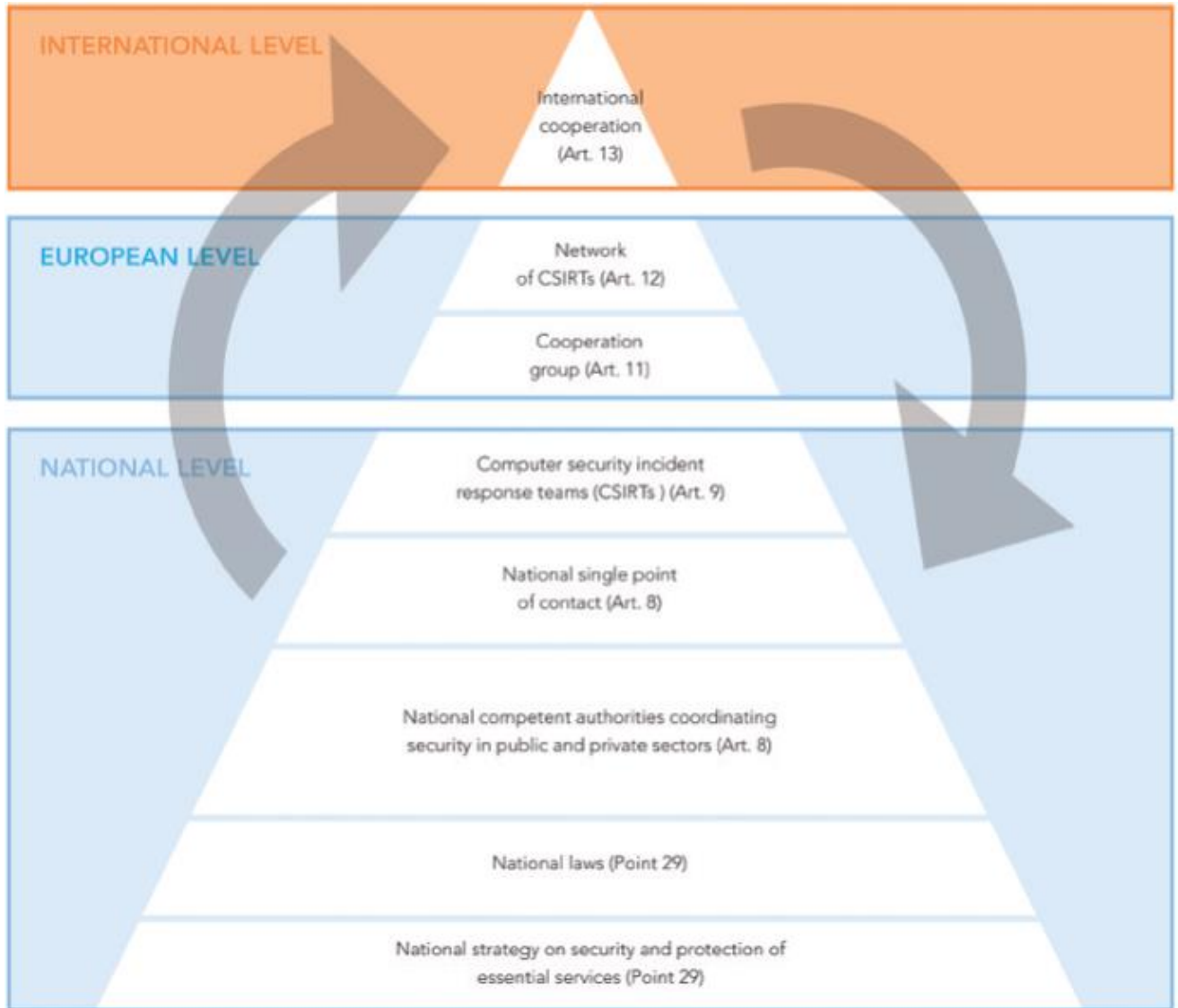


FIGURE 9. Organisational cooperation levels of the NIS Directive. (Vincent, 2018)

According to the NIS Directive (European Union, 2016a), Cooperation Group<sup>33</sup> in figure 9 should be placed above CSIRT network as Cooperation Group conducts *strategic* tasks, such as guidance and planning, exchange of information, developing trust and confidence, and fundamentally aims to achieve high common level of security of NIS within the EU. Frankly, all these are clashing on each other; all levels are emphasised with *information exchange* but from different perspectives *id est* on different levels. Additionally, there is ENISA acting on side which, in the future, could be nominated as an “EU Cyber Security Agency” (European Commission, 2017). Thereby, instead of “only” supporting, its role in NIS cooperation could be modified towards more central one in coming decade when ENISA and the Directive progress. Finally, we are having international cooperation where, enabled by the NIS Directive<sup>34</sup>, cooperation with third countries or international organisations and agreements

<sup>33</sup> NISD article 11, subsection 4.2.3. (European Union, 2016a)

<sup>34</sup> NISD article 13, subsection 4.2.3. (European Union, 2016a)

are made possible. This allows external parties to participate to Cooperation Group when adequate data protection is guaranteed. (European Union, 2016a)

#### **4.4 Conclusions**

The NIS Directive is presented in this chapter throughout its articles and with further elaboration of requirements. The main purpose of the chapter has been to provide a deep in-sight on the Directive and further open what are required by different entities.

Objectives of the NIS Directive were elaborated. There were viewed what consist within OES and DSPs, as well as that voluntary notifications can be made. Requirements must have implemented on national laws and national competent authorities must have been designated by Member States to coordinate security in public and private sectors. There are national single point of contacts and national CSIRTs that should, together with OES, DSPs and competent authorities, to guarantee operational cooperation. There are CSIRT network and Cooperation Group, together with the Commission and ENISA that ought to improve strategic level and international cooperation.

## **5 CHALLENGES OF THE COOPERATION**

### **5.1 Introduction**

The NIS Directive is a new regulative document; first of its kind. There are challenges around it as there are 28 Member States which of each are implementing the Directive with their own perspective. Also, the Directive itself has provided rather broad definitions which may require further clarifications to enable effective, coherent and harmonised cyber security cooperation in Europe.

Fundamentally, this chapter answers to the third sub-question (What challenges are enunciated of the cooperation?). Based on found literature, it provides a view to the present landscape of the NIS Directive and its implementation challenges.

The chapter is divided into nine sections, beginning with this introduction. The sections include discussion about variety in approaches, variety in maturity and resources, as well as trust and language issues. They are followed by identification of entities regarding to OES, DSPs and other relevant stakeholders, reporting and confidentiality issues, as well as compliance and sanction variations. In the end, there is elaboration of matters that are left out of scope of the NIS Directive. Finally, conclusive section ends the chapter.

### **5.2 Variety in Approaches**

Since there are 28 Member States, there are equally as many ways of approaching and implementing the NIS Directive. Carrapico and Barrinha (2017) have researched the EU whether it is a coherent (cyber)security actor or not. There have been internal and external security concerns which have led to calls for more intensive EU security policies coherence. Though, as Carrapico and Barrinha argue, because the coherence has not been systematically operationalised, the EU security field has become more or less fragmented. If



the EU would be more coherent overall, it would be more integrated union in the security field too. There are principal values of democracy that the EU defend but when values are fragmented, it becomes problematic. To be a coherent actor in the security field the EU must be coherent with the values that the EU defends.

When we are considering, not only cyber, but overall security perspectives in Europe, we notice that perceptions of the EU as a security actor varies. As the following figure 10 illustrates, the above-mentioned coherence is lacking:

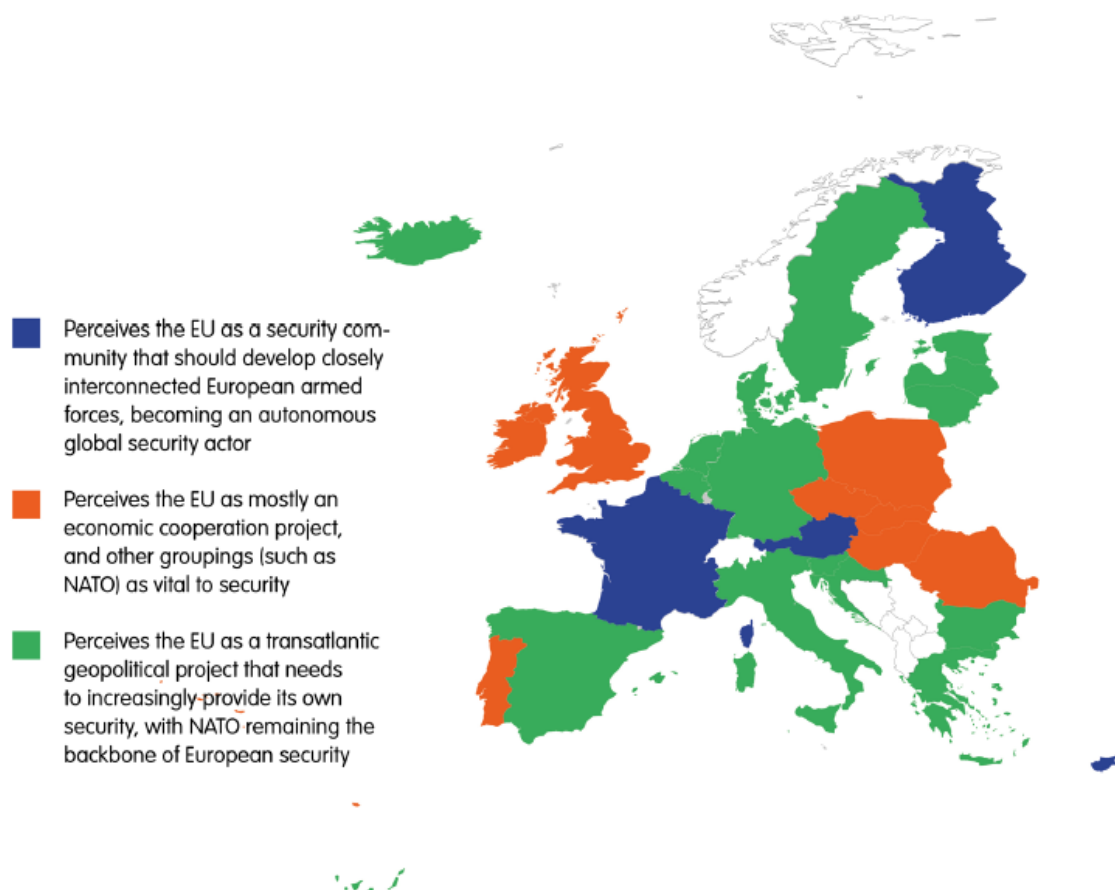


FIGURE 10. Perceptions of the EU as a security actor. Original source: European Council on Foreign Relations (ECFR). (Dennison et. al., 2018)

This means that perceptions and expectations of the EU are different. When security within Member States is approached so many ways and expectations of the EU as a security actor are so different it cannot be expected that security issues could be handled with very clear unity either. (Dennison et. al., 2018)

Like the figure 10 above shows, some Member States see rather NATO as a provider of security than the EU. Despite overlapping between these two major players in Europe, Lukas et. al. (2016) express that cooperation between the EU and NATO, and transatlantic cyber security cooperation (and security in general) are needed. The current cyber threat landscape, as discussed in chapter three, drives towards cooperation. As an example of effective cooperation across authorities of different countries, Lukas et. al. mention efforts of Europol

against cybercrime. The EU and NATO could achieve similar results. By far, their cooperation has been promising but only foundational. So, there is still room to grow.

