UNIVERSITY OF TWENTE

Faculty of Behavioral, Management and Social Sciences (BMS)

European Public Administration – Module 12

Bachelor Thesis

Facing 21st Century Challenges: An Assessment of the EU's Security Provisions in the Light of increasing Cybercrime

---

Author: Zoe Lechner

s1734628

First Supervisor: Dr. Claudio Matera

Second Supervisor: Dr. Martin Rosema

Enschede 06 July 2017 Word Count (excl. references): 19.803

Keywords: Cybersecurity; Cybercrime; NIS; CSDP and AFSJ; EU competences; ENISA; EUCSS

Summary

This research aims at complementing the field of legal studies regarding European cybersecurity policies. Ensuing from the research question to what extent the existing EU regulatory framework on cybercrime is contributing to the security of the Union, this study elaborates on the concepts of cybercrime and cybersecurity to proceed with an analysis of provisions within and beyond the security paradigm of the European Union. Norms and instruments within the CSDP, AFSJ and the internal market are assessed in the light of their contribution to a coherent cybersecurity policy demanded by the Commission in its Cybersecurity Strategy and conclusions are drawn subsequently. For the purpose of conducting this research, a systematic and qualitative literature review will be the method of analysis. Data will be derived mainly from databases of the European Union. The literature comprises normative texts such as case law, primary law and secondary law as well as policy papers. Furthermore, scientific and relevant publications on the state of the art will be reviewed. The EU is stepping up its efforts to protect its cyberspace but is still pursuing a fragmented approach characterized by uncertainties.

Abbreviations

AFSJ	Area of Freedom, Security and Justice
CERT	Computer Emergency Response Teams
CFSP	Common Foreign and Security Policy
CIA-CRIMES	Crimes against the Confidentiality, Integrity and Availability of Data
CSDP	Common Security and Defence Policy
CSIRT	Computer Security Incident Response Team
DSP	Digital Service Provider
EC3	European Cybercrime Center
ECJ	European Court of Justice
EDA	European Defence Agency
EESC	European Economic and Social Committee
ENISA	European Union Agency for Network and Information Security
EPPO	European Public Prosecutor's Office
EU	European Union
EUCSS	Cybersecurity Strategy of the European Union
EUGS	Global Strategy for the European Union's Foreign and Security Policy
HR/VP	High Representative of the Union for Foreign Affairs and Security Policy / Vice President of the Commission [Federica Mogherini]
ICT	Information and Communication Technology
NAC	National Competent Authority
NATO	North Atlantic Treaty Organization
NIS	Network and Information Systems
NIS-DIRECTIVE	Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union

Table of Contents

1 INTRODUCTION ……..1

1.1 Background Information and Theory ..……1

1.2 Scientific and Societal Relevance ……4

1.3 Research Question and Sub-Questions ……5

1.4 Methodology ……5

2 THE CYBERSECURITY REALM AND THE MENACE OF CYBERCRIME ……..8

2.1 The Concept of Cybersecurity and Critical Infrastructure ……...8

2.2 Cybercrime – A known Unknown ……10

2.3 The Budapest Convention on Cybercrime ……12

2.4 Nature and Risk Potential of Cybercrime ……..14

2.5 Conclusions ……16

3 ADVANCING CYBERSECURITY POLICY USING THE EU SECURITY PARADIGM ..18

3.1 Establishing the Legal Basis ……..18

3.2 Defence Provisions within the Common Security and Defence Policy ……..…20

3.2.1 Instruments derived from CSDP Provisions ……..23

3.2.2 Evaluation ……..28

3.3 Law Enforcement within the Area of Freedom Security and Justice …….31

3.3.1 Instruments derived from AFSJ Provisions ……...……35

3.3.2 Evaluation ……..39

3.4 Conclusions and Assessment of the EU Security Paradigm …….…….40

3.4.1 Prospects of the use of a dual legal basis …….……..41

4 CYBERSECURITY PROVISIONS BEYOND THE SECURITY PARADIGM ……43

4.1 The Economic Rationale as a Complement to the Security Paradigm ……...43

4.2 The NIS-Directive ……..44

4.2.1 Evaluation of the NIS-Directive ……47

4.3 The European Network and Information Security Agency ……48

4.3.1 Evaluation of the work of ENISA ……..50

4.4 Conclusions and Assessment ……52

5 CONCLUSION AND FUTURE PERSPECTIVES ……53

6 BIBLIOGRAPHY……..……58

1 INTRODUCTION

1.1 Background Information and Theory

During the last years, the field of security studies experienced considerable transition from traditional security concerns to new focal points among which terrorism, hybrid threats and cybersecurity are perceived as the most eminent. The latter developed in the course of growing interdependence between society and cyberspace and its implications. Alongside with the enormous advantages and innovations it entails, the technological revolution of the 21st century similarly allowed for new criminal activities to develop online and presents governments with enormous challenges. It is estimated that the annual financial loss to global economy from cybercrime was more than $400 billion in 2014 tending upwards every year[1] with important questions about the actual damage inflicted on the victims remaining unanswered. Indeed, cybersecurity failures can cause more than just financial harm; the safety of the society will be threatened if essential services such as energy supply or health services are disturbed. When in May 2017 the ransomware attack *WannaCry* blocked the British National Health Service (NHS),[2] fundamental rights of citizens and the internal security were impugned with minimal logistical efforts. And yet, traditional crime laws and law enforcement provisions are ill-suited to handle these challenges.[3] Cybersecurity therefore found its way into international and European security considerations. The European Union is challenged to prove its capability of reacting against new kinds of security threats with the security of all citizens being a core objective (Article 3(2) TEU) and forming part of the *raison d'être* of the Union. Preserving public trust in the Union's ability to guarantee security in every field therefore is essential and demanded in the face of cybercrime. For a reason cybercrime is included as a prioritized threat to the EU in the European Agenda on Security.[4]

Still, the issue of security concerns and precautions has always existed in an area of tension with the upholding of freedom. Reinforced security measures are often perceived as threatening individual freedoms and rights guaranteed by law. As discussed in other policy areas such as

[1] McAfee, 'Net Losses: Estimating the Global Cost of Cybercrime', *Center for Strategic and International Studies* (June 2014), available at < https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf>.
[2] R. Goldman, 'What We Know and Don't Know About the International Cyberattack', *The New York Times,* 12 May 2017, available at < https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html>.
[3] J. Clough, 'Cybercrime', 37 *Commonwealth Law Bulletin* 2011, at 671.
[4] European Commission, '*Communication from the Commission to the European Parliament, Council, EESC and the Committee of the Regions: The European Agenda on Security*', COM (2015) 185 final, 28.4.2015, at 11.

migration policies the increasing *securitisation* of cyber policy concerns is criticized for overemphasizing security above data protection and privacy.[5] This was intensified by the Edward Snowden revelation in 2013 which exposed 'mass' surveillance of Europeans by US intelligence agencies accentuating questions on the right balance between information gathering and sharing to enforce cybersecurity as well as data protection and privacy.[6] Any EU legislative act taken in the context of cybercrime is therefore to be scrutinized for compatibility with European citizens' freedom and security, in full compliance with the Union's values, including the rule of law and fundamental rights.[7] Making individual rights and security concerns consistent is a major challenge for democratic fundamental principles.

Hence, extensive deliberations on cybercrime and on the security paradigm of the EU are required. In the past years the concerns on cybercrime have incrementally become the focus of attention in several policy areas since the menace to online services ultimately affects all domains of public life and essentially core areas of the Union's mission such as commercial policy, security and freedom in the internal market. In fact, the EU's interest in cybercrime emerged in the first place from economic concerns related to the advancement of the single market through ensuring consumer protection and subsequently trust in electronic commerce.[8] The change from an economic rationale towards a security driven rationale is often associated with the Commission's Communication on *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*[9] containing policy proposals on planned legislative acts.[10] Several policy documents succeeded gradually following different approaches and sub-themes of cybercrime. Only in 2005 the EU

[5] Discussions on whether the EU migration policies have been securitized have been going on in the academic literature for some time, see one of the main publications on the topic by J. Huysmans, 'The European Union and the Securitization of Migration', 38 *Journal of Common Market Studies* 2000, 751-777, available at < http://s3.amazonaws.com/academia.edu.documents/36305135/JCMS_2000.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1498212135&Signature=SH4WXCWbOe%2BocgfpJfmo0IqsLrk%3D&response-content-disposition=inline%3B%20filename%3DThe_European_Union_and_the_securitisatio.pdf>. The question has been raised again after 9/11 and terrorist attacks in London and Madrid, and especially over the course of the Migration Crisis in 2015.

[6] G. Christou, *Cybersecurity in the European Union – Resilience and Adaptability in Governance Policy* (Basingstoke: Palgrave Macmillan 2016), at 144.

[7] European Commission, *supra* note 4, at 3.

[8] H. Carrapiço and B. Farrand, 'The European Union's fight against cybercrime', in M. Fletcher *et al*. (eds.), *The European Union as an Area of Freedom, Security and Justice* (London: Routledge 2017), at 463.

[9] Commission of the European Communities, *'Communication from the Commission to the Council, European Parliament, EESC and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'* COM (2000) 890 final, 26.1.2001.