When we consider the NIS Directive (which is a directive not a regulation as the GDPR) each of Member States have unique approach on it. Member States are creating new laws or amending the existing ones. Approaches on nominating competent authorities vary by having many different sector-based authorities compared to just single one. It is also possible that a company is identified as an OES in one Member State, but not in another (Billois et. al., 2017). This is “an unprecedented information sharing and data gathering exercise” (Surguy, 2017). Thereby, the fragmentation of the NIS Directive will lead to a situation where tracking the impact of the NIS Directive is rather complicated. There is no single manner to compare Member States or compare implementations of the Directive. (Evans & White, 2016)

The fragmentation can be well illustrated when reflecting table 2 differences in nominating single point of contact, competent authorities and national CSIRTs throughout the EU. As discussed in subsection 4.2.2 about these authorities and the requirement of Member States having national cyber security strategy, it is notable that not all elements were in place when the derivation from website of European Commission (2018) was made on 7 September 2018.

	Country	Status of Transposition	National Strategy	Single Point of Contact (SPoC)	National Competent Authority for DSPs	National Competent Authority for OES	National CSIRT(s)
1	Austria	In progress	Details TBD	Details TBD	Details TBD	Details TBD	Details TBD
2	Belgium	In progress	Yes	Centre for Cybersecurity Belgium	Same as the SPoC	Same as the SPoC	Centre for Cybersecurity Belgium
3	Bulgaria	In progress	Yes	State "E-gov" Agency	Information Technologies and communications	6 authorities nominated	National CSIRT bg
4	Croatia	In progress	Yes	The Office of the National Security Council	Entrepreneurship and Crafts	11 authorities nominated	National CERT, Security Bureau
5	Cyprus	Transposition	Details TBD	Digital Security Authority (DSA)	Details TBD	Details TBD	National CSIRT (CSIRT-CY)
6	Czech Republic	Transposed	Yes	National Cyber and information security agency	CZ NIC	Same as the SPoC	GovCERT (OES), CSIRT.CZ (DSPs)
7	Denmark	Partially transposed	Yes	The Danish Centre for Cybersecurity	Danish Business Authority	4 authorities nominated	Same as the SPoC
8	Estonia	Transposed	Yes	Estonian Information System Authority	Same as the SPoC	Same as the SPoC	Same as the SPoC
9	Finland	Transposed	Yes	Finnish Communications Regulatory Authority	Same as the SPoC	6 authorities nominated	Same as the SPoC
10	France	Partially transposed	Yes	Agence nationale de la sécurité des systèmes d'information (ANSSI)	Same as the SPoC	Details TBD	CERT-FR
11	Germany	Transposed	Yes	Federal Office for Information Security / Bundesamt für Sicherheit in der Informationstechnik	Same as the SPoC	Same as the SPoC	Same as the SPoC
12	Greece	In progress	Yes	National Cyber Security Authority (General Secretariat of Digital Policy - Ministry of Digital Policy, Telecommunications and Media)	Same as the SPoC	Same as the SPoC	National Authority Against Electronic Attacks - National Cert
13	Hungary	Partial transposition	No	National Cyber Security Centre	National Directorate General for Disaster Management	National Directorate General for Disaster Management	Same as the SPoC
14	Ireland	In progress	Yes	CSIRT-IE	Same as the SPoC	Same as the SPoC	Same as the SPoC
15	Italy	Transposed	Details TBD	Details TBD	Details TBD	Details TBD	Details TBD
16	Latvia	In progress	Yes	Ministry of Defence	Ministry of Transport	8 authorities nominated	Information Technology Security Incident Response Institution
17	Lithuania	Partially transposed	Draft	National Cyber Security Centre (NCSC/CERT-LT)	Same as the SPoC	Same as the SPoC	Same as the SPoC
18	Luxemburg	In progress	Yes	Institut Luxembourgeois de Régulation	Same as the SPoC	5 authorities nominated	CERT Gouvernemental / CERT National
19	Malta	In progress	Details TBD	Infrastructure Protection Unit	Same as the SPoC	Same as the SPoC	CSIRTMalta
20	Netherlands	In progress	Yes	National Cyber Security Centre (NCSC)	Affairs and Climate Policy	5 authorities nominated	Details TBD
21	Poland	In progress	Yes	Ministry of Digital Affairs	Same as the SPoC	Same as the SPoC	Same as the SPoC
22	Portugal	In progress	Yes	Portuguese National Cybersecurity Centre	Same as the SPoC	Same as the SPoC	CERT.PT
23	Romania	In progress	Yes	Details TBD	Details TBD	Details TBD	Details TBD
24	Slovakia	Transposed	Yes	National Security Authority	Same as the SPoC	Same as the SPoC	National SK - CERT
25	Slovenia	Transposed	Yes	Government Office for the Protection of Classified Information	Slovenian National Cyber Security Incident Response Centre	Slovenian National Cyber Security Incident Response Centre	Slovenian National Cyber Security Incident Response Centre
26	Spain	In progress	Yes	National Security Council, through the National Security Department	Secretary of State for Information Society and Digital Agenda (private), Ministry of the Presidency and for the Territorial Administrations, through the National	Secretary of State for Security, -Ministry of Interior-, through the National Center for the Protection of Infrastructures and Cybersecurity (CNPIC)	INCIBE-CERT, National Cybersecurity Institute (private), CCN-CERT, National Cryptologic Centre
27	Sweden	In progress	Yes	Myndigheten för samhällsskydd och beredskap - MSB	Post-och telestyrelsen	5 authorities nominated	MSB/CERT-SE
28	United Kingdom	Transposed	Yes	National Cyber Security Centre (NCSC)	Commissioner's Office (ICO)	9 authorities nominated	Same as the SPoC

TABLE 2. State-of-play of the transposition of the NIS Directive, derived on 7 September 2018. The information applied from the European Commission (2018) website.

Also, notable in table 2 is that how different approaches Member States have taken. For example, when comparing two countries sized close to each other, Estonia and Latvia, they have completely diverse approach on nominated competent authorities for OES. Estonia has chosen one competent authority strategy, whereas Latvia has eight authorities nominated for different sectors. Germany and the UK have similar results. SPoC serves all in Germany, whereas there are nine nominated authorities for OES in the UK. When OES authorities are generally compared, it can be observed that some have only the Single Point of Contact (SPoC) nominated, whereas others have from 1 to 11 other than SPoC authorities nominated. Spain, on the other hand, do have two national competent authorities for DSPs, one for public and one for private sector, unlike anybody else. Some have CSIRT and SPoC separately, some have SPoC appointed on every column of their row. Overall, it could be argued that effectiveness and harmonisation are hard to compare when approaches are vastly different. (European Commission, 2018)

Requirements among Member States and in different sectors will likely diverge too. Thereby, cooperation is naturally difficult. It would be essential for all Member States to have an agreement that would define the minimum level of cyber security maturity in businesses (BBVA, 2016). Whether or not, there will be a mass amount of information to collect and the Cooperation Group, with combination of the EU agencies and institutions, will have challenging moments in exchanging ideas, comparing national strategies and gathering best practices. (Surguy, 2017) These are, undoubtedly, contrary to the goal of the NIS Directive to harmonise European cyber security incident handling scheme. (Evans & White, 2016)

### **5.3 Variety in Maturity and Resources**

As there is variety in approaches, there is also variety in maturity level and resources across Member States. This is quite natural if not all Member States and companies have invested in cyber security equally. Considering all the threats described in chapter three, the situation is certainly challenging. Basically, the standard of security of information systems does vary from Member State to another. In practice, this means that business and information of consumers are better protected in some countries and more vulnerable in others. (Surguy, 2017)

Indeed, when looking at figure 11 and resilience in whole spectrum of Europe, we see quite major differences.

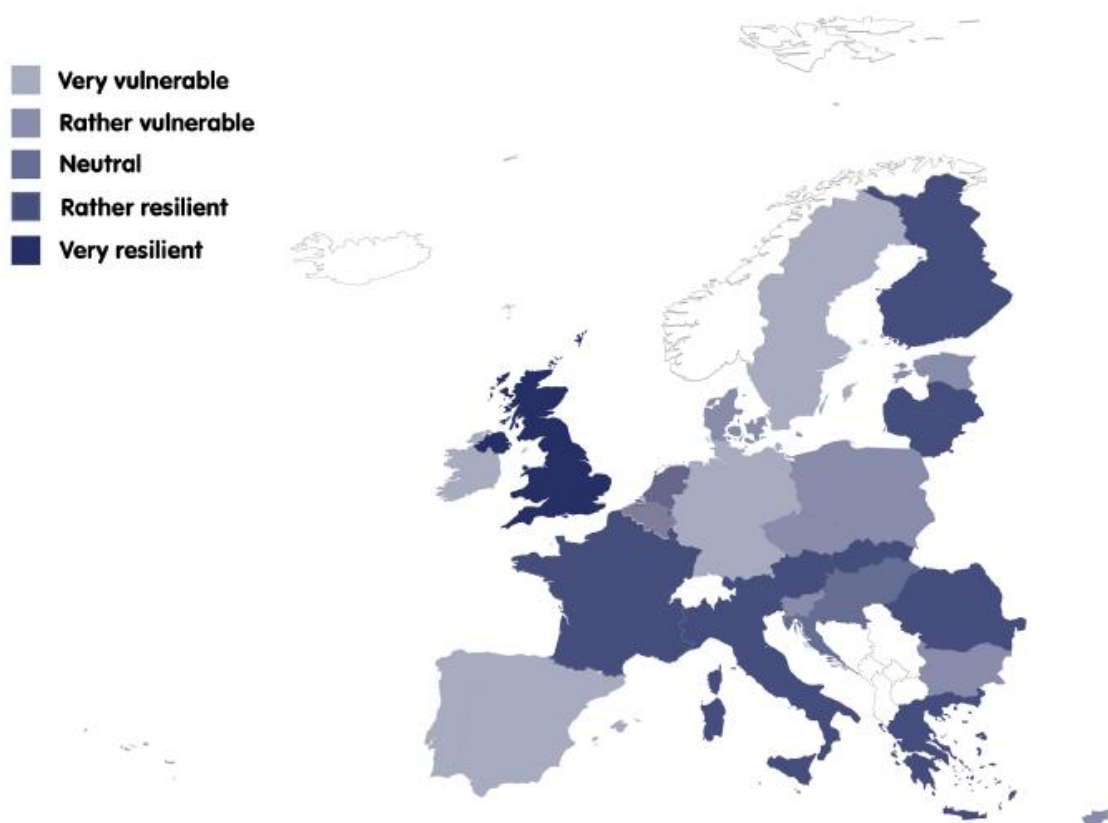


FIGURE 11. Perceived vulnerability to cyber-attacks. Original source: European Council on Foreign Relations (ECFR). (Dennison et. al., 2018)

For the benefit of the EU, all Member States would be good to have coloured with dark blue. To some extent, one solution for such security maturity improvement could be standardisation. The NIS Directive encourage to adopt international information security management standards, such as ISO/IEC 27001, NIST or other similar European or national standards, as discussed in subsection 4.2.6<sup>35</sup>. To improve security maturity across Europe, the implementation of standards could at least ease the situation. Simultaneously, exchange of best practices could improve standards overall, as well. Better security maturity level of each Member State would help on struggle against occurring incidents. (Surguy, 2017)

When some Member States have been more mature, some may need new resources. Some may have needed to form new competent authority, whereas some could have designated an existing one. Either way, it is crucial for cooperation to work well that sufficient resources are provisioned by governments. To work well, appropriate staffing is significant too. (Surguy, 2017)

According to Chantzios<sup>36</sup> (2017), a key to success is always nearly the same: (1) There must be competent individuals brought together *id est* right people, (2)

<sup>35</sup> NISD Article 19: Standardisation. (European Union, 2016a)

<sup>36</sup> Ilias Chantzios, Senior Director at Symantec Government Affairs at the time of the reference date. (EU2017EE, 2017)

trust among employees must be built to have effective cooperation between them, and (3) well defined, enough narrow mission where a clear goal is emphasised. Additionally, governance in an organization is critical since through governance the necessary trust can be built. Basically, to have better cyber security, community around it must be trustable. There have to be the competence to handle provided data and to find a solution. So, correct resources and staff are important when growing maturity.

Obviously, many of investments mentioned above are about costs. The NIS Directive requires appropriate and proportionate security measures to ensure security of NIS. They should be appropriate and proportionate to the risks and have ability to prevent and minimise the impacts of incidents on the services and NIS. For example, in implementing the security measures, DSPs should consider: “(i) security of systems and facilities, (ii) incident handling, business continuity management, monitoring, (iii) auditing and testing, and (iv) compliance with international standards” (Bickerstaff et. al., 2016). Because of expectations by the NIS Directive, industry standards may arise and for the concerned companies, these may increase security and infrastructure costs. (Bickerstaff et. al., 2016)

Even with proper resources, it is challenging to detect cyber threats early on. Especially regarding to critical infrastructures, it would be essential to involve industry, and bridge the gap between industry and public entities. More proactive detection of threats would be needed. On the other hand, this may require further investments by different entities and that is somewhat hard for some entities and Member States. At least, cooperation in this sense would be vital. (European Political Strategy Centre, 2017)

## 5.4 Trust and Language

Even there are differences in approaches, resources and maturity, nevertheless, trust must be gain and speak the same language. By far, the CSIRT network has been an important step in creating trust between Member States, which has been lacking. Though, improvements towards ever more efficient cooperation and, thereby, trust are needed. It may take time to build trust, but it should be achievable throughout cooperation. (Demaison<sup>37</sup>, 2017)

Throughout cooperation and information sharing, it should be possible to break any existing silos. Though, according to Chantzou (2017) information sharing is not the solution to every problem. At the core of trust is that not any information can be shared. For example, private companies are custodians of data that concerns victims or customers which they will not disclose. Thus, there should be discussed how and what will be shared to CSIRTs and law enforcement authorities, such as toolkits used to launch attack, indicators of

---

<sup>37</sup> Jean-Baptiste Demaison, Senior Policy Adviser, ANSSI, France, at the time of the reference date. (EU2017EE, 2017)

compromise, or information of criminal infrastructure. Either way, not any information can be shared and what is absolutely critical is that the shared information is under control. If the data would leak it would have adversary advantage, it would worsen the situation and confidence. Information sharing parties must be comfortable on how and under what conditions information is being shared. Otherwise, there is no trust.

For being able to work together in the name of cooperation, using the same language is equally important. For gaining the same language, it has been done in conferences and in the Cooperation Group but it requires more discussions and time. (Demaison, 2017) For example, in private sector there is different language used than on public sector where words, such as recycling or critical infrastructure are unfamiliar or genuinely not common. (Purser<sup>38</sup>, 2017)

The comprehensive discussions and implementing the existing requirements are important in creating coherent cooperation. Standard operating procedures and taxonomies create abilities to work together. There are already in place entities, bodies and tools provided by the treaties, such as solidarity clause in the Treaty on European Union<sup>39</sup> (European Union, 1992). Also, one possible solution for EU external trust gaining would be to improve EU cyber partnerships which means cyber diplomacy, or a traditional diplomacy applied to a new policy area (Renard, 2018). The EU has done crisis management before, but the problem is that no crisis management has been done within cyber space and language used might vary from member state to member state, and from member state to private sector. (Demaison, 2017)

Responsibilities, including language and trust within work are yet to be clarified. However, these are elements that should get to work. Demaison (2017) argues that the next step what should be done is “doing the first step” *id est* have all the above-mentioned elements to work where vital role is especially played by the CSIRT network (not-forgetting occasional work of Cooperation Group either). Thereby, trust and same language can be built. On the other hand, there are people who already think about next steps, expecting more than already is occurring even though the current implementation steps are not yet completely fulfilled. As long as these are not completely fulfilled, lack of trust and same language remain challenges that elements of the EU cyber security cooperation must continue to overcome. (Demaison, 2017)

---

<sup>38</sup> Steve Purser, Head of Core Operations Department at ENISA at the time of the reference. (EU2017EE, 2017)

<sup>39</sup> Treaty on European Union (TEU), also referred as the Maastricht Treaty or the Treaty of Maastricht. The TEU includes a solidarity clause for Member States to support each other when in need. (European Union, 1992)

## 5.5 Reporting and Confidentiality

Among some private companies, concerns are raised regarding to reporting requirements. Concerns originate from obligation of competent authorities or CSIRTs, in certain circumstances, to inform other Member States of incident details notified to them by OES or DSPs. Concerns affiliate to confidentiality and thereby security, including general incident management, if confidential information is shared across the EU. (Evans & White, 2016)

Information sharing between Member States can be easier compared to between private companies and CERTs. According to Grigoras (2017), the requirement of sharing information is very important for tactical level since CERTs cannot overcome cyber security issues on their own and they need PPP for solving incidents. Grigoras argues that often public and private sector have the same interest on solving issues, but sometimes private sector has a problem in sharing information. The problem originates from that private companies have non-disclosure agreements, or they might have number of other similar type of engagements which do not allow them to contribute incident information. On the other hand, Grigoras states that these type of PPP issues can be solved with appropriate policy making and continuum of increasing cooperation within CSIRT network.

Additionally, when private companies deliver information on public sector they expect to have something back. Though, very often, private sector companies do not receive anything. This is because in many cases CERTs must deal with law enforcement. CERTs receive the information and provide it to law enforcement, but due to procedures or instruments of cybercrime cases they cannot provide information back. This could be problematic for private sector companies. When they do not receive anything, they cannot improve their security measures. (Grigoras, 2017)

Even reporting mechanisms would work they require resources that not all entities are capable of having and similarly executing. Surguy (2017) argues that reporting can be expensive and onerous. In the worst-case scenario, competent authority can be overwhelmed of the amounts of information received. Surguy states that OES and DSPs want to be aware how notification and incident reporting will work in practise. There must be an identifiable line on what is reportable and what is not. As presented in subsections 4.2.1<sup>40</sup>, 4.2.4<sup>41</sup> and 4.2.5<sup>42</sup> the NIS Directive certainly provides some descriptions, but daily cooperative work may be required to perceive accurate limits on reporting.

Accurate level of reporting is important. There are guidelines as mentioned in the paragraph above, but each Member State must develop

---

<sup>40</sup> NISD article 6: Significant disruptive effect. (European Union, 2016a)

<sup>41</sup> NISD article 14: Security requirements and incident notification of OES. (European Union, 2016a)

<sup>42</sup> NISD article 16: Security requirements and incident notification of DSPs. (European Union, 2016a)



appropriate threshold mechanism. Kaskina (2017) argues that Member States must find the best definitions on cyber incidents. Only with the correct definitions sufficient information to national CSIRT teams can be achieved. Simultaneously, number of incidents should not overload the NIS subjects with excessive obligatory reporting. Once again, it may take time to have suitable solutions on accurate level of reporting.

Interconnections of incidents can be difficult to identify and thereby hard to perceive whom the reports should be shared. As Kaskina (2017) argues, it is hard not only for CSIRT teams and a Member State but sometimes for private companies as well. Private companies own information on “how their services depend on data or connectivity to another country” (Kaskina, 2017). Even they might not always have a clear view on how interruptions in their services could cause problems for other entities in other countries. Of course, more information could be shared but, as stated in the previous paragraph, extensive reporting may not be a solution either. Identification of cross-border dependencies among Member States is very hard task accomplish. Thereby, it is challenging to comprehend what data and to whom such incident reports should be notified, not forgetting confidentiality either.

In conclusion, what is being shared in reports is important. Even more important is to be careful *how* information is being shared. Confidentiality is vital in reporting as they include valuable business or vulnerability information. The right information should be shared for the right purpose. (Purser, 2017)

## 5.6 Identification of Entities

As described in subsection 4.2.1<sup>43</sup>, the identification criteria is very broad. Despite that the Cooperation Group assists in the process of identification of OES, there is still as many possibilities to interpret the requirement as there are Member States. Due to generality, the identification is not an easy task. In a particular sector, not all entities are providing essential services. Instead, there should be considered how dependable provided service is on NIS and can they undergo a “significant disruptive effect” as described in subsection 4.2.1<sup>44</sup>. Certainly, the description may apply on most of businesses but not all. Defining criteria on some sectors, such as healthcare and water supply, is difficult and there might be either very few organisations or simply too many (Kaskina, 2017). It is very likable that we may see divergence between Member States in approach of the identification of OES. (Surguy, 2017)

In PPP clear identification of entities would be extremely good to have. Now there seem to be variation across Member States (Kaskina, 2017). Additionally, benefits of PPP are debatable and does not always deliver win-win situation for both sides. There could be (1) disagreements about the scope,

---

<sup>43</sup> NISD article 5: Identification of operators of essential services. (European Union, 2016a)

<sup>44</sup> NISD article 6: Significant disruptive effect. (European Union, 2016a)

methods and definition, (2) complications of sharing confidential information and lack of trust, and (3) “the dissonance between the ‘better safe than sorry’ logic of public security agencies and the ‘profit first’ logic of private companies” (Bures, 2016, 299). So, PPP is not always simple but that is most likely what the NIS Directive drives to remedy. (Bures, 2016) However, Grigoras<sup>45</sup> (2017) emphasises PPP and argues that the cooperation between public and private sector is really important. This is because on tactical level, cooperation within PPP is a “must have”. For effective cooperation, it is important to have PPP working and the identification of entities clarified as CERTs cannot tackle cyber security issues on their own.

When evaluating the NIS Directive identification requirements, there should be considered that large countries have plenty of both OES and DSP entities, whereas smaller countries do not have even nearly as many, or none at all. (Kaskina, 2017) Though, when considering the number of critical infrastructure entities, there should also be considered interdependencies between them which the following figure 12 of ICS/SCADA illustrate.