[10] E. Wennerström, 'EU-legislation and Cybercrime. A Decade of European Legal Developments', 47 *Scandinavian Studies in Law* 2004, at 459.

adopted the first legally binding EU instrument on cyberattacks[11] revealing that, although considered, cyber security was not, until 2005, part of the EU's security priorities.[12] Preeminent is especially the European Cybersecurity Strategy (EUCSS) adopted in 2013 which sets the objectives and the structure of cybersecurity policy.[13] In order to make the "*EU's online environment the safest in the world*" the strategy aims at linking a variety of policy areas and actors to achieve effective and comprehensive cybersecurity policies. In fact, instead of pursuing one 'cover-all' approach cybersecurity is guided by a legal, a security and an economic logic. Concrete measures were subsequently adopted among the Area of Freedom, Security and Justice (AFSJ), the Common Security and Defence Policy (CSDP) and the internal market.

However, the competences of the EU to regulate policy areas are determined in a complex system of distribution of powers. The fundamental principle of conferral laid down in Article 5 Treaty on European Union (TEU) allows the EU to act only where it is provided for in the treaties. Furthermore, powers are determined on the vertical level between the EU and Member States and on the horizontal level between different policies. This construct hampers a comprehensive EU approach and requires a precise analysis of primary law provisions to identify the proper legal basis. Despite the dispersion of powers, the EU has to ensure coherence between these different components to be effective. Since cybersecurity is a complex field surmounting traditional divisions of national and global, internal and external or public and private, policies have to be coordinated while similarly respecting the related legal arrangements. In fact, coherence regarding EU action is highlighted repeatedly and serves as a basis for the development of a strategic vision for security and further institutional reforms.[14] By analyzing the various claims and objectives this thesis shall assess provisions within and beyond the security paradigm to infer to what extent the EU is pursuing an effective and coherent cybersecurity policy.

[11] Council Framework Decision 2005/222/JHA, [*OJ*] L 69/67, 16.3.2005.
[12] H. Carrapiço and B. Farrand, *supra* note 8, at 464.
[13] European Commission, '*Joint Communication to the European Parliament, Council, EESC and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace',* JOIN (2013) 1 final, 7.2.2013.
[14] H. Carrapiço and A. Barrinha, 'The EU as a Coherent (Cyber)Security Actor?', *Journal of Common Market Studies* 2017.

1.2 Scientific and Societal Relevance

This study contributes to the scientific discussion on the division of competences within the European Union, not only regarding the vertical division between Member States and Union but primarily the horizontal division between different policy areas. The analysis shall be used to address the question whether security competences in the Union are clearly and efficiently divided or whether the division ultimately results in loopholes for cybercriminals. From a scientific point of view, it is also useful to examine possible instruments beyond national cooperation and harmonization and eventually the effectiveness of European policy programs.

Primarily this study is of societal relevance since 85 % of European households have access to the internet from home and therefore act in cyberspace.[15] Citizens are concerned about their security in the virtual world while their everyday life is similarly becoming more digitalized. Beyond that, nearly all vital public services are conducted by means of connected computer networks and data. All major areas of public life are to some degree dependent on Information and Communication Technology (ICT) which makes cybersecurity one of the most important topics in the years to come. This is of vital significance in essential services when exemplarily the energy supply is potentially exposed to cyberattacks, menacing the security of society. It is crucial to be prepared at the best before Member States are put to the test by a severe cyberattack. The European Union is demanded to revise the existing framework to adopt to new challenges for maintaining public trust in the EU's ability to provide security and freedom internally, constituted as fundamental objectives in Art.3(2) TEU. Failing to guarantee online security to its citizens affects nearly all 500 million Europeans and would seriously damage the support for further European integration processes. When a new security agenda is to be set in 2020, the Union is advised to effectively condemn cybercrime.

[15] Data on Internet access and use is gathered by *eurostat* in 2016, on <http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_access_and_use_statistics_-_households_and_individuals>.

1.3 Research Question and Sub-Questions

On the basis of these reflections, the following research question *RQ* has been identified: *To what extent is the existing EU regulatory framework on cybercrime contributing to the security of the Union?* Based on the typology of legal research by van Hoecke, this question follows explanatory, empirical, hermeneutic and evaluative approaches.[16] This main research question is supported by several sub-questions:

SQ1: What knowledge is available on how cybercrime is defined, how cyberattacks are conducted and which potential threats these pose towards EU essential services? (Instrumental)

SQ2: How is the correct legal basis for cybersecurity threats to be established in the interplay between the Common Security and Defence Policy and the Area of Freedom, Security and Justice? (Explanatory, Empirical)

SQ3: To what extent does the scope of conferred competences in the field of cybersecurity enable the Union to proceed with legislation and implementation without violating the principle of conferral? (Logical, Explanatory)

SQ4: How does Directive 2016/1148 and its application add to the regulatory framework on enforcing cybersecurity? (Evaluative)

SQ5: Which mandate and possible instruments are awarded ENISA in order to combat cyber criminality? (Evaluative)

1.4 Methodology

As introduced above, this research is conducted from a legal perspective which implies a qualitative and conceptual approach. Given the nature of a legal study, a new enquiry of data is not part of the analysis. Instead, it is based on data deduced mainly from legal, institutional and policy documents. Every chapter focuses after a short introduction on one or two sub-questions on which to elaborate before closing with a preliminary conclusion. In the following, the concrete methodology for each chapter shall be presented.

For the introduction and background information on the topic recent newspaper articles are reviewed to understand the current state of the art on the topic of cybercrime. Additionally, associated EU publications on the topic are included since the analysis will later focus on the EU realm. Especially the EU Cybersecurity Strategy serves as a basis for the first chapter and

[16] M. van Hoecke (ed.), *Methodologies of Legal Research. Which kind of method for what kind of discipline?* (Oxford: Hard Publishing Ltd 2011).

subsequently for the whole analysis since it sets the guidelines for the overall EU cybersecurity approach and determines succeeding policy action. The literature is also groundwork for the understanding of the societal relevance of the issue. To capture the scientific relevance a first overview on academic publications is conducted.

The assessment of the concepts belonging to cybersecurity and their evaluation is covered in chapter 2 and gives answers to *SQ1*. This includes an explicit ascertainment of cybersecurity threats to clarify the imminence originating from cyberattacks as well as the need of EU action. To conceptualize first of all the notions of cybercrime, cybersecurity and essential services a qualitative and systematic literature review of policy papers as well as scientific and relevant publications is deployed. This chapter also grounds on the Budapest Convention as an international law provision for currently applied definitions on the topic to approach *SQ1*. Since this is a primarily instrumental sub-question, the literature is reviewed in order to elaborate proper concepts on which the analysis shall be built. The literature is chosen based on formal factors such as the kind of journals the articles where published in, the number of citations but also the year of publication since older documents on such innovative topics as cybercrime run the risk of being outdated. Certainly, also substantive factors as the content and relevance for the analysis are essential for the selection of literature.

SQ2 and *SQ3* on EU law provisions are answered in chapter 3 mainly by analyzing normative and policy documents. Of concern are the primary law provisions on the policy areas constituting the EU security paradigm, namely the CSDP and the AFSJ respectively. The analysis shall result in the establishment of the correct legal basis and interpretation of EU norms. To analyse the statutory provisions of the CSDP and AFSJ, the primary sources Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU) shall provide the necessary norms as well as literature elaborating on EU law. Based on these findings it is to be established to what extent the EU is able to act in these policy areas and whether this complements cybersecurity. Therefore, secondary sources laid down in Article 288 TFEU or special guidelines applicable for the area of Common Foreign and Security Policy are used. Supplementary law is considered in form of case law by the European Court of Justice or international law requirements when appropriate. Additionally, European policy documents and scientific publications are included to substantiate the analysis. Since the amount of relevant EU publications exceeds the scope of this thesis a non-exhaustive selection had to be made based on the topicality, the determination of new relevant insights and the frequency of references made to this document in other policy papers.

Subsequently the literature from the first parts and the focus on Directive 2016/1148 as well as data published by ENISA shall help answering *SQ4* and *SQ5*. The focus is laid on the question whether internal market provisions contribute to cybersecurity even though they do not belong to the security paradigm of the EU. This is based not only on publications from European institutions and the agency itself, but also on released academic revision when available. This analytical groundwork thus results in a final conclusion in chapter 5 including answers to the research question of the contribution of the EU regulatory framework on cybercrime to the security domain. The final chapter includes current criticism on the *status quo* of the cybersecurity framework as well as an outlook on potential future policies which is underpinned by recent publications and press releases by the EU. As a last point, it shall be clarified that this thesis is based on the normative assumption that a more effective EU is by default a positive achievement given the fundamental values and rights it pursues.

2 THE CYBERSECURITY REALM AND THE MENACE OF CYBERCRIME

With the growth of global connectivity, the social and political life has changed immensely. The widely-cited role the Internet played during the Arab Spring in promoting freedom of speech purports that computer networks are at the frontline of defending freedom, fundamental rights and rule of law.[17] However, freedom online just as offline requires security too.[18] In fact, the internet can similarly be used as an efficient instrument to surveil and attack opponents or commit harm and crime in any possible way. The degree to which cyberspace brought freedom to users similarly gave rise to security threats that can be used against the very same citizen. Between the poles of the right to freedom and the guarantee of safety, cybersecurity is challenged to secure principles of democracy, rule of law and fundamental rights and to provide as much freedom to citizens as possible while at the same time controlling that the freedom cannot be abused to harm others. Consequentially, cybersecurity and cybercrime are gaining growing attention in the public discourse. However, divergent notions of the concepts are prevailing which is posing challenges when it comes to systemically addressing the issue. To obtain certainty on the concepts this chapter aims at answering *SQ1* '*What knowledge is available on how cybercrime is defined, how cyberattacks are conducted and which potential threats these pose towards EU essential services?'.* Therefore, a clarification of the concepts of cybersecurity, critical infrastructure and cybercrime is in order based on a qualitative literature review of policy documents and scientific publications in the field. Subsequently, reference is made to the definitions prevailing in the Budapest Convention before proceeding with a nature and risk assessment of cybercrime.