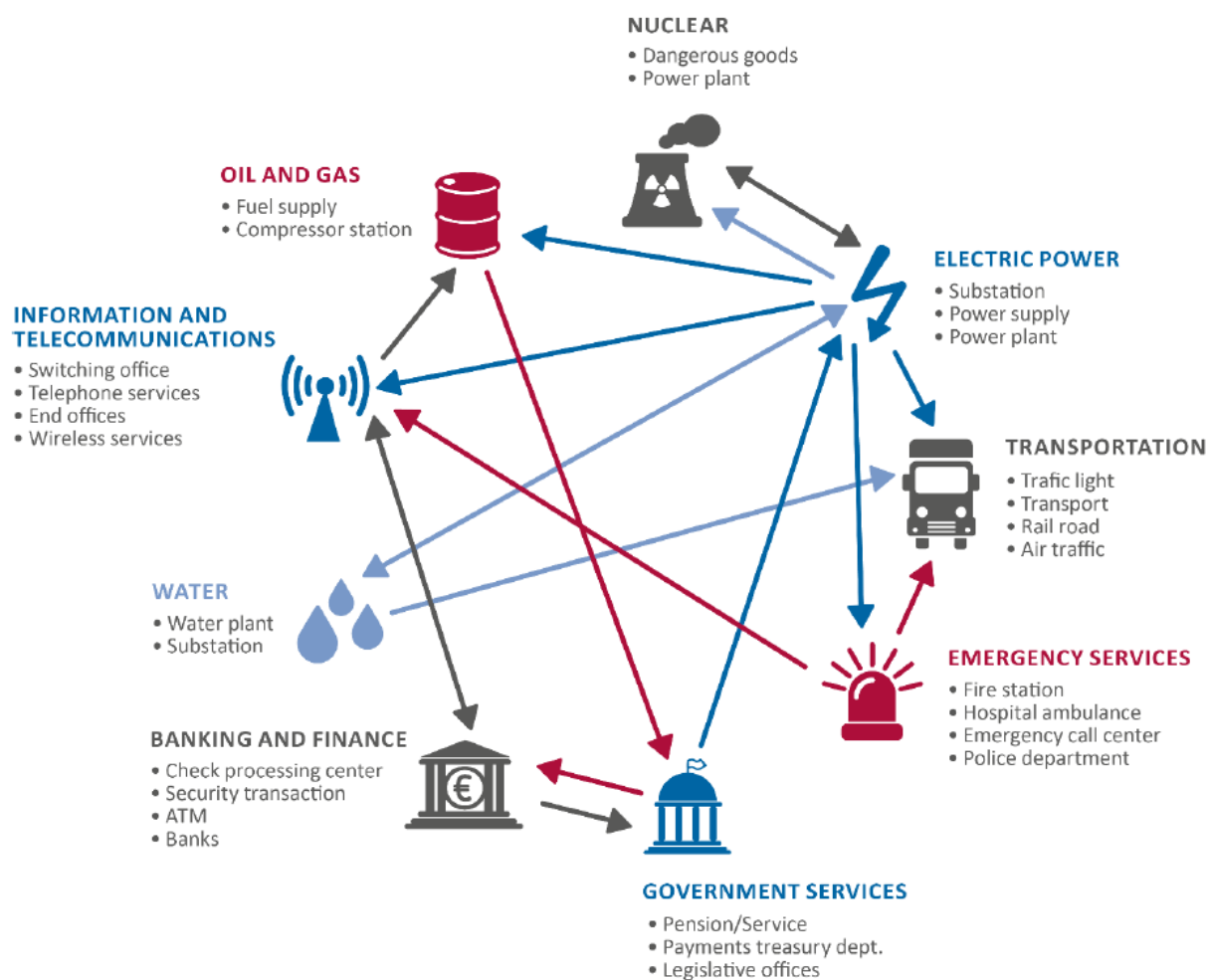


FIGURE 12. Interdependencies of each Critical Infrastructure. (ENISA, 2017)

<sup>45</sup> Mircea Grigoras, CERT-RO Deputy Director, Romania at the time of the reference. (EU2017EE, 2017)

To prevent catastrophic consequences, there should be understanding of risks that an attack may cause to other dependent on another. Especially, energy providers are crucial. (ENISA, 2017)

However, as referred in appendix III<sup>46</sup>, and in points 4 and 5 of appendix IV<sup>47</sup>, definitions of DSPs are short and broad. Small countries, such as Estonia and Latvia, may not have many DSPs as subjects of the NIS Directive requirements. With such parameters of OES and DSPs, we will see great variation between smaller and larger Member States. (Kaskina, 2017)

## 5.7 Compliance and Sanctions

Different security cultures cause different approaches on compliance and sanctions. Also, varying supervision schemes drive different ways of implementing flow. Karsberg <sup>48</sup> (2017) states that national supervision authorities should not be seen as an obstacle, but as a possibility. For building a trustful national information sharing culture, sanctions should be the last step when everything else has failed. The same view is not shared across Member States and there are variations in approaches to this matter. Instead, Karsberg argues that entities should courage on reporting. The view is also supported by Carrapico and Barrinha (2017) by stating that “carrot-and-stick” may not be effective.

Karsberg (2017) argues that there should be a continuous learning curve which would lead to continuous improvements in security. It would consist of three elements. (1) An actor would learn from its experiences and would continuously improve. (2) Supervisors would learn what they should focus on. (3) If a relationship would be really mature, there could be gatherings within sector where information of vulnerabilities, threats and incidents could be shared, and have accurate information to act upon. This kind of information sharing exercise would benefit cross-border cooperation too.

Nonetheless, sanctions in Member States vary. For example, penalties for non-compliance with the NIS Directive in the UK can be up to 17 million pounds in some circumstances (Hadwin, 2018). In Spain and Sweden, sanctions can be up to 1 million euros. In Germany and in the Netherlands, up to 5 million euros. In Poland, up to 50 000 euros. Some countries, such as Denmark and Finland have not determined any specific sum and apply existing sanction regimes. Some Member States have not yet determined their sanctions.

---

<sup>46</sup> NISD annex III. (European Union, 2016a)

<sup>47</sup> NISD article 4: Definitions. (European Union, 2016a)

<sup>48</sup> Christoffer Karsberg, Program Manager International Affairs at the Office of Cybersecurity and Critical Infrastructure Protection, the Swedish Civil Contingencies Agency at the time of the reference. (EU2017EE, 2017)

Therefore, it can be argued that sanctions are not harmonised. (Bird & Bird, 2018)

## 5.8 Out of Scope

This section discusses about elements that are left out of scope of the NIS Directive. Importance of the topics may vary but they are certainly relevant to consider. The NIS Directive is first of its kind in the EU and it might require further or broader development in the future.

When the NIS Directive regulates about different sectors of OES and DSPs, it does not consider anyhow computer hardware manufacturers and software developers when they do not provide essential or digital services *per se*. Lack of them within the scope rise concerns among some security professionals. Hardware and software are in a central role in cyber security. (Petri<sup>49</sup>, 2017)

Surguy (2017) argues that they simply cannot be ignored. Of course, hardware and software manufacturers do have commercial and reputational interests as incentive. They do have incentive also due to risk of expensive lawsuits if the product does not fulfil rules of product requirements. Surguy refers to Cal Leeming - a reformed hacker - in stating that incentive for "security by design" in manufacturing and software developing phase is insufficient. Therefore, Surguy presumes that hardware manufacturers and software developers might be set to the scope of frontline operators in the future. (Surguy, 2017)

Even the NIS Directive itself does not take a stand on hardware and software, generally the EU has taken steps forward in this sense. On 13 September 2017, the European Commission released a "Proposal for a Regulation of The European Parliament and of the Council on ENISA, the 'EU Cybersecurity Agency', and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ('Cybersecurity Act')" (European Commission, 2017a). Ever since the proposal has been for round of statements (Council of the European Union, 2018). However, the objective of the new proposal is to (1) foster the role and grant a permanent mandate for ENISA as the EU Cybersecurity Agency, and more importantly regarding to this paragraph, to (2) release a new, voluntary based, EU-wide certification framework, Cybersecurity Act, which purpose is to enhance cyber resilience within the EU and build trust on ICT processes, products, and services security. The new framework could improve security areas that the NIS Directive does not cover. Though, it may take a while to come into force. The history roadmap of the NIS Directive begun first with a mention in the EU cyber security strategy and a proposal was adopted in March 2014 (Long, 2014). It circulated for statements for two years, got officially

---

<sup>49</sup> Axel Petri, Senior Vice President of Group Security Governance, Deutsche Telekom AG at the time of the reference. (EU2017EE, 2017)

regulated in 2016, and was implemented by Member States in 2018. The gap between the proposal and implementation of the NIS Directive was four years. Therefore, it is very likable that we may not expect the new proposal of “EU Cybersecurity Agency” and “Cybersecurity Act” to be actualised in the EU and in our daily lives very soon. (European Council and Council of the European Union, 2018)

Regardless of how secure tools or networks are or how securely end-users operate, attackers aim to find new loopholes. Thus, the degree of dependency on whole NIS, in the first place, is somewhat something to be considered. As we are so reliant on technology, there should be discussion on whether there are some areas where the use of NIS could be reduced. For example, during the above mentioned 2017 ransomware attacks, many victims had to use traditional paper and pen because they had no other options. When their systems were encrypted, paper and pen were the only solution for operation continuum. When investments on cyber security and cyber incident costs are quantified in a long period, sums may be notable. Practically, this means that in some areas less dependency on technology could be worth of consideration. If an organisation is less dependent on technology, in the best-case scenario, it would be both more cost effective and safer at the same time. Therefore, the topic of technology reliance is certainly one not to be overlooked. (Surguy, 2017)

## 5.9 Conclusions

There are many challenges related to the NIS Directive. Some of them take time to be clarified. Some may require daily and annual cooperation. Some, on the other hand, may require regulations and instruction by Member States or the EU itself.

Approaches to the NIS Directive vary when there is no clear coherence between Member States. Security is seen differently, so is implementations of the NIS Directive. Each Member State has their own way to implement it and this may harden to follow the harmonisation and compliance of the Directive.

Maturity level and resources across Member States vary. Some had multiple CERTs before the NIS Directive and some have had to form a new one. Obviously, those that have begun their security activities recently are not that high in maturity as those with years of experience. Investments are required but not always easy to fund. In the present world, there should also be appropriate, well-educated persons to handle incidents and keep up security.

Trust should be gained, and same language should be spoken. Trust is one of the main issues in cyber security cooperation when valuable economical, anomaly or personal information are shared. There should be clear means how to operate with incident data and to minimise possibilities for leaks. There the same terms and language are essential.

Confidentiality in reporting is vital. There are concerns about where vulnerabilities will be forwarded because such information could harm

organisations. PPP is important in this sense as CERTs cannot tackle cyber security issues on their own. Information sharing should benefit all but it is matter of how information is shared. There should be clear requirements on the reporting which would guarantee confidentiality.

As the NIS Directive is a directive, not a regulation, there are variations in identification of entities. Even countries that are similar size, they do have variations between each other. An organisation could be part of the OES in one country, but not necessarily in another. This is contrary to the goal of harmonisation.

Compliance is seen differently in Member States. Varying approaches drive different ways of implementing the NIS Directive. Also, sanctions vary throughout Europe. Some have major penalties on severe cases, some apply existing laws.

Computer hardware manufacturers and software developers are out of scope of the NIS Directive. Though, if the Cybersecurity Act will come into force in the future, it could ease the situation and harmonise these parts of cyber security. Certainly, considerable would be to think if some parts information usage could be left out of digitalisation.

In conclusion, there are many challenging parts, but it could be argued that these are somewhat possible to overcome. Though, this would require coherence throughout the EU. Cooperation in the name of the NIS Directive will show how these challenges can be overcome.

## 6 DISCUSSION

This chapter provides own thoughts by the author. They further elaborate many topics that are discussed in the chapters above. They are ideas that have been processed during the research process.

The chapter is divided into three core sections which are concerns, opportunities and recommendations on future research areas. Purpose of this chapter is to discuss about own subjective views on to the subject.

### 6.1 Concerns

Many times, in this thesis there is stated that threat landscape is evolving among evolvement of technology and increasing expertise of attackers. Cyber space enables easy ways to have financial gain or gather information, which perpetrators utilise without hesitation. It is quite likable that, based on the results shown in this thesis, we will still see major data breaches, malwares, ransomwares, financial frauds, DDoS attacks, information leakages, phishing, rise of different criminal organisations, and so forth. Resilience against these will not get any better if there is no will to invest on security and cooperation.

Certainly, the NIS Directive can be observed as a positive element for the EU which may have had to be enforced sooner or later. Otherwise, it could have left individual Member States more vulnerable. Though, we need to consider that with 28 Member States there are 28 cultures and 28 ways of fulfilling the requirements. Also, maturity level of cyber security varies across the EU, both on public and private sector, leaving some more vulnerable than others, whereas some are more advanced than others. The NIS Directive requires cooperation and notifications of major cyber incidents, but concerns are raised whether the process will work as supposed. It requires right systems and entities on appropriate level to have effective notification grid. In such a vast and ever-changing environment as cyber space is, a fully operational

cooperation requires hard work and most likely will take time to be fully effective.

It is interesting to see how different approaches Member States have taken (table 2). For example, national competent authorities for OES vary. Will it be easier to handle incidents when there is one on each sector, or will it be too slow. Could only one nominated authority for OES be the most effective or could it be overwhelmed by all notifications.

Unfortunately, security-by-design is not at the core of development as it should. As long as the situation remains, organisations and citizens are vulnerable for attacks. Alternative solutions for technology should be considered as stated by Surguy (2017). Especially, when we fuss about digitalisation. The NIS Directive does not consider hardware and software as its object. This could rise problems if not aware of the origins of the hardware. Security-by-design would be the solution for many problems but not many organisations are willing to invest on security as discussed subsection 3.3. Security should be seen as the one that makes business possible.

This thesis has not taken stand on Internet of Things (IoT) or Industrial Internet of Things (IIoT). Their usage seem to be broadening quickly and rises concerns whether their security is taken care of appropriately. Also, blockchain and artificial intelligence (AI) are worth to consider and how they change cyber space overall. AI could accelerate issues in cyber space evermore which may cause more economical losses.

In the EU Cyber Security Conference in Tallinn 2017, trust was one of the most used word among the participants (EU2017EE, 2017). Trust is something that has not gotten enough attention in this thesis. The author's personal view is that this is one of the main problems within the cooperation. Whom the information of incidents can be shared, are they able to use the information, and especially are they reasonably trustable entity not to leak any information. There are so many bodies of Member States and private parties involved that once the information is released it cannot be known how the information is used in the end. Obviously, none of private companies wish to peril their security, reputation or business for the sake of reporting. Thereby, the information that one releases, they have to be fully aware of consequences what the information might cause if ending up into wrong hands. Obviously, this would not build trust among stakeholders.

When looking at all the evidence it is quite clear that the beginning phase of the NIS Directive implementation is not easy task to complete. There are many variations of approach (for instance, the information in table 2) and different maturity in implementation. The Cooperation Group will certainly ease on tracking the impact of the NIS Directive. Question on whether it still be sufficient remains unanswered. Will CSIRT network actually build trust among Member States, it remains seen. Otherwise, there could be only cooperation between those entities and Member States that separately trust each other. According to Demaison (2017), the trust in not build in a year or two. It is built with coherent and constant step by step cooperation.



## 6.2 Opportunities

Despite all challenges mentioned in this thesis, it is extremely good that the EU has taken the major step onwards with the NIS Directive. Some could say “finally” when it was first proposed already in 2013. When imaging all the threats mentioned in chapter three (and those not mentioned) there are loads of attractive possibilities for attackers to perceive various types of threats in the modern and in the future cyber space. The threat landscape is evolving fast and due to complexity of internet cost-benefit relation favours perpetrators making attacking even more attractive. Attacks will continue, and it will become even harder for individual organisations to tackle cyber threats on their own. Therefore, cooperation could ease the situation for many, both on public and private sector.

Overall, it is good to do something than nothing at all. Despite all expressed challenges, the NIS Directive responds to the need of collaboration. It obligates organisations to achieve higher level of security. Especially, critical infrastructure is vital to have in scope. The need for collaboration originates from more intense cyber space where attackers openly share effective means. Sharing is crucial to be conducted on defensive side too because together better results in security can be achieved. If vulnerabilities, incidents and best-practices are shared they would benefit critical infrastructure as a whole. Certainly, these should be done in respect of the data and any concerns regarding to confidentiality should be clarified. It may not be easy, but it surely is significant.

The NIS Directive affects all around Europe, and most likely beyond. How challenges will be overcome remains seen. Though, it appears that cooperation within Europol against cybercrime has been somewhat successful. Probably with their example, the cyber security cooperation that has not been done in the same scale before, could work as well. It is interesting to see how proposed strengthen role of ENISA will change cooperation since it could become as strong (or weak) as any other EU agency.

This thesis consists loads of expressed challenges, but not that many solutions. In the planning phase, there was an idea to have a dedicated chapter for solutions, but it was rejected due to lack of scale and confidence on found sources. Though, there were some exceptions. One is “Recommendations for Public-Private Partnership against Cybercrime” by World Economic Forum (WEF, 2016). Despite they are quite strategic ones, the document provides comparably many recommendations.

However, in ever evolving and accelerating cyber space, threats and attackers evolve in parallel. Therefore, more intensive security cooperation within the Union is obviously needed. It might take a few years for cooperation to become more cost effective which of Digital Single Market should benefit.

International companies should see this as an opportunity. Security should be seen as an enabler to more confident marketplace, not as an obligatory villain.

### **6.3 Future Research**

There areas that this research was not able to cover. The following list of subjects have come in to mind as opportunities for future research. They are in random order.

Regarding to threats, it could interesting area to explore what different motivations threat-makers might have against the EU or individual Member States, or are there specifically any. Understanding them could help to understand how to defend against them or what cures there could be, such as education.

Surrounding new documents and guidelines will most likely change the cooperation. Deeper exploration on them and other supporting documents could be rewarding. Therefore, it could be good to have a similar type of research in a few years.

Significant are to explore would be how national implementation of the NIS Directive proceeds. This research was done when OES and DSPs were not yet nominated. This could change the whole spectrum around the NIS Directive. Probably, with increase of legal perspective could be affordable.

This research did not focus on civil-military cooperation which certainly could be interesting and valuable area to research. Additionally, based on statistics, what type of numbers will be formed of annual summary reporting compared to previous years, how the cooperation proceeds.

## 7 CONCLUSIONS

Threats and challenges around European cyber security cooperation in the context of European Union directive on security of network and information systems is a complex phenomenon. This thesis was conducted with a qualitative research design, as a case study on the current views regarding to the subject using a pragmatic worldview. This thesis has discussed thoroughly about the subject by providing a view on the current and emerging threat landscape, objectives of the EU on the NIS Directive, and elaborated challenges around it. Based on the research, own views on to the subject were provided in the previous chapter.

Western societies, including the EU, face increasing amount of threats in cyber space. Attackers have plenty of tools to use and their both expertise and technologies evolve. There were only 15 of threat types presented, which represented the most common types of threats. Targets and motives of perpetrators vary. Whether they are cyber criminals, hackers, state-sponsored attackers, insider-threat, or simply script-kiddies, they may cause significant harm in the worst-case scenario. Too often, critical infrastructure, such as healthcare, transport and telecommunications or financial institutions are being targeted. No matter if in purpose or without, incidents may cause serious problems. It is very likely that more intensive trend in threats will remain. The threats create need for cyber security cooperation that the NIS Directive aims to respond.

The NIS Directive could ease the situation against threats. It is an unprecedented regulative document which objective is to increase cooperation in cyber space across the EU. There are plenty of requirements for public and private sector, especially those regarding to critical infrastructure. There are plenty of organisations belonging under OES or DSPs, where purpose is to guarantee workability of Digital Single Market despite attacks. Also, voluntary notification is possible for those not belonging to either of the group. Some of the requirements are broad and, as a directive, it leaves room for Member States to apply the Directive on their own. OES and DSPs must report of major incidents to national competent authorities. OES, DSPs, national competent

authorities and national CSIRTs cooperate on national level. CSIRT network and Cooperation Group, with support of ENISA and the Commission, are about to deal on European level in improving the cooperation, and Cooperation Group could have international stakeholders within when appropriate. As there are broad requirements in the NIS Directive and many variations to implement it, challenges of the Directive have been enunciated.

Regarding to challenges, there were seven types of groups identified in this research. There could have more of them, or some could have grouped together. However, the seven types were the following. (1) Directive type of regulation enables different approaches onto the NIS Directive by Member States. It is in contrary with the objective of harmonisation of the NIS Directive. Simultaneously, there is lack of coherence in European politics and security views, some Member States does not consider the EU as a security actor which does not bolster the objectives of the NIS Directive. Coherence and common values are vital for effective cooperation. (2) Maturity level and resources vary. Some Member States have incident response activity before others. For reaching higher maturity, investments are needed. Right people should be hired. Sometimes these are hard to get. (3) Trust must be gained, and language must be equalised. If there is no trust, there is no cooperation. If there is cooperation, the same language must be spoken. (4) Confidentiality is emphasised. There should be clear policies and guidelines for operations to avoid any possible leaks in reporting. Also, reporting thresholds would need further clarifications. (5) Identification of entities do vary when an organisation could be part of the OES in one, whereas not necessarily in another. Member States have also taken many different approaches on designating competent authorities for OES. Even Member State with same size do have variations between each other. Once again, this is contrary to the harmonisation goal and makes it difficult to track applications of the NIS Directive. (6) Compliance and sanctions are different in different Member States. The ways of seeing compliance vary. Sanctions are across Member States and this could due to different economical level, though, some Member States apply only existing laws, whereas others have major fines on severe cases. (7) There are elements that are left out of scope. Vital parts in cyber chain, such as hardware manufacturers and software developers, are out scoped. Cybersecurity Act may take stand on this in the future, regardless that it might be voluntary. It can also be questioned whether not all processes should be digitalised to gain extremely proofed cyber security.

Consequently, it can be argued that there are plenty of challenges around the cyber security cooperation. Though, to actively and effectively response on threats, cooperation should get working. It could become extremely valuable tool that could save from many economical and reputational disasters or even save lives. It may take time to reach the "high common level of security" but with constant interaction, tactical, operational and strategical cooperation the objective may be achievable.

In conclusion, there must be trust among different entities as described by many in the EU Cyber Security Conference in 2017 (EU2017EE, 2017). To gain

trust, the EU cannot be fragmented. Instead, according to Carrapico and Barrinha (2017), there must be common values – coherence – that drives towards common goals. Even with these two principles, Member States, cyber security cooperation and the Digital Single Market would already have a giant leap forward.