2.1 The Concept of Cybersecurity and Critical Infrastructure

Due to the broad scope of cybersecurity several definitions are used within international academic discussion on the topic. While some scholars refer to cyber defence and cyber resilience as forming components of an overall cybersecurity strategy, others use the term interchangeably which already indicates disagreement on approaching the topic. Generally, cybersecurity focuses on the protection of computers, networks and data from unintended or unauthorized access, change or destruction. The scope, severity and transnational nature have

[17] S. Manacorda (ed.), *Cybercriminality. Finding A Balance Between Freedom And Security* (Milan: ISPAC 2012), at 34.
[18] European Commission, *supra* note 13, at 2.

induced law enforcement and international security organizations, along with governments and the private sector to define and approach the issue.[19] Similarly, ensuring cybersecurity has become a top priority in EU politics where a trenchant and at the same time blurry notion of cybersecurity has been found: "*Cybersecurity is the first line of defence against cybercrime*".[20] This is further clarified in the EUCSS where cybersecurity is composed of *Network and Information Security, law enforcement* and *defence* which span across diverging policy areas and thereby operate within different legal frameworks.[21] Furthermore, the European Commission establishes four principles that shall genuinely guide the policy of achieving cybersecurity. These principles are the protection of fundamental rights, freedom of expression, personal data and privacy, access for all, democratic and efficient multi-stakeholder governance and a shared responsibility to ensure security which clearly points in the direction of upholding the right of online freedom.[22] Fundamental rights thereby are the higher goods that shall be protected by a common security approach.

Our ever-growing reliance upon cyberspace places all governments, businesses, organisations and individual users at the risk of cyberattacks.[23] It means in effect that cybersecurity concerns strike all parts of society not only the economic and political sphere but also every citizen in his private life who is connected to the internet. In effect, the importance of cybersecurity traditionally gained more momentum in the public through cybercrimes mainly directed at credit card scams or account theft, thereby harming primarily the individual.[24] However, recently the cybersecurity of larger institutions with certain online infrastructures has been focused upon in the literature due to their high potential for damage. The enforcement of cybersecurity is mainly concerned with the protection of essential services, also called critical infrastructures.

[19] M. Portnoy and S. Goodman (eds.), *Global Initiatives to Secure Cyberspace. An Emerging Landscape* (Springer: New York 2009), at 1.
[20] European Commission, *supra* note 4, at 19.
[21] A. Segura Serrano, 'Cybersecurity: towards a global standard in the protection of critical information infrastructures', 6 *European Journal of Law and Technology* 2015, at 9.
[22] European Commission, *supra* note 13, at 4.
[23] F. Wamala, 'The ITU National Cybersecurity Strategy Guide' (September 2011), at 13, available at <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>.
[24] M.-C. Frunza, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets* (Elsevier: Waltham 2016), at. 208.

Critical infrastructures constitute especially vulnerable systems since their connectedness and dependencies between national infrastructures provide compelling targets for criminal attacks.[25] This concept entails critical infrastructure crucial for maintaining vital public functions, health, safety, security, economic or social wellbeing of people.[26] The EU commonly stresses services in certain sectors, namely energy, transport, banking, financial market infrastructures, healthcare, drinking water supply and distribution as well as digital infrastructure.[27] Furthermore, for the determination of essential service operators, Directive 2016/1148 provides a detailed guideline for the Member States. Primarily Article 5(2) of the latter lists the criteria for the typology of public or private essential service providers which thus need to be crucial for the maintenance of critical societal and/or economic activities, with the provision of the service dependent on network and information systems and significantly disrupted in the service provision by an incident.

2.2 Cybercrime – A known Unknown

Hence, while cybersecurity refers to safety provisions that shall protect cyberspace, 'cybercrimes' are the actual criminal actions that threat the security. However, not all offences committed in cyberspace are covered by the term cybercrime of which the most prominent are cyber-warfare and cyber-terrorism. Even though there are no clear criteria yet for determining the various offences internationally, cyber-warfare is typically conceptualized as state-on-state action equivalent to an armed attack[28] while cyber-terrorism primarily generates fear due to destruction and violence based on ideological goals.[29]

This study solely covers the term 'cybercrime' which still refers to a range of cases where technology is used in the commission of crime which is often financially motivated and encompasses different concepts of varying levels of specificity.[30] In fact, the term cybercrime was created by the public between mass media and the professional discourse; it has hardly any

[25] A. Haase, 'Harmonizing Substantive Cybercrime Law through European Union Directive 2013/40/EU - From European Legislation to International Model Law?', *IEEE Explore Digital Library – First International Conference on Anti-Cybercrime (ICACC)* (2015), available at <http://ieeexplore.ieee.org/document/7351931/>, at 2.
[26] A. Haase, *supra* note 25, at 2.
[27] Directive (EU) 2016/1148, *OJ* [2016] L 194/1, 19.7.2016.
[28] C.A. Theohary and J.W. Rollins, 'Cyberwarfare and Cyberterrorism: In Brief', *Congressional Research Service* (27 March 2015), at 2.
[29] S. Gordon and R. Ford, 'Cyberterrorism?', *Symantec Security Response White Paper*, at 4, available at <https://www.symantec.com/avcenter/reference/cyberterrorism.pdf>.
[30] H. Jahankhani *et* al., 'Cybercrime classification and characteristics', in B. Akhgar, *et* al. (eds.), *Cyber Crime and Cyber Terrorism. Investigator's Handbook* (Waltham: Elsevier 2014), at 149.

reference point in in legal documents.[31] Given that in some cases the expression is even used interchangeably with 'computer crime',[32] 'high-tech crime' or 'internet-crime' the discourse on a universally valid definition is taken further. Generally, the ambit of cybercrime contains a large set of different criminal activities where computers and information systems constitute either the main target or the primary tool of the attack.[33] Since this definition is a broad approach to specify the concept, scholars throughout the academic literature usually distinguish cybercrimes along three different typologies, crimes against electronic networks, traditional crimes now committed through electronic means and content-related crimes. A table shall help clarifying the different types:

Cybercrime	CIA-crimes / Cyberattack	Computer-related crimes	Content-related crimes
Origins	Cyber-dependent; new crime	Cyber-enabled; traditional crime	Cyber-enabled; (traditional crime)
Computer network is:	Main target	Main instrument	Main instrument
Concrete Offences	Hacking; Spam; Denial of Service	Fraud ('phishing'), Forgery	Child Pornography; Copyright infringements

Cyber-terrorism
Cyber-warfare

Table 1: Offences committed in cyber space[34]

Thus, cybercrimes might firstly be traditional crimes which are now committed in the ITC environment. Scholars refer to these crimes as cyber-enabled crimes since the use of ITC did not initiate the crime but highly increased the scale or reach and enabled a new quality of crime.[35] These are offences that already exist in the physical domain but are now conducted by

[31] K. A. DeTardo-Bora and D.J. Bora, 'Cybercrimes: an overview of contemporary challenges and impending threats', in J. Sammons (ed.), *Threatscape and Best Practices* (Waltham: Elsevier 2016), at 120.
[32] The term 'computer crime' is used in Art. 83 TFEU; the EU itself is therefore not clear on the definition of the terms which will be discussed later in the paper.
[33] H. Carrapiço and B. Farrand, *supra* note 8, at 464.
[34] This table was created based on the literature review conducted for this thesis without attempting to be comprehensive. Different typologies of cybercrime exist in the literature.
[35] B. Brewster *et al.*, 'Cybercrime: Attack Motivations and Implications for Big Data and National Security', in B. Akhgar (eds.), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies* (Waltham: Elsevier 2015), at 111.

means of computer systems. Within the scope of this category fall computer-related crimes as fraud ('phishing') and forgery. Through phishing criminals attempt to illegally obtain sensitive information such as passwords or payment details by disguising as a trustworthy entity in electronic communication.

Additionally, content-related crimes usually belong to the same category of computer-enabled crimes although they are not clearly classified as traditional offences and cover the publication of illegal content over electronic media such as the dissemination of child pornography and copyright offences such as property right infringements.[36]

Cybercrimes can also be offences unique to the ITC world which originate in the digital evolution. McGuire and Dowling therefore apply the typology of cyber-dependent crimes, since ICT have allowed for a new field of criminality.[37] Cyber-dependent crimes violate the confidentiality, integrity or availability of computer system networks or digital data (CIA-crimes) and are targeted at the computer system. Most prominent examples of these crimes are hacking, spam or denial of service. Although these offences are primarily directed at harming computers or networks they might similarly imply secondary outcomes of traditional crime such as fraud. The distinction therefore is naturally blurry and poses challenges to criminal justice systems which are bound to the principle of law that only an offence that is properly recognized by the law can be pursued. While a narrow definition which only applies to cyber-enabled crimes is at risk of excluding harmful crimes, a broad definition is criticized for being vague and therefore meaningless.[38] This discussion shows that while the threat of cybercrime is generally known by now, the actual scope of the topic remains relatively unknown.

2.3 The Budapest Convention on Cybercrime

Naturally the discussion on cybersecurity is led not only within Europe but also internationally given its transnational character. Apart from countless cooperation initiatives in the field[39] binding agreements are rare due to the nature of international law. A milestone in the

[36] M. Chawki *et al.*, *Cybercrime, Digital Forensics and Jurisdiction* (Cham: Springer 2015), at 5.
[37] M. McGuire and S. Dowling, 'Cyber crime: A review of the evidence', *Home Office* (October 2013), at 5, available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf>.
[38] A. Shkëmbi and D. Sina, 'Cybercrime in the Perspective of the European Legal Framework', 4 *Mediterranean Journal of Social Sciences* 2013, at 327.
[39] *See* for example: The United Nations specialized agency *International Telecommunication Union* (ITU) <http://www.itu.int/en/about/Pages/default.aspx>, or the annual Global Conference on CyberSpace, for the GCCS 2015 in The Hague see <https://www.gccs2015.com/>.

international attempt to conceive cybercrime was the adoption of the Council of Europe's Convention on Cybercrime in 2001 (Budapest Convention).[40] 54 mainly European countries have since ratified this international criminal justice treaty which strives primarily for the establishment of *"a common criminal policy aimed at the protection of society against cybercrime, inter alia by adopting appropriate legislation and fostering international co-operation".*[41] Regarding substantive law provisions the Budapest Convention requires signatories to establish criminal offences in domestic legislation which are listed among Article 2-13 within five categories: Title 1 lists offences against the confidentiality, integrity and availability of computer data and systems (CIA-crimes) which applies to the narrow definition of cybercrime targeted at computer networks. In addition, the subsequent Titles enumerate offences by means of computers focusing on conducts that acquire a new quality when committed through computers,[42] namely computer-related offences of forgery and fraud in Title 2, content-related offences in Title 3 and again in Title 4 for offences related to infringements of copyright and related rights. Hence the Convention adopts a broad definition of cybercrime classifying not only cyber-enabled but also traditional crimes modified by the cyberspace as criminal acts to be pursued domestically. Procedural law is also regulated among to enable criminal justice authorities to effectively investigate criminal offences such as search and seizure of stored computer data or the interception of communications. Furthermore, international cooperation is demanded explicitly.

Being the most substantial document on cybercrime internationally the Budapest Convention serves as a baseline with many countries using it as a 'model law' in the preparation of domestic legislation.[43] Even the United Nations General Assembly recommended to *"ascertain whether your country has developed necessary legislation for the investigation and prosecution of cybercrime, noting existing frameworks (…) including the Council of Europe Convention on Cybercrime".*[44] The substantive law on cybercrime offences has influenced national legislation as well as EU policies.[45] In fact, the EU has not adopted an equivalent definition applicable to all policy spheres concerned. Most documents published by the Union on the topic refer to the

[40] Council of Europe, 'Convention on Cybercrime', *European Treaty Series No. 185,* 23.11.2001.
[41] Council of Europe, *supra* note 40, at 2 (Preamble).
[42] A. Seger, 'The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web', 16.2.2012, at 2, available at < https://rm.coe.int/16802fa3e0>.
[43] A. Seger, *supra* note 42, at 2.
[44] Resolution adopted by the General Assembly on 21 December 2009, United Nations A/RES/64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17.3.2010.
[45] F. Calderoni, 'The European legal framework on cybercrime: striving for an effective implementation', 54 *Crime, Law and Social Change* 2010, at 340.

validity of the Convention such as it is "*the predominant European and international instrument in this field"*[46] or even the appropriate legal framework of reference at the global level.[47] Since the analysis of the European legal framework forms a considerable part of this thesis, the definitions included in the Budapest Convention shall be adopted for the analysis.

However, whether the Convention truly created effective cybercrime prosecution is doubtful. Among the main points of criticism is the failure to ratify the Convention by member and non-member states.[48] Not only major powers such as Russia and China but also EU Member States still refrain from the Convention. Given that the EU itself is not a signatory a coherent EU policy is harder to reach and prompts the EU Commission to repeatedly urge remaining states to ratify.[49] Secondly, the deficiency of international law is visible in the lack of competent law enforcement authorities. International cooperation is declared theoretically but difficult to achieve in practice due to divergent national efforts in executing the orders. The Convention is sometimes even declared to be only of symbolic nature without any real change.[50] Still, the fact that a normalization of definitions exists internationally and is even accepted beyond Europe is striking. The Budapest Convention serves as a baseline for criminal justice law regarding cybercrime with political relevance due to its comparatively high number of signatories within and beyond Europe but it might already be the maximum achievable on the international stage. A starting point for stronger European cybersecurity regulation is thereby given.

2.4 Nature and Risk Potential of Cybercrime

After having defined and demarcated the terms cybersecurity, critical infrastructures and cybercrime it is essential to disclose the problematic nature of cybercrime. Firstly, as has already been conveyed above, there is no universally accepted definition. While some countries have already proceeded relatively far with pursuing cybercrime with legally binding instruments (see the Budapest Convention) other regions still have not included the importance

[46] Commission of the European Communities, 'Communication from the Commission to the European Parliament, Council and Committee of the Regions: Towards a general policy on the fight against cyber crime', COM (2007) 267 final, 22.5.2007, at 6.
[47] European Council, 'The Stockholm Programme – An Open and Secure Europe serving and protecting citizens' *OJ* [2010] C 115/1, 4.5.2010, at 22.
[48] 43 out of 47 Members have ratified the Convention; 12 Non-Member States have also ratified it.
[49] *See* for example in: European Commission, *supra* note 4, at 9.
[50] N. E. Marion, 'The Council of Europe's Cyber Crime Treaty: An exercise in Symbolic Legislation', 4 *International Journal of Cyber Criminology* 2010.

of cybersecurity as an issue in their national security strategy.[51] Naturally accompanying is a lack of a clear definitions of the offence which is problematic as it impacts upon every facet of prevention, protection and remediation.[52] This already puts the respective jurisdictional system in conflict with the rule of law principle. But it is not only unconcern of national governments that averted efforts for implementing a legal definition; one of the major problems with adequately defining cybercrime is the lack of concrete statistical data on these offences. Businesses often refrain from reporting attacks out of fear to release sensitive data or lose trust of customers. As the reporting of crime as yet is predominantly voluntary the figures are almost certainly much lower than the actual occurrence of crime.[53]

Moreover, the prosecution of cybercrimes remains challenging to governments and law enforcement due to the inherent global interconnectedness. This is also captured in the European Agenda on Security, stating that *"cybercrime is by its nature borderless, flexible and innovative*".[54] Borderless refers to the fact that it disregards traditional operational criteria of European criminal justice systems such as sovereignty and the territoriality principle.[55] Cybercrimes defy the conventional jurisdictional realms of sovereign states when attacks originate from almost any computer in the world, pass across multiple national boundaries, or are designed to appear to be originating from foreign sources which creates uncertainties regarding the competent jurisdiction.[56] Problematic are also the divergent national levels of legislation which facilitate the exploitation of gaps in crime laws of other countries without prosecution of the criminals. The absence of international harmonization can create 'crime shelters' similar to 'tax shelters' created by the legislation in certain states.[57] The boundlessness of crimes coexistent with the absence of an international law regime in the cyberspace causes a jurisdictional dilemma. Hence, states cannot handle the issue individually but need to seek transnational or global cooperation to effectively tackle cybercrime.

Adding to the problematic of boundlessness of cybercrimes, the EU also refers to the flexibility and innovativeness of crimes as potential threats. The characteristic of being innovative implies

[51] China as an example conceives cybersecurity as an open concept which can be used to control the content available on the Web; there is no reference to the protection of fundamental rights of users in the cyberspace, *see* A. Seguro Serrano, supra note 21, at 14.
[52] H. Jahankhani *et* al., *supra* note 30, at 152.
[53] M. Chawki *et al.*, *supra* note 36, at 6.
[54] European Commission, *supra* note 4, at 19.
[55] F. Calderoni, *supra* note 45, at 341.
[56] McConnell International, 'Cyber Crime… and Punishment? Archaic Laws threaten Global Information' (December 2000), at 2, available at < http://www.witsa.org/papers/McConnell-cybercrime.pdf>.
[57]M. Chawki *et al.*, *supra* note 36, at 22.

the rapidly changing environment of ICT. Criminal law enforcement procedures adjusted to the physical world are confronted with new challenges in the virtual world. Whether proofs are being deleted or altered online or new technologies diversifying the market constantly, the legal framework must change to adopt to these new crimes. New cyber-dependent crimes challenge the criminal law framework due to the absence of references in the law. Cyber-enabled crime in its origin might already have a reference in criminal law for instance fraud or theft of property. Still, these crimes are pursued in a new dimension and entail new options that are not covered by the respective legislation. It remains unclear to what extent the existing legal references are applicable to cybercrimes and especially to hybrid forms of cyber-dependent and cyber-enabled crimes which raises not only legal but also technical complexities of prosecuting cybercrime. This holds true for the problematic evidence tracking, since the dynamic nature of cyberspace makes it difficult to collect all relevant digital evidence of cybercrimes.[58] The question is raised whether cybercrime law exists in the first place and whether the existing crime law is applicable. And finally, the technological requirements for conducting a crime have become more easily accessible. Compared to other crimes and offences, it generally requires a smaller investment and is not restricted by tight controls such as gun control law.[59] In this regard the European Cybercrime Center (EC3) points to the characteristic of scalability meaning that the replication of crimes on a massive scale due to standardization of software easily affects millions of computers without any logistical constraints.[60] To conclude, cybercrimes differ significantly in their nature from terrestrial crimes which is visible in four main aspects: the lack of clear definition as crimes, the borderless nature, the quick technical changes as well as the resources needed to cause damage.