## REFERENCES

- Acunetix. (2018). What is a web application attack and how to defend against it. Retrieved from <https://www.acunetix.com/websitesecurity/web-application-attack/>
- Alexander, D. (2012). Cyber Threats in the 21st Century. *Security: Solutions for Enterprise Security Leaders*, 49(9), 70-76. Retrieved from <http://search.ebscohost.com/login.aspx?direct=true&db=buh&AN=79461978&site=eds-live>
- Alton, L. (2018). Cyber-Espionage: A Bigger Problem than We Realize. *American Thinker*, (18 April 2018). Retrieved from [https://www.americanthinker.com/articles/2018/04/cyberespionage\\_a\\_bigger\\_problem\\_than\\_we\\_realize.html](https://www.americanthinker.com/articles/2018/04/cyberespionage_a_bigger_problem_than_we_realize.html)
- ANSSI (Agence nationale de la sécurité des systèmes D'information). (2014). *Passeport de conseils aux voyageurs*. ANSSI (Agence nationale de la sécurité des systèmes D'information). Retrieved from [https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport\\_voyageurs\\_anssi.pdf](https://www.ssi.gouv.fr/uploads/IMG/pdf/passeport_voyageurs_anssi.pdf)
- BBC. (2017). Equifax says almost 400,000 Britons hit in data breach, 15 September 2017. Retrieved October 21, 2018, from <https://www.bbc.com/news/technology-41286638>
- BBVA. (2016). The Network and Information Security (NIS) Directive. Part 2 of 2. *Digital Economy Outlook*, (May). Retrieved from [https://www.bbvaresearch.com/wp-content/uploads/2016/05/DEO\\_May16\\_Cap3.pdf](https://www.bbvaresearch.com/wp-content/uploads/2016/05/DEO_May16_Cap3.pdf)
- Bell, J. (2010). *Doing Your Research Project* (5th ed.). Maidenhead: McGraw-Hill Open University Press.
- Berr, J. (2017). "WannaCry" ransomware attack losses could reach \$4 billion. Retrieved October 20, 2018, from <https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/>
- Bickerstaff, R., Niemann, F., Schüßler, L., & Shooter, S. (2016). NIS Directive: New Security and Reporting Requirements for Infrastructure Providers and certain Digital Businesses, 08 July 2016. Retrieved August 17, 2018, from <https://www.twobirds.com/en/news/articles/2016/global/new->

security-and-reporting-requirements-for-infrastructure-providers-and-certain-digital-businesses

- Billois, G., Capgras, É., Joubert, T., & Lyonnet, E. (2017). CYBERSECURITY AND THE NIS DIRECTIVE: THE EUROPEAN UNION FACED WITH A NEW DUTY OF CONSISTENCY. *Wavestone: Riskinsight*. Retrieved from <https://www.wavestone.com/app/uploads/2017/02/cybersecurity-nis-directive-europe-1.pdf>
- Bird & Bird. (2018). Sanctions regime. Retrieved October 29, 2018, from <https://www.twobirds.com/en/in-focus/cybersecurity/nisd-tracker/country-comparison-by-topic/sanctions-regime>
- Braun, V., & Clarke, V. (2013). *Successful Qualitative Research: A Practical Guide for Beginners*. London: Sage.
- Bryman, A. (2011). *Social Research Methods* (4th ed.). New York: Oxford University Press.
- Bures, O. (2017). Contributions of private businesses to the provision of security in the EU: beyond public-private partnerships. *Crime, Law and Social Change*, 67(3), 289–312. <https://doi.org/10.1007/s10611-016-9650-6>
- Carrapico, H., & Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. *European Politics and Society*, 19(3), 299–303. <https://doi.org/10.1080/23745118.2018.1430712>
- Carrapico, H., & Barrinha, A. (2017). The EU as a Coherent (Cyber)Security Actor? *Journal of Common Market Studies*, 55(6), 1254–1272. <https://doi.org/10.1111/jcms.12575>
- CERT-UK. (2015). *Phishing: What is it and how does it affect me?* Retrieved from <https://www.northhampshireccg.nhs.uk/wp-content/uploads/2015/07/Phishing-in-the-UK-1.pdf>
- Chantzou, I. (2017). EU Cyber Security Conference: The challenges of operational cooperation in Europe, 14 September 2017. Retrieved August 25, 2018, from <https://www.youtube.com/watch?v=8na0j2KzkwE>
- Council of the European Union. (2018). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”) – General Approach. Retrieved from <https://data.consilium.europa.eu/doc/document/ST-9350-2018-INIT/en/pdf>

- Creswell, J. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (3rd ed.). Los Angeles: Sage.
- Demaison, J. (2017). EU Cyber Security Conference: The challenges of operational cooperation in Europe, 14 September 2017. Retrieved August 25, 2018, from <https://www.youtube.com/watch?v=8na0j2KzkwE>
- Dennison, S., Franke, U. E., & Zerka, P. (2018). *Security Scorecard: The Nightmare of the Dark* (July). European Council on Foreign Relations.
- Eltzholtz, K. L. (2017). *Cooperation in European Cyber Security: An International Relations Perspective on Collective Cyber Security in the European Union*. Aalborg University. Aalborg University. Retrieved from [https://projekter.aau.dk/projekter/files/260246274/Thesis\\_2017\\_\\_Kristian\\_Linnet\\_Eltzholtz.pdf](https://projekter.aau.dk/projekter/files/260246274/Thesis_2017__Kristian_Linnet_Eltzholtz.pdf)
- ENHESA. (2014). EU Directive vs EU Regulation: What's The Difference? Retrieved October 29, 2018, from <http://www.enhesa.com/blog/eu-directive-vs-eu-regulation-whats-difference?language=en>
- ENISA (European Union Agency for Network and Information Security). (2017). *Communication network dependencies for ICS/SCADA Systems*. Retrieved from <https://www.enisa.europa.eu/publications/ics-scada-dependencies>
- ENISA (European Union Agency for Network and Information Security). (2018). *ENISA threat landscape report 2017 - EU Law and Publications*. <https://publications.europa.eu/en/publication-detail/-/publication/d4d64bd6-0af1-11e8-966a-01aa75ed71a1/language-en/format-PDF/source-66667278>
- EU2017EE. (2017). EU Cyber Security Conference, Tallinn, 14-15 September 2017. Tallinn: EU2017EE. Retrieved from <https://www.eu2017.ee/political-meetings/eu-cyber-security-conference-digital-single-market-common-digital-security-2017>
- European Commission. (2013). JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. *European Commission*, 20. [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=1667](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667)
- European Commission. (2014). EU position in world trade. Retrieved October 29, 2018, from <http://ec.europa.eu/trade/policy/eu-position-in-world-trade/>



- European Commission. (2017a). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the “EU Cybersecurity Agency”, and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification (“Cybersecurity Act”), 0225 § (2017). Retrieved from <http://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF>
- European Commission. (2017b). COMMISSION RECOMMENDATION (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises. *Official Journal of the European Union*, L 239(36), 7. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN>
- European Commission. (2018a). The Directive on security of network and information systems (NIS Directive). Retrieved August 30, 2018, from <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>
- European Commission. (2018b). State-of-play of the transposition of the NIS Directive. Retrieved September 7, 2018, from <https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive>
- European Council & Council of the European Union. (2018). EU to create a common cybersecurity certification framework and beef up its agency – Council agrees its position, 08 June 2018. Retrieved October 27, 2018, from <https://www.consilium.europa.eu/en/press/press-releases/2018/06/08/eu-to-create-a-common-cybersecurity-certification-framework-and-beef-up-its-agency-council-agrees-its-position/>
- European Political Strategy Centre. (2017). Building an Effective European Cyber Shield. *European Commission*, (24), 16. [http://ec.europa.eu/epsc/sites/epsc/files/strategic\\_note\\_issue\\_24.pdf](http://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf)
- European Union. (1992). Treaty on European Union: Treaty of Maastricht. *Official Journal of the European Communities*, C 325(5). [http://europa.eu/eu-law/decision-making/treaties/pdf/treaty\\_on\\_european\\_union/treaty\\_on\\_european\\_union\\_en.pdf](http://europa.eu/eu-law/decision-making/treaties/pdf/treaty_on_european_union/treaty_on_european_union_en.pdf)
- European Union. (2012). CONSOLIDATED VERSION OF THE TREATY ON THE FUNCTIONING OF THE EUROPEAN UNION. *Official Journal of the European Union*, 326(47). <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN>

- European Union. (2016a). Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. *Official Journal of the European Union*, L 194. <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>
- European Union. (2016b). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*, L 119. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&qid=1538077699574&from=EN>
- Europol (European Union Agency for Law Enforcement Cooperation). (2018). *Internet Organised Crime Threat Assessment (IOCTA)*. European Union Agency for Law Enforcement Cooperation. [https://www.europol.europa.eu/sites/default/files/documents/iocta\\_2018\\_0.pdf](https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf)
- Evans, M., & White, L. (2016). NIS Directive Published: EU Member States Have Just Under Two Years to Implement, 21 July 2016. Retrieved August 16, 2018, from <https://www.dataprotectionreport.com/2016/07/nis-directive-published-eu-member-states-have-just-under-two-years-to-implement/>
- Experian. (2017). Fourth annual 2017 data breach industry forecast. Retrieved from <http://www.experian.com/assets/data-breach/white-papers/2017-experian-data-breach-industry-forecast.pdf>
- Fisher, T. (2018). What Is Malware? Malware: What it means, common types, & how to deal with it. *Lifewire*, (January 16, 2018). Retrieved from <https://www.lifewire.com/what-is-malware-2625933>
- GCSP. (2017). Cyber 9/12 Student Challenge 2017, Geneva, 20-21 April 2017. Retrieved from <https://www.gcsp.ch/Events/Cyber-9-12-Student-Challenge-2017>
- Gressin, S. (2017). The Equifax Data Breach: What to Do, 8 September 2017. Retrieved October 14, 2018, from <https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do>

- Grigoras, M. (2017). EU Cyber Security Conference: The challenges of operational cooperation in Europe, 14 September 2017. Retrieved August 25, 2018, from <https://www.youtube.com/watch?v=8na0j2KzkwE>
- Hadwin, S. (2018). UK NIS Regulations impose new cybersecurity obligations (and a new penalties regime) on operators of essential services and digital service providers in the UK, 10 May 2018. Retrieved October 28, 2018, from <https://www.dataprotectionreport.com/2018/05/uk-nis-regulations-impose-new-cybersecurity-obligations-and-a-new-penalties-regime-on-operators-of-essential-services-and-digital-service-providers-in-the-uk/>
- Hellwig, O., Quirchmayr, G., Huber, E., Goluch, G., Vock, F., & Pospisil, B. (2016). Major challenges in structuring and institutionalizing CERT-communication. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, (2), 661-667. <https://doi.org/10.1109/ARES.2016.57>
- Holzleitner, M.-T., & Reichl, J. (2017). European provisions for cyber security in the smart grid - an overview of the NIS-directive. *Elektrotechnik Und Informationstechnik*, 134(1), 14-18. <https://doi.org/10.1007/s00502-017-0473-7>
- Hunt, T. (2017). Everything you need to know about the WannaCry / Wcry / WannaCrypt ransomware, 13 May 2017. Retrieved October 21, 2018, from <https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/>
- Ilves, L., Evans, T., Cilluffo, F., & Nadeau, A. (2016). European Union and NATO Global Cybersecurity Challenges - A Way Forward. *Prism*, 6(2), 126-142. Retrieved from <http://cco.ndu.edu/News/Article/840755/european-union-and-nato-global-cybersecurity-challenges-a-way-forward/>
- Karsberg, C. (2017). EU Cyber Security Conference: The challenges of operational cooperation in Europe, 14 September 2017. Retrieved August 25, 2018, from <https://www.youtube.com/watch?v=8na0j2KzkwE>
- Kaskina, B. (2017). How the European Union is tackling cybersecurity: a look at the NIS directive. Retrieved August 17, 2018, from <https://news.itu.int/eu-cybersecurity-nis-directive/>
- Kaspersky Lab. (2018). What is spam? Retrieved May 15, 2018, from <https://securelist.com/threats/what-is-spam/>
- Kharif, O. (2017). 2016 Was a Record Year for Data Breaches, 19 January 2017. Retrieved October 20, 2018, from