2.5 Conclusions

This chapter aimed at concretizing the concepts of cybercrime, cybersecurity and critical infrastructures and the arising security concerns. Acknowledging that a universally accepted conceptualization is lacking, cybercrimes are generally divided in cyber-dependent and cyber-enabled crimes. The former are unique to the ITC environment targeting computer data and systems harming the confidentiality, integrity and availability of computer networks (CIA-crimes). The latter group of crimes is broader and usually originating in traditional crimes.

[58] M. Chawki *et al.*, *supra* note 36, at 20.
[59] M. Chawki *et al.*, *supra* note 36, at 10.
[60] European Cybercrime Center – Europol, 'First Year Report', at 26, available at <https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report>.

These crimes are conducted by means of computer networks and can be computer- or content-related. Lately, these crimes are mostly directed at essential services/critical infrastructures of nations which are vital to the functioning of the public life and whose outage impacts the whole of society. The objective to be achieved by the prevention of cybercrime, defence and the resilience of essential services is cybersecurity, meaning the protection of computers, networks and data from unintended or unauthorized access, change or destruction while always respecting fundamental rights.

However, cybercrime inherits certain characteristics which challenge the preservation of cybersecurity. These characteristics are the lack of an internationally accepted definition, the question of competent jurisdictions for transnational crimes and applicable laws as well as the very nature of cyberspace as innovative and flexible. The EU alongside the USA are among the first regulatory powers in addressing these challenges.[61] Therefore, the following chapter shall analyse EU security policy and possible instruments based on the current security concerns elaborated above.

[61] A. Segura Serrano, *supra* note 21, at 1.

3 ADVANCING CYBERSECURITY POLICY USING THE EU SECURITY PARADIGM

Having established the concepts of cybersecurity and cybercrime highlighting its borderless scope the question arises how transnational authorities are equipped in facing these challenges. In the focus of this analysis shall be the acting of the European Union being one of the pioneers in addressing cybercrime.[62] Since these security threats are inadequately met in the frame of national jurisdiction the community approach of the EU may appear promising. However, the exceptional structure of the EU entails that action is always conditioned by peculiar obstacles. Therefore, this chapter assesses EU regulatory provisions and restrictions of complementary policy areas to conclude with a realistic assessment of the EU's position in the face of combating cybercrime. Essential for the analysis is the identification of competences which refers to *SQ2* on how the correct legal basis for regulating cybersecurity is to be established in the interplay between the CSDP and the AFSJ. Moreover, answers to *SQ3* deal with the scope of conferred competences enabling the Union to proceed with legislation and implementation without violating the principle of conferral. Answers to the sub-questions shall enable an assessment of the possibilities given at the Union level to develop a cybersecurity policy.

3.1 Establishing the Legal Basis

The EU regulatory framework is a diverse consolidation created by almost 70 years of European integration. Being an ongoing legal and political experiment of integrating 28 Member States, not all necessarily agree on what should be the future direction of this process.[63] This holds especially true for the security realm which has traditionally been considered as one of the core areas of national oversight. Frequently, the basic principle of conferral laid down in Article 5 TEU is underlined so that the Union shall only act within the limits of the competences conferred upon it by the Member States ensured in primary law. Respecting the choice of the correct legal basis and the separation of policy provision is in a legal sense imperative for EU policy making.[64] Besides, it is of political importance as it not only defines the role and involvement of the Institutions or the decision-making procedures (a 'legislative procedure' or

[62] A. Segura Serrano, *supra* note 21, at 1.
[63] B. van Vooren and R.A. Wessel, *EU External Relations Law. Text, cases and materials* (Cambridge: Cambridge University Press 2014), at xxxiii.
[64] The constitutional significance of the proper legal basis has been reaffirmed by the EUCJ, see for example: Opinion 1/08 Amendments to EU Schedules of Commitments under GATS [2009] ECR I-11129, at para. 110.

not) but also voting rules in the Council and thereby determining powers on the horizontal and vertical axis.[65]

However, the determination of the correct legal basis in primary law is not always clear. Starting from profound economic communitisation processes other policy areas were gradually included but not always to the same degree as in the Customs Union[66] mainly due to national hesitation to cede power. As a result, the regulations and competences vary across the distinct policy areas. The connection of security concerns to various policy fields similarly implies that not one definite reference of cybersecurity exists in EU primary law. It certainly has a Fundamental Rights anchoring which is explicitly expressed in the EUCSS: "*The legal obligations enshrined in the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the EU Charter of Fundamental Rights should be also respected online"*.[67] Additionally, the pursuit of cybersecurity has its roots in the reflections on economic issues. In fact, the topic was taken seriously due to its menace for the internal market and trade relations. In the proposal for a new directive in 2013 the legal basis is connected to Article 26 TFEU enabling the Union to adopt measures on the internal market.[68] It is therefore also connected and referred to in the Agenda on the Digital Single Market since the growing number of cyber offences as data interception or trade secret theft is clearly leading to significant economic losses.[69] However, the pursuit of security is primarily connected to the CSDP with the treaties stating in the specific provisions on the Common Foreign and Security Policy (CFSP) that the Union action shall include *"all areas of foreign policy and all questions relating to the Union's security"* (Art. 24 TEU). And finally, internal security and the prosecution of criminal matters is anchored in the realm of the AFSJ already mentioned in the EU's objective in Article 3 TEU. Due to the explicit mentioning as security policies, the CSDP and the AFSJ are in this study referred to as forming the *security paradigm* of the Union.

[65] R.A. Wessel, 'Towards EU cybersecurity law: Regulating a new policy field' in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing 2015), at 420.
[66] The Customs Union is one of the policy areas listed in Art. 3(1) a TFEU where the Union has exclusive competences. This means that competences were completely shifted from the national to the community level.
[67] European Commission, *supra* note 13, at 15.
[68] European Commission, *'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union'*, COM (2013) 48 final, 7.2.2013.
[69] European Commission, '*Communication from the Commission to the European Parliament, Council, EESC and Committee of the Regions: A Digital Single Market Strategy for Europe'* COM (2015) 192 final 6.5.2015, at 12.

Foreign policy and criminal prosecution have traditionally always formed part of the key sovereign competences of national governments and thus have for a long time remained national competences. The Maastricht Treaty in 1993 formally included both areas in the 'three-pillar' structure outside the community pillar with salient intergovernmental characteristics. With the entry into force of the Lisbon Treaty the structure was changed considerably. The 'three-pillar' structure was dissolved and substituted by legal unity for the purpose of enhancing coherence and effectiveness of EU action. Despite all integration efforts both domains follow peculiar procedures shaped by strong national influence which determine EU action in the field. As the CSDP and the AFSJ both constitute the traditional security paradigm in the Union their statutory framework shall be analysed in detail. Adding to the assessment of the respective policy field the combination of both shall be considered subsequently. The EU is increasingly ambitious about establishing coherence between its policies with a special focus on the linkage between the AFSJ and CSDP.[70] Even though EU policy usually requires a specific legal basis the possibility of a dual legal basis was affirmed by the EUCJ in exceptional circumstances.[71] Its application shall be considered in this chapter.

3.2 Defence Provisions within the Common Security and Defence Policy

The CSDP is defined among the special provisions for the CFSP in Title V TEU. It has always been an area dominated by intergovernmental ruling and the reluctance of Member States to confer competences to the Union's Institutions. A break with this tradition came with the Maastricht Treaty which included CFSP for the first time in the legal construct of the European Union as a 'three-pillar' model: Even though the Union became responsible for its foreign and security policy it was still highly influenced by national competences and interests as it remained outside the community pillar. Still, some progress has been made from the former second pillar separated from the community policies in the Maastricht Treaty to the inclusion in the Lisbon Treaty and incremental steps towards supranational provisions. It remains to this day a special construct within the treaties based on an interplay between intergovernmental and community approaches even though a balance has not been reached yet with the intergovernmental sphere seemingly prevailing.[72] The intergovernmental character is expressed

[70] *See* for example: European Commission, *'Joint Staff Working Paper: Strengthening Ties between FSJ and CSDP Actors. Proposals for a way ahead'*, SEC (2011) 560 final, 5.5.2011, para. 4.
[71] C-178/03 Commission v Parliament and Council, paragraph 43.
[72] M. Piechowicz, 'Intergovernmental Cooperation and the Idea of Community in the Institutional and Decision-making Sphere of the EU Common Foreign and Security Policy', 23 *European Review* 2015, at 550.

in the common provisions on the CFSP with Art. 24 (1) stating that *"it shall be defined and implemented by the European Council and the Council acting unanimously, except where the Treaties provide otherwise. The adoption of legislative acts shall be excluded."* Therefore, the deployment of common legislative instruments of the Union namely regulations, directives, decisions, recommendations and opinions defined in Art. 288 TFEU is not permitted in CFSP. Furthermore, the primarily concerned institutions in the process of implementing CFSP are the European Council defining general guidelines and strategic lines and the Council framing the CFSP and taking the necessary decisions (refer to Art. 26(2) TEU) which represent rather national than common interests. Similarly, when adopting binding decisions on foreign and security policy the European Council and the Council usually act unanimously (Art. 31 TEU) so that no Member State can be ruled over in their realization of foreign policy. Besides, the power of the Court of Justice is narrowed down to the monitoring of Art. 40 TEU and Art. 275 TFEU. These common provisions which similarly apply to the CSDP reflect one of the most intergovernmental policy areas with minimal Union competences. However, Article 26 also highlights the role of the High Representative for Foreign and Security Policy (HR/VP) and entrusts him with ensuring the unity, consistency and effectiveness of the action of the Union as well as putting into effect the common foreign and security policy with the Member States using national and Union resources. Furthermore, Article 27 allows the HR/VP assisted by the European External Action Service (EEAS) to submit proposals on the development of the CFSP and ensure the implementation of decisions adopted. Through the creation of the HR/VP the Union was given partial competences in the field.

The specific provisions for the CSDP are found in Art. 42-46 TEU. Art. 42(1) sets the core tasks of peace-keeping, conflict prevention and strengthening international security using national capabilities on the CSDP agenda. It clearly refers to the strengthening of international security without reference to internal security. Art. 43 further specifies the tasks ('Petersberg-tasks') which include *"joint disarmament operations, humanitarian and rescue tasks, military advice and assistance tasks, conflict prevention and peace-keeping tasks, tasks of combat forces in crisis management, including peace-making and post-conflict stabilisation"* without reference to cybersecurity or cyber defence. Generally, CSDP operations are, by nature, conducted outside the EU in distant theatres.[73] The traditional four military domains of CSDP land, air, sea and space are covered by traditional means of security in the physical world.

[73] Council of the European Union, *'Cover note on the European Union Concept for EU-led Military Operations and Missions'*, 17107/14 (2014), 19 December 2014.

However, the scope of the CFSP domain is defined in Article 24 TEU stating that *"the Union's competence in matters of common foreign and security policy shall cover all areas of foreign policy and all questions relating to the Union's security"*. Considering this provision, the imminent threat of cybercrime falls within the scope of CFSP since it affects internal peace by disrupting the functioning of institutions as well as interferes with the peaceful living. This is exemplified in the 2007 attack on Estonia when cash machines were out of action and newspapers and broadcasters unable to inform the public.[74] Attacks against essential services such as nuclear power plants or health services can threaten National Security. In addition to the broad conception of security, Article 26 TEU allows the Council *"to determine the objectives and define general guidelines for the common foreign and security policy, including for matters with defence implications"* and to adopt decisions accordingly leaving room to mainstream new security issues in the CFSP. Based on that, Article 42(3) requires Member States to respect the objectives defined by the Council and to provide civilian and military capabilities to contribute to the objectives. Even though cyber defence was initially not provided for by statute it is nowadays understood as one of the most serious security implications of threats inherent to society's reliance upon cyberspace for Europe.[75] Therefore, it gains more attention within CSDP policy where cyberspace is now listed as the fifth traditional domain alongside with land, sea, air and space but similarly highlighting the warfare rationale behind cyberspace in CSDP.[76] Through mainstreaming cyber defence in the objectives of CSDP it is likely to play an increasing role within CSDP since resistance from Member States is expected to decrease when realizing that they are no longer able to cope with cyber defence on the national level only.

[74] D. McGuinness, 'How a cyber attack transformed Estonia', *BBC News*, Tallinn, 27 April 2017, available at <http://www.bbc.com/news/39655415>.
[75] N. Robinson, 'EU cyber-defence: a work in progress', European Union Institute for Security Studies (ISS) Brief No. 10 (14 March 2014), at 1, available at < http://www.iss.europa.eu/publications/detail/article/eu-cyber-defence-a-work-in-progress/>.
[76] Council of the European Union, *'EU Cyber Defence Policy Framework',* 15585/14 (2014), 18 November 2014, at 2.

3.2.1 Instruments derived from CSDP Provisions

From the beginning in 1999 the focus of CSDP was laid on civilian and military security and peace promotion in the world. With the adoption of the first European Security Strategy by the European Council in 2003 as a conceptual framework for CFSP and CSDP however, the EU took the next step towards the advancement of its security policy. Asserting its role as a global player and admitting the emergence of new security threats, the EU entered the stage of global security considerations. With terrorism, weapons of mass destruction, state failure, regional conflicts and organized crime on the security agenda a new level was reached beyond traditional security concerns.[77] Even though cybersecurity has not been included in the first strategy the EU still acknowledged that the nature of security threats has changed and that a new paradigm in contrast to the military approach prevailing in the Cold War was needed requiring a mixture of military, economic, civilian, political or judicial instruments. While the strategy correctly describes the new threat environment as more diverse, less visible and less predictable it misses to list cybercrime as one of the new menaces with terrorism and organized crime which were included by then. In the report on the implementation of the strategy in 2009 cybercrime is mentioned for the first time as a potential new economic, political and military weapon demanding more work in this field.[78]

In 2016 the new Global Strategy for the European Union's Foreign and Security Policy (EUGS) was presented by HR/VP Mogherini and initiated a shift in focus compared to the 2003 strategy, adjusting to a more connected, contested and complex world.[79] The new strategy lists five priorities for the Union, namely the security of the Union, state and societal resilience to the East and South of the EU, the development of an integrated approach to conflicts, cooperative regional orders and global governance for the 21st century.[80] The first priority focuses on internal security and the threats it faces and explicitly refers to efforts in cyber issues.[81] The EUGS also captures the new notion that coherence beyond CSDP across policy domains is essential which is also repeated in the Implementation Plan[82]: *"This priority will be pursued in cooperation with Freedom, Security and Justice (FSJ) actors. While CSDP missions and*

[77] European Council, *'A secure Europe in a better world European Security Strategy'*, 12 December 2003, at 4.
[78] Council of the European Union, '*Report on the Implementation of the European Security Strategy'*, S407/08 (2008), 11 December 2008, at 5.
[79] N. Tocci, 'The making of the EU Global Strategy', 37 *Contemporary Security Policy* 2016, at 462.
[80] European Parliament, 'Common Security and Defence Policy', *Fact Sheet on the European Union*, June 2017.
[81] F. Mogherini, *'Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy'*, June 2016, at 9.
[82] Council of the European Union, *'Note on the Implementation Plan on Security and Defence'*, 14392/16 (2016), 14 November 2016, at 3.

operations are deployed outside the Union, the EU can contribute from a security and defence perspective to strengthening the protection and resilience of its networks and critical infrastructure (…).” [83]

These strategies lay the foundations for EU security and defence policies and reflect the increasing attention for cybersecurity threats. Given the provisions of the CSDP framework elaborated in section 3.2 and the nature of CSDP it is hardly surprising that the EUGS does not include a call for legislative instruments but primarily draws on existing mechanisms. Member States are to translate their commitments to mutual assistance and solidarity enshrined in the treaties into action as well as recall the close cooperation with NATO which is reaffirmed by the Council: [84]

“Existing EU policies in these areas should be taken forward in a comprehensive manner. The importance of Mutual Assistance and/or Solidarity in line with Article 42.7 TEU and Article 222 TFEU respectively is highlighted in this context as well. The Council recalls that NATO remains the foundation for the collective defence for those States which are members of it. The specific character of the security and defence policy of all EU Member States will be fully respected.”

While Article 42(7) TEU calls for mutual assistance in the case of an armed aggression (which is most likely not employable in the case of cyberattacks) the solidarity clause linked to security could be invoked in particularly serious cyber incidents:

“1. The Union and its Member States shall act jointly in a spirit of solidarity if a Member State is the object of a terrorist attack or the victim of a natural or man-made disaster. The Union shall mobilise all the instruments at its disposal, including the military resources made available by the Member States, to:

(a) — prevent the terrorist threat in the territory of the Member States;

— protect democratic institutions and the civilian population from any terrorist attack;

[83] F. Mogherini, *supra* note 81, at 21.
[84] Council of the European Union, *‘Council conclusions on implementing the EU Global Strategy in the area of Security and Defence’,* 14149/16 (2016), 14 November 2016, at 5.

— assist a Member State in its territory, at the request of its political authorities, in the event of a terrorist attack;

(b) assist a Member State in its territory, at the request of its political authorities, in the event of a natural or man-made disaster."