<https://www.bloomberg.com/news/articles/2017-01-19/data-breaches-hit-record-in-2016-as-dnc-wendy-s-co-hacked>

- Leary, J. (2018). Equifax Breach Impacts 147.9 Million: Steps to Keep Your Identity Protected, 11 May 2018. Retrieved October 20, 2018, from <https://www.identityforce.com/business-blog/equifax-breach-impacts-143-million-steps-to-keep-your-identity-protected>
- Lehto, M. (2015). Kybermaailma ja turvallisuus 16.-17.1.2015. In *ITKST41 Kybermaailma ja turvallisuus*. University of Jyväskylä, unpublished.
- Levin, B., & Simpson, D. (2018a). Ransomware, 17 August 2018. Retrieved October 13, 2018, from <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/ransomware-malware>
- Levin, B., & Simpson, D. (2018b). Exploits and exploit kits, 17 August 2018. Retrieved October 20, 2018, from <https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/exploits-malware>
- Long, W. (2014). What to expect from Europe's NIS Directive. Retrieved October 27, 2018, from <https://www.computerweekly.com/opinion/What-to-expect-from-European-NIS-Directive>
- Malwarebytes. (2018). All about ransomware. Retrieved October 13, 2018, from <https://www.malwarebytes.com/ransomware/>
- Malwarebytes Labs. (2017a). Petya-esque ransomware is spreading across the world, 13 December 2017. Retrieved October 21, 2017, from <https://blog.malwarebytes.com/cybercrime/2017/06/petya-esque-ransomware-is-spreading-across-the-world/>
- Malwarebytes Labs. (2017b). BadRabbit ransomware strikes Eastern Europe, 13 December 2017. Retrieved October 20, 2018, from <https://blog.malwarebytes.com/cybercrime/2017/10/badrabbit-ransomware-strikes-eastern-europe/>
- NCSC (National Cyber Security Centre); NCA (National Crime Agency). (2018). *The cyber threat to UK business: 2017-2018 Report*. Crown. Retrieved from [https://www.ncsc.gov.uk/content/files/protected\\_files/article\\_files/ncsc\\_nca\\_report.pdf](https://www.ncsc.gov.uk/content/files/protected_files/article_files/ncsc_nca_report.pdf)
- Newman, L. H. (2017). The Biggest Cybersecurity Disasters of 2017 So Far, 01 July 2017. Retrieved October 21, 2018, from <https://www.wired.com/story/2017-biggest-hacks-so-far/>

- Niebler, A. (2018). EU can become a leading player in cybersecurity. *The Parliament Magazine*, (June). Retrieved from <https://www.theparliamentmagazine.eu/printpdf/8008>
- ODNI (Office of the Director of National Intelligence). (2013). *U.S. Insider Threat Security Classification Guide*. Retrieved from <https://www.dni.gov/files/documents/FOIA/DF-2016-00161.pdf>
- Olavsrud, T. (2017). 5 data breach predictions for 2017, 9 January 2017. Retrieved May 20, 2018, from <https://www.cio.com/article/3155724/security/5-data-breach-predictions-for-2017.html>
- Orlowski, A. (2016). Meet DDoSaaS: Distributed Denial of Service-as-a-Service: Cracking the grey market in rent-a-borkers. *The Register*. Retrieved from [https://www.theregister.co.uk/2016/09/12/denial\\_of\\_service\\_as\\_a\\_service/](https://www.theregister.co.uk/2016/09/12/denial_of_service_as_a_service/)
- Palo Alto Networks. (2018). What is a Denial of Service Attack (DoS)?: An Overview of DoS Attacks. Retrieved from <https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos>
- Petri, A. (2017). EU Cyber Security Conference: The challenges of operational cooperation in Europe, 14 September 2017. Retrieved August 25, 2018, from <https://www.youtube.com/watch?v=8na0j2KzkwE>
- Pollari, J. (2017). *Tietoturvallisuuden hallintamallin kehittäminen*. Savonia University of Applied Sciences. Savonia University of Applied Sciences. Retrieved from [https://www.theseus.fi/bitstream/handle/10024/131992/Pollari\\_Janne.pdf?sequence=1&isAllowed=y](https://www.theseus.fi/bitstream/handle/10024/131992/Pollari_Janne.pdf?sequence=1&isAllowed=y)
- Purser, S. (2016). Implementing The NIS Directive. In *NLO Meeting, Athens, European Union Agency for Network and Information Security (ENISA)*. Retrieved from <https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/meetings/june-2016/nis-directive-nlo-meeting.pdf>
- Purser, S. (2017). EU Cyber Security Conference: The challenges of operational cooperation in Europe, 14 September 2017. Retrieved August 25, 2018, from <https://www.youtube.com/watch?v=8na0j2KzkwE>
- Rantala, J. (2017). *NIS-direktiivin kahdet kasvot - riskit ja riskienhallinta*. University of Jyväskylä. University of Jyväskylä. Retrieved from <https://jyx.jyu.fi/dspace/bitstream/handle/123456789/55810/URN%3ANBN%3Afi%3Aju-201711084172.pdf?sequence=1>

- Renard, T. (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society*, 19(3), 321–337. <https://doi.org/10.1080/23745118.2018.1430720>
- RFSID. (2017). How Can Threat Intelligence Help the Cyber Attack Kill Chain? Retrieved October 21, 2018, from <https://www.recordedfuture.com/cyber-attack-kill-chain/>
- RFSID. (2016). Proactive Defense: Understanding the 4 Main Threat Actor Types, 23 August 2016. Retrieved October 21, 2018, from <https://www.recordedfuture.com/threat-actor-types/>
- Samee, S. (2017). Identity fraud soars to new levels. Retrieved October 14, 2018, from <https://www.cifas.org.uk/newsroom/identity-fraud-soars-to-new-levels>
- Saraste, A. (2018). Uusi kyberraportti Saksasta varoittaa: hakkerit voisivat pimentää koko Euroopan sähköverkon, 25 August 2018. Retrieved October 21, 2018, from <https://yle.fi/uutiset/3-10369841>
- Schaake, M. (2018). Dutch Foreign Ministry warns citizens to only take ‘empty’ devices... Retrieved from <https://twitter.com/marietjeschaake/status/983227640885796864?s=12>
- Sears, O. (2017). What is a Web-based Data Breach And Why Law Firms Should Care. *Ntrepid Corporation*, (September 13, 2017). Retrieved from <https://ntrepidcorp.com/general/web-based-data-breach-law-firms-care/>
- Sherr, I. (2017). WannaCry ransomware: Everything you need to know, 19 May 2017. Retrieved October 20, 2018, from <https://www.cnet.com/news/wannacry-wannacrypt-uiwix-ransomware-everything-you-need-to-know/>
- Surguy, M. (2017). The NIS Directive and the potential for European Member State cooperation, 22 September 2017. Retrieved August 15, 2018, from <https://www.weightmans.com/insights/the-nis-directive-and-the-potential-for-european-member-state-cooperation/#>
- Symantec. (2009). White Paper: Web Based Attacks. *Prevention*, (February). Retrieved from [http://eval.symantec.com/mktginfo/enterprise/white\\_papers/b-whitepaper\\_web\\_based\\_attacks\\_03-2009.en-us.pdf](http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_web_based_attacks_03-2009.en-us.pdf)
- Trend-Micro. (2017). 2017 Midyear Security Roundup: The Cost of Compromise - Security Roundup - Trend Micro USA. Retrieved from

<https://documents.trendmicro.com/assets/rpt/rpt-2017-Midyear-Security-Roundup-The-Cost-of-Compromise.pdf>

- U.S. Department of Justice. (2018). What Are Identity Theft and Identity Fraud? Retrieved October 14, 2018, from <https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud>
- United Nations. (2015). A/70/174: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. *General Assembly, 12404*(July). Retrieved from [http://www.un.org/ga/search/view\\_doc.asp?symbol=A/70/174](http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174)
- Walker, J. (2018). Information leakage: The most misunderstood security risk. Retrieved October 20, 2018, from <https://www.isaca.org/Knowledge-Center/Blog/Lists/Posts/Post.aspx?ID=24>
- van Zadelhoff, M. (2016). The Biggest Cybersecurity Threats Are Inside Your Company, 19 September 2016. Retrieved October 20, 2018, from <https://hbr.org/2016/09/the-biggest-cybersecurity-threats-are-inside-your-company>
- WEF. (2016). Recommendations for Public-Private Partnership against Cybercrime. *World Economic Forum*, (January), 12. Retrieved from [http://www3.weforum.org/docs/WEF\\_Cybercrime\\_Principles.pdf](http://www3.weforum.org/docs/WEF_Cybercrime_Principles.pdf)
- Verizon. (2018). 2018 Data breach investigations report. *Trends*, 1–62. Retrieved from [https://www.verizonenterprise.com/resources/reports/rp\\_DBIR\\_2018\\_Report\\_execsummary\\_en\\_xg.pdf](https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf)
- White Hat Security. (2018). Information Leakage. Retrieved October 20, 2018, from <https://www.whitehatsec.com/glossary/content/information-leakage>
- Vincent, E. (2018). Countdown to the NIS Directive: The Challenges of Compliance. Retrieved September 24, 2018, from <https://blog.wallix.com/nis-directive-challenges-of-compliance>
- Yin, R. (2009). *Case Study Research: Design and Methods* (4th ed.). Los Angeles: Sage.
- YLE. (2018). Supo: Cyber spying, traditional espionage, terrorism threat continue. YLE. Retrieved from [https://yle.fi/uutiset/osasto/news/supo\\_cyber\\_spying\\_traditional\\_espionage\\_terrorism\\_threat\\_continue/10126028](https://yle.fi/uutiset/osasto/news/supo_cyber_spying_traditional_espionage_terrorism_threat_continue/10126028)

## APPENDIX I: THE NIS DIRECTIVE ANNEX I: REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

### ANNEX I

#### REQUIREMENTS AND TASKS OF COMPUTER SECURITY INCIDENT RESPONSE TEAMS (CSIRTs)

The requirements and tasks of CSIRTs shall be adequately and clearly defined and supported by national policy and/or regulation. They shall include the following:

- (1) Requirements for CSIRTs:
    - (a) CSIRTs shall ensure a high level of availability of their communications services by avoiding single points of failure, and shall have several means for being contacted and for contacting others at all times. Furthermore, the communication channels shall be clearly specified and well known to the constituency and cooperative partners.
    - (b) CSIRTs' premises and the supporting information systems shall be located in secure sites.
    - (c) Business continuity:
      - (i) CSIRTs shall be equipped with an appropriate system for managing and routing requests, in order to facilitate handovers.
      - (ii) CSIRTs shall be adequately staffed to ensure availability at all times.
      - (iii) CSIRTs shall rely on an infrastructure the continuity of which is ensured. To that end, redundant systems and backup working space shall be available.
    - (d) CSIRTs shall have the possibility to participate, where they wish to do so, in international cooperation networks.
  - (2) CSIRTs' tasks:
    - (a) CSIRTs' tasks shall include at least the following:
      - (i) monitoring incidents at a national level;
      - (ii) providing early warning, alerts, announcements and dissemination of information to relevant stakeholders about risks and incidents;
      - (iii) responding to incidents;
      - (iv) providing dynamic risk and incident analysis and situational awareness;
      - (v) participating in the CSIRTs network.
    - (b) CSIRTs shall establish cooperation relationships with the private sector.
    - (c) To facilitate cooperation, CSIRTs shall promote the adoption and use of common or standardised practices for:
      - (i) incident and risk-handling procedures;
      - (ii) incident, risk and information classification schemes.
-



## APPENDIX II: THE NIS DIRECTIVE ANNEX II: DEFINITIONS OF OPERATORS OF ESSENTIAL SERVICES

### ANNEX II

#### TYPES OF ENTITIES FOR THE PURPOSES OF POINT (4) OF ARTICLE 4

Sector	Subsector	Type of entity
1. Energy	(a) Electricity	— Electricity undertakings as defined in point (35) of Article 2 of Directive 2009/72/EC of the European Parliament and of the Council <sup>(1)</sup> , which carry out the function of 'supply' as defined in point (19) of Article 2 of that Directive
		— Distribution system operators as defined in point (6) of Article 2 of Directive 2009/72/EC
		— Transmission system operators as defined in point (4) of Article 2 of Directive 2009/72/EC
	(b) Oil	— Operators of oil transmission pipelines
		— Operators of oil production, refining and treatment facilities, storage and transmission
	(c) Gas	— Supply undertakings as defined in point (8) of Article 2 of Directive 2009/73/EC of the European Parliament and of the Council <sup>(2)</sup>
		— Distribution system operators as defined in point (6) of Article 2 of Directive 2009/73/EC
		— Transmission system operators as defined in point (4) of Article 2 of Directive 2009/73/EC
		— Storage system operators as defined in point (10) of Article 2 of Directive 2009/73/EC
		— LNG system operators as defined in point (12) of Article 2 of Directive 2009/73/EC
		— Natural gas undertakings as defined in point (1) of Article 2 of Directive 2009/73/EC
		— Operators of natural gas refining and treatment facilities
	2. Transport	(a) Air transport
— Airport managing bodies as defined in point (2) of Article 2 of Directive 2009/12/EC of the European Parliament and of the Council <sup>(4)</sup> , airports as defined in point (1) of Article 2 of that Directive, including the core airports listed in Section 2 of Annex II to Regulation (EU) No 1315/2013 of the European Parliament and of the Council <sup>(5)</sup> , and entities operating ancillary installations contained within airports		

Sector	Subsector	Type of entity
		— Traffic management control operators providing air traffic control (ATC) services as defined in point (1) of Article 2 of Regulation (EC) No 549/2004 of the European Parliament and of the Council <sup>(6)</sup>
	(b) Rail transport	— Infrastructure managers as defined in point (2) of Article 3 of Directive 2012/34/EU of the European Parliament and of the Council <sup>(7)</sup>
		— Railway undertakings as defined in point (1) of Article 3 of Directive 2012/34/EU, including operators of service facilities as defined in point (12) of Article 3 of Directive 2012/34/EU
	(c) Water transport	— Inland, sea and coastal passenger and freight water transport companies, as defined for maritime transport in Annex I to Regulation (EC) No 725/2004 of the European Parliament and of the Council <sup>(8)</sup> , not including the individual vessels operated by those companies
		— Managing bodies of ports as defined in point (1) of Article 3 of Directive 2005/65/EC of the European Parliament and of the Council <sup>(9)</sup> , including their port facilities as defined in point (11) of Article 2 of Regulation (EC) No 725/2004, and entities operating works and equipment contained within ports
		— Operators of vessel traffic services as defined in point (o) of Article 3 of Directive 2002/59/EC of the European Parliament and of the Council <sup>(10)</sup>
	(d) Road transport	— Road authorities as defined in point (12) of Article 2 of Commission Delegated Regulation (EU) 2015/962 <sup>(11)</sup> responsible for traffic management control
		— Operators of Intelligent Transport Systems as defined in point (1) of Article 4 of Directive 2010/40/EU of the European Parliament and of the Council <sup>(12)</sup>
3. Banking		Credit institutions as defined in point (1) of Article 4 of Regulation (EU) No 575/2013 of the European Parliament and of the Council <sup>(13)</sup>
4. Financial market infrastructures		— Operators of trading venues as defined in point (24) of Article 4 of Directive 2014/65/EU of the European Parliament and of the Council <sup>(14)</sup>
		— Central counterparties (CCPs) as defined in point (1) of Article 2 of Regulation (EU) No 648/2012 of the European Parliament and of the Council <sup>(15)</sup>
5. Health sector	Health care settings (including hospitals and private clinics)	Healthcare providers as defined in point (g) of Article 3 of Directive 2011/24/EU of the European Parliament and of the Council <sup>(16)</sup>

Sector	Subsector	Type of entity
6. Drinking water supply and distribution		Suppliers and distributors of water intended for human consumption as defined in point (1)(a) of Article 2 of Council Directive 98/83/EC <sup>(17)</sup> but excluding distributors for whom distribution of water for human consumption is only part of their general activity of distributing other commodities and goods which are not considered essential services
7. Digital Infrastructure		— IXPs
		— DNS service providers
		— TLD name registries

<sup>(1)</sup> Directive 2009/72/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC (OJ L 211, 14.8.2009, p. 55).

<sup>(2)</sup> Directive 2009/73/EC of the European Parliament and of the Council of 13 July 2009 concerning common rules for the internal market in natural gas and repealing Directive 2003/55/EC (OJ L 211, 14.8.2009, p. 94).

<sup>(3)</sup> Regulation (EC) No 300/2008 of the European Parliament and of the Council of 11 March 2008 on common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002 (OJ L 97, 9.4.2008, p. 72).

<sup>(4)</sup> Directive 2009/12/EC of the European Parliament and of the Council of 11 March 2009 on airport charges (OJ L 70, 14.3.2009, p. 11).

<sup>(5)</sup> Regulation (EU) No 1315/2013 of the European Parliament and of the Council of 11 December 2013 on Union guidelines for the development of the trans-European transport network and repealing Decision No 661/2010/EU (OJ L 348, 20.12.2013, p. 1).

<sup>(6)</sup> Regulation (EC) No 549/2004 of the European Parliament and of the Council of 10 March 2004 laying down the framework for the creation of the single European sky (the framework Regulation) (OJ L 96, 31.3.2004, p. 1).

<sup>(7)</sup> Directive 2012/34/EU of the European Parliament and of the Council of 21 November 2012 establishing a single European railway area (OJ L 343, 14.12.2012, p. 32).

<sup>(8)</sup> Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security (OJ L 129, 29.4.2004, p. 6).

<sup>(9)</sup> Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security (OJ L 310, 25.11.2005, p. 28).

<sup>(10)</sup> Directive 2002/59/EC of the European Parliament and of the Council of 27 June 2002 establishing a Community vessel traffic monitoring and information system and repealing Council Directive 93/75/EEC (OJ L 208, 5.8.2002, p. 10).

<sup>(11)</sup> Commission Delegated Regulation (EU) 2015/962 of 18 December 2014 supplementing Directive 2010/40/EU of the European Parliament and of the Council with regard to the provision of EU-wide real-time traffic information services (OJ L 157, 23.6.2015, p. 21).

<sup>(12)</sup> Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport (OJ L 207, 6.8.2010, p. 1).

<sup>(13)</sup> Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 (OJ L 176, 27.6.2013, p. 1).

<sup>(14)</sup> Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (OJ L 173, 12.6.2014, p. 349).

<sup>(15)</sup> Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives, central counterparties and trade repositories (OJ L 201, 27.7.2012, p. 1).

<sup>(16)</sup> Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare (OJ L 88, 4.4.2011, p. 45).

<sup>(17)</sup> Council Directive 98/83/EC of 3 November 1998 on the quality of water intended for human consumption (OJ L 330, 5.12.1998, p. 32).

## **APPENDIX III: THE NIS DIRECTIVE ANNEX III: DEFINITIONS OF DIGITAL SERVICE PROVIDERS**

### *ANNEX III*

#### **TYPES OF DIGITAL SERVICES FOR THE PURPOSES OF POINT (5) OF ARTICLE 4**

1. Online marketplace.
  2. Online search engine.
  3. Cloud computing service.
-

## APPENDIX IV: THE NIS DIRECTIVE ARTICLE 4: TERM DEFINITIONS

The NIS Directive definitions for terms, described in article 4, are listed underneath as a citation (bolds and cursives made by the author).

### Article 4

#### Definitions

For the purpose of this Directive, the following definitions apply:

- (1) **'network and information system'** means:
  - a. an *electronic communications network* within the meaning of point (a) of Article 2 of Directive 2002/21/EC;
  - b. any *device or group of interconnected or related devices*, one or more of which, pursuant to a program, perform automatic processing of digital data; or
  - c. digital data *stored, processed, retrieved or transmitted* by elements covered under points (a) and (b) for the purposes of their operation, use, protection and maintenance;
- (2) **'security of network and information systems'** means the ability of network and information systems to *resist*, at a given level of confidence, any action that compromises the *availability, authenticity, integrity or confidentiality* of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems;
- (3) **'national strategy on the security of network and information systems'** means a framework providing strategic objectives and priorities on the security of network and information systems at national level;
- (4) **'operator of essential services'** means a *public or private* entity of a type referred to in Annex II, which meets the criteria laid down in Article 5(2);
- (5) **'digital service'** means a service within the meaning of point (b) of Article 1(1) of Directive (EU) 2015/1535 of the European Parliament and of the Council <sup>(50)</sup> which is of a type listed in Annex III;
- (6) **'digital service provider'** means *any* legal person that provides a digital service;
- (7) **'incident'** means any event having an *actual adverse effect* on the security of network and information systems;
- (8) **'incident handling'** means all procedures supporting the *detection, analysis and containment* of an incident and the response thereto;
- (9) **'risk'** means any reasonably identifiable *circumstance or event* having a potential adverse effect on the security of network and information systems;
- (10) **'representative'** means any natural or legal person established in the Union explicitly designated to *act on behalf of a digital service provider* not established in the Union, which may be addressed by a national competent authority or a CSIRT instead of the digital service provider with regard to the obligations of that digital service provider under this Directive;

---

<sup>50</sup> Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (OJ L 241, 17.9.2015, p. 1).

- (11) '**standard**' means a standard within the meaning of point (1) of Article 2 of Regulation (EU) No 1025/2012;
- (12) '**specification**' means a technical specification within the meaning of point (4) of Article 2 of Regulation (EU) No 1025/2012;
- (13) '**internet exchange point (IXP)**' means a network facility which *enables the interconnection of more than two independent autonomous systems*, primarily for the purpose of facilitating the exchange of internet traffic; an IXP provides interconnection only for autonomous systems; an IXP does not require the internet traffic passing between any pair of participating autonomous systems to pass through any third autonomous system, nor does it alter or otherwise interfere with such traffic;
- (14) '**domain name system (DNS)**' means a hierarchical distributed naming system in a network which *refers queries* for domain names;