However, it remains questionable whether triggering the solidarity clause in the event of a cyberattack is both appropriate and effective. Firstly, the drafting of Article 222 TFEU is kept rather open without determining specific details on the application which leaves authorities with uncertainties and possibly reluctance to enter these uncertain procedures.[85] Some improvements have been achieved through the accompanying Decision[86] clarifying concepts. Since cyberattacks do not fall within the scope of terrorist attacks[87] it is to be seen whether they are covered by 'natural or man-made disasters'. Disasters are hereby only defined as *"any situation, which has or may have an adverse impact on people, the environment or property"* (Art. 38(b)) which is the case when cybercrimes against critical infrastructures are committed (*see* section 2.1). The European Parliament takes the view that the solidarity clause should be invoked when the response capacities of the affected Member State are overwhelmed or a multisector response involving a number of actors is required which also applies to the nature of cyber offences.[88] However, an official listing of cybercrime among natural or man-made disasters is not given. For the sake of clarification, the Commission published a document[89] which includes cyberattacks among man-made malicious disaster risks even though again a blurry definition of cyberattacks is used including for example cyber-espionage.

Despite the recurring emphasis on mutual assistance and solidarity as CSDP priorities the shift towards acknowledging the need for increased and coherent cybersecurity policies beyond solidarity is evident – not only since the EUGS. A mayor step was taken with the adoption of the EUCSS in 2013. It establishes the first common framework for a comprehensive approach framing the fields of resilience of Network and Information Systems (NIS), law enforcement

[85] J. Keller-Noellet, 'The Solidarity Clause of the Lisbon Treaty's', *Note Europe,* June 2011, at 329.
[86] European Commission, 'Joint Proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity clause' JOIN (2012) 39 final, 21.12.2012.
[87] Terrorist Attacks are explicitly defined in the Council Framework Decision 2002/475/JHA which was amended by Council Framework Decision 2008/919/JHA.
[88] European Parliament, 'Resolution on EU mutual defence and solidarity clauses: political and operational dimensions', *OJ* [2015] C 419/138, 16.12.2015, at para. 22.
[89] European Commission, 'Commission Staff Working Document on an Overview of natural and man-made disaster risks in the EU', SWD (2014) 134 final, 8.4.2014.

and criminal justice as well as defence and CSDP among a coherent cybersecurity policy.[90] This is illustrated in Table 2:

	NIS / RESILIENCE	LAW ENFORCEMENT	DEFENCE
EU	Internal Market Rationale	AFSJ Rationale	CSDP Rationale
	European Commission ENISA CERT-EU Competent Authorities DG Economic Affairs	EC3/Europol CEPOL Eurojust DG Home/Justice	HR/VP EEAS EDA
NATIONAL	National CERTs NIS competent authorities	National Cybercrime Units	National Defence and Security Authorities

Table 2. Central Pillars of the EU Cybersecurity Strategy 2013 (modified)[91]

Since the EU acknowledges in the EUCSS the key challenge for cybersecurity being the involvement of these different legal frameworks and jurisdictions and therefore the division of responsibilities between the many actors involved it aims at clarifying roles to accomplish its strategic priorities.[92] These are *(1) achieving cyber resilience, (2) drastically reducing cybercrime, (3) developing cyber defence policy and capabilities related to the CSDP, (4) develop industrial and technological resources for cybersecurity and (5) establish a coherent international cyberspace policy for the European Union and promote core EU values.*

Within the CSDP domain the focus is laid on the priority of developing cyber defence policy and capabilities (3). It is aimed at increasing the resilience of the communication and information systems supporting Member States' defence and national security interests. This shall be achieved through cyber defence capability development concentrating on detection, response and recovery from sophisticated cyber threats. Cyber defence in CSDP here has a military reasoning with the protection of critical infrastructures used in military operations and the focus on efforts within CSDP missions focusing rather on cyber-warfare than on

[90] N. Robinson, *supra* note 75, at 4.
[91] European Commission, *supra* note 13, at 17.
[92] European Commission, *supra* note 13, at 17.

cybercrime. Also, the EUCSS entails the adoption of a cyber defence policy framework for CSDP prioritizing the *development of Member States cyber defence capabilities, the protection of CSDP communication networks used by EU entities, the promotion of civil-military cooperation, improved training, education and exercises opportunities as well as enhanced cooperation with relevant international partners.*[93] Similar to the EUCSS, the policy framework includes the demand for a continuous assessment of the vulnerabilities of the information infrastructures that support CSDP missions and operations. Several measures are proposed in that regard including the creation of a Defence Fund to support investment[94] or the use of the Capability Development Plan by the EDA that facilitates cooperation between Member States to improve convergence in the planning of defence requirements, support cyber defence related projects, facilitate exchanges between Member States in national cyber defence doctrines or improve cooperation between military Computer Emergency Response Teams (CERTs) of the Member States on a voluntary basis.

What becomes clear is the sensitivity of the CSDP domain regarding Union action. While the EUCSS calls for binding legislation among other policy areas it is formulated relatively indecisive regarding CSDP and confines the measures to be 'related to CSDP': while defence now forms part of the cybersecurity strategy its share is limited. It adheres to recommendations and assistance for Member States' national security interests leaving out concrete EU action except for the development of the EU cyber defence policy framework. The latter – as elaborated above – similarly sticks to soft approaches 'between Member States' 'on a voluntary basis' to 'support projects'.

The cooperation is reinforced by responsible bodies in the field: The creation of the European Defence Agency (EDA) was arranged in Art. 42(3) TEU to support the work in the fields of defence capabilities development, research, acquisition and armaments. But similar to the Union itself, the agency is confined in its power primarily supporting Member States in delivering the required technologies as well as incorporating cybersecurity in the capability development plan.[95] Still, the EDA might be a crucial actor in the implementation of cyber defence since technical and intelligence information levels are still low within Europe which is

[93] Council of the European Union, *supra* note 76.
[94] European Commission, 'European Defence Action Plan: Towards a European Defence Fund' (30 November 2016), available at < http://europa.eu/rapid/press-release_IP-16-4088_en.htm>.
[95] European Defence Agency, 'Cyber Defence', Fact Sheet, last updated 10 February 2015, available at <https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-02-10-factsheet_cyber-defence>.

seen as a serious deficiency (*see* section 2.4). Additionally, due to cooperation initiatives with other cybersecurity bodies such as the European Union Agency for Network and Information Security (ENISA, *see* section 4.3) and EC3 which are explicitly invited to participate in defence policies[96] coherence might be achieved on the agency-level.

Even though the EUCSS is referred to as an important achievement, its impact is hard to measure. Firstly, regarding clarification of the concept of cybercrime which is needed for the achievement of a coherent understanding and implementation it does not help to clear up confusion. While it firstly only refers to the need to protect information systems from incidents (resembling the narrow definition of CIA-crimes) it includes in a footnote a broad definition "*of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target".*[97] Additionally, the document at another point even includes cyber-espionage and -terrorism which softens the definition and entails uncertainty in the implementation of these policies. Secondly, the EUCSS is a starting-point setting the objectives for further EU action without mandatory authority. Whether the actors in the different pillars successfully manage to tackle their respective policy fields is to be assessed later in the thesis. For now, one still must acknowledge despite these flaws that the EUCSS is a major step forward in EU cybersecurity policy. Indeed, it points out clear objectives and priorities of EU cybersecurity policy and is used as a benchmark for further policy publications with its most significant contribution being the preparation of the NIS-Directive.[98] The merging of policies which were priorly dispersed enables for the first time a coordinated approach necessary for effective security policies.

3.2.2 Evaluation

Ever since the adoption of the EUGS in 2016 the coverage of EU security policies changed from peace-keeping, conflict prevention and strengthening international security to a broader perception which now mainstreams new security threats into the CSDP realm. Concluding on the CSDP framework however, one must firstly acknowledge the still dominant intergovernmental rationale on which it operates. Even though it was included in the cybersecurity strategy as a fundamental pillar its specific provisions among Title V TEU limit

[96] Council of the European Union, *supra* note 70, at 8.
[97] European Commission, *supra* note 13, at 3.
[98] A. Segal, 'Guest Post: Two Years Later, the EU's Cybersecurity Strategy Stumbles Forward', Council on Foreign Relations Blog Post (3 February 2015), available at < https://www.cfr.org/blog-post/guest-post-two-years-later-eus-cybersecurity-strategy-stumbles-forward>.

its contribution to a coherent policy. Regarding common EU regulations it appears to be the hardest to merge with areas of EU competences due to the exclusion of legislative measures and the diverging decision-making procedures.[99] Guided by the 'centre of gravity-approach'[100] only actions taken in cybersecurity referring primarily to defence would find their basis in the CSDP provisions. Aligning this complex inter-institutional construct requires respecting the EU law principles as the principle of conferral as well as respecting EU values as freedom of expression or the right to data protection.[101] Therefore, the statutory provisions in primary law for the CSDP exercise enable the EU in the field of cyber defence to coordinate efforts but does not confer powers regarding law enforcement or a comprehensive cybersecurity approach. The EUGS approach to foster cooperation and information-sharing will hardly be enough for a common, resilient cybersecurity culture.[102] Also, the persistent focus on cyber-warfare and protecting military infrastructures fails to capture the bigger picture of cybersecurity. Therefore, other policy areas contributing to cybersecurity are considered.

The basic principle on which CSDP has been functioning so far in military and civilian missions is the force contribution of Member States for EU operations. The Union is clearly dependent on the willingness and involvement of Member States for it does not have standing military forces on its own. To a certain degree this principle also translates to cyber defence with the Member States being the key to force generation.[103] In contrast to the USA for example, the EU does not yet dispose of strong military and intelligence capabilities in cyberspace and therefore does not follow a deterrence and militarization logic but rather employs policy areas other than CSDP for building resilience and fighting cybercrime.[104]

Cyber defence policies are, similar to all policies rooted in CSDP, based on the guiding principle of mutual assistance and solidarity highlighting once again national powers. If the political willingness and level of capabilities among Member States is given in the field of cyber defence, the solidarity clause might be a provision in the case of an attack. Furthermore,

[99] R.A. Wessel, *supra* note 65, at 423.
[100] The 'centre-of-gravity' test was developed by the EUCJ to find the appropriate legal basis in cases of two or more competing Treaty articles. Attention is given to the aim and content of the respective measure to match it to the correct legal basis. *See* to B. van Vooren and R. A. Wessel, *supra* note 63, at 159.
[101] N. Robinson, *supra* note 75, at 3.
[102] F. Mogherini, *supra* note 81, at 22.
[103] W. Röhrig and R. Smeaton, 'Viewpoints: Cyber Security and Cyber Defence in the European Union', European Defence Agency (EDA) Opinion (11 June 2014), available at <https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union>.
[104] G. Christou, 'The EU's Approach to Cyber Security', *EU-China Security Cooperation: performance and prospects. Policy Paper Series* (Autumn/Winter 2014), at 6, available at http://eusc.essex.ac.uk/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf>.

following the blurry objectives of the cyber defence policy framework it might be possible to push Member States to enhance defence capabilities on cybersecurity on the technological level and reinforce cooperation on the political level which is enforced in several initiatives for instance the European Defence Fund.[105] Whether these ideas will be implemented remains to be seen in the future.

The area of CSDP – even if not outstanding through milestone regulation – is still politically important. Cybercrime is more than any other issue transnational and requires leaving behind the divisions between 'internal' and 'external' or 'economic' and 'security' policies. As an intersection between internal and external EU policy it might reconcile these ambiguities and lead to more coherence.[106] Lately, the Council acknowledged that implementing the EUGS for the protection of the Union and its citizens requires cooperation with the AFSJ along the nexus of internal and external security in the areas of protection and resilience of networks and critical infrastructure as well as cybersecurity.[107] Also, the EU strives for coordination among policy areas determined in the EUCSS (*see* Table 2 in section 3.2.1). This is supported beyond the demarcation of the CSDP by the EDA working with other EU-level organisations – including ENISA, EC3 and CERT-EU[108] benefitting from synergies in sharing products such as training and exercise material, access to information and expertise as well as the exploitation of national level practice identified, collected and disseminated by other actors.[109] Other recent developments still have to prove whether they are translated into real action plans and capabilities. There is a high probability that more will be achieved in the future in cyber defence since states come to realize that the nature of cyberspace makes traditional arrangements based on national sovereignty less effective.[110] Increased defence cooperation and liaison with security is gaining more attention recently[111] and is also desired by the European Public

[105] J. Solana and S. Blockmans, 'EU defence plan is no "game-changer"', *EU Observer* (Brussels, 16 December 2016), available at <https://euobserver.com/opinion/136315>.
[106] DG for external policies, *'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU'*, PE 433.828 (2011), at 47, available at <http://www.oiip.ac.at/fileadmin/Unterlagen/Dateien/Publikationen/EP_Study_FINAL.pdf>.
[107] Council of the European Union, *supra* note 84, at 3.
[108] European Parliament, 'Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and Risks for the EU', PE 603.175, *Scientific Foresight Unit (STOA)* (May 2017), at 9, available at <http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf>.
[109] N. Robinson, *supra* note 75, 3-4.
[110] K. F. Sliwinski, 'Moving beyond the European Union's weakness as a cyber-security agent', 35 *Contemporary Security policy* 2014, at 482.
[111] *See* for example: European Parliament News, 'EU defence: how Parliament wants to boost cooperation' (6.6.2017), available at <http://www.europarl.europa.eu/news/en/headlines/priorities/20170616TST77649/20170602STO76617/eu-defence-how-parliament-wants-to-boost-cooperation>.

according to a Eurobarometer survey[112]; the cyber defence domain related to the framework of the CSDP is therefore sometimes referred to as the most interesting but unsettled part of cybersecurity in terms of academic research.

3.3 Law Enforcement within the Area of Freedom, Security and Justice

Even though security issues are often connected to the foreign policy realm the European Union explicitly frames security as an objective in Article 3(2) TEU referring to cooperation among Member States in home affairs and justice policies. Being politically sensitive policy areas the willingness by Members to confer powers to the Union has always been constrained which changed partly in the 1990s: With the development of the internal market in the last 25 years the Member States of the European Union came to realize that a purely national conception of judicial policies and internal security would seriously hamper the criminal prosecution and thereby weaken the economy.[113] The notion of economic consolidation and the provision of the European Single Market with its four fundamental freedoms necessarily entailed cooperation in justice affairs with provisions for the internal security for its proper functioning.

Provisions regarding the internal security have been gradually incorporated finding their basis in the 'third pillar' on police and judicial cooperation in criminal matters or since the entry into force of the Lisbon Treaty in the provisions of Title V TFEU defining the AFSJ.[114] Even though this was perceived as a significant step in the integration process the common provisions are unequivocally shaped by intergovernmental interests. The fundamental principle of the AFSJ is the respect for fundamental rights and the different legal systems and traditions of the Member States (Art. 67(1) TFEU) which merely prescribes the harmonisation of laws explicitly for fundamental rights and not uniformed law in general.[115] Similarly the influence of national governments can be seen in the provisions on competent institutions and decision-making procedures. Art. 68 TFEU grants the European Council the right to define strategic guidelines and Art. 69 TFEU reinforces the applicable subsidiarity principle, given the particular political

[112] "68% of Europeans would like the EU to do more on security and defence policy, according to a Eurobarometer survey from March 2017." *See* European Parliament, 'Two years until the 2019 European elections. Special Eurobarometer of the European Parliament', *European Parliamentary Research Service* (April 2017), at 26, available at <http://www.europarl.europa.eu/pdf/eurobarometre/2017/2019ee/two_years_until_ee2019_synthesis_en.pdf>.
[113] R. Bieber *et al., Die Europäische Union Europarecht und Politik* (Baden-Baden: Nomos Verlag, 12th edition 2016) p. 460.
[114] R.A. Wessel, *supra* note 65, at 413.
[115] K.-D. Borchardt, *Die rechtlichen Grundlagen der Europäischen Union. Eine systematische Darstellung für Studium und Praxis* (Wien: Facultas Verlags- und Buchhandels AG, 6th edition 2015), at 585.

relevance of the measures to be taken: They concern not only sovereign core powers but also fundamental rights of citizens. In this sense, further concessions have been made for the Member States in Art. 72 TFEU with the exercise of the responsibilities regarding the maintenance of law and order and the safeguarding of internal security remaining with the states. While these provisions reflect a considerable national influence the EU in the field of AFSJ was also given power to act and adopt legislative measures. As opposed to the CSDP the AFSJ is listed in primary law as one of the policies with a conferred, shared competence between the Union and the Member States (Art. 4(2) j TEU) allowing the Member States to exercise competences only where the Union has not acted yet or decided not to do so. The EU shall act to ensure security through measures to prevent and combat crime, racism and xenophobia, measures for coordination and cooperation between police and judicial authorities and other competent authorities, as well as through the mutual recognition of judgements in criminal matters and, if necessary, through the approximation of criminal laws (Art. 67(3) TFEU).

Despite the broad objectives codified in Article 3(2) TEU the mandate of the EU within the AFSJ is constrained to determined areas which by wording of Article 67 TFEU comprise besides the regulations on the free movement of persons a policy on asylum, immigration and external border control (Chapter 2), judicial cooperation in civil matters (Chapter 3), judicial cooperation in criminal matters (Chapter 4) and police cooperation (Chapter 5).[116] While Article 67 TFEU outlines the general competence to regulate criminal law the proper legal basis on judicial cooperation in criminal matters is given with the *lex specialis* in Article 83 TFEU which allows for the approximation of the laws and regulations of the Member States in the form of establishing

"minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis.

These areas of crime are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money

[116] B. van Vooren and R.A. Wessel, *supra* note 63, at 477.

laundering, corruption, counterfeiting of means of payment, computer crime and organised crime".

Not only is Article 83 TFEU the only explicit reference to computer crime in primary law, it also confers the competence to the European Parliament and the Council to adopt directives. Due to the entry into force of the Lisbon Treaty, the EU now has an explicit competence for legislating in the field of computer crime suitable for the development of EU criminal law legislation.[117] However, this provision is restrained by certain conditions: Firstly, deducing from the wording of Article 67 TFEU the approximation of laws is only listed as 'a last resort' with preferences given to softer measures as coordination and cooperation and the mutual recognition of judgements. Additionally, the norm is only conceding the establishment of *minimum* rules concerning the definition of criminal offences. Directives adopted are therefore quite narrow in their scope confined to minimum ruling. It is therefore unlikely that Article 83 TFEU will serve as a general basis for a comprehensive cybercrime policy approach. Moreover, as analyzed in section 2.2, the conceptualization of 'computer crime' is not followed up and the distinction between 'computer crime' and 'cybercrime' is non-existent. A clarification therefore needs to be adopted based on this article to solve uncertainties. Adding to that and given that the provision only allows for a directive as a legislative act, *"it is up to the individual countries to devise their own laws on how to reach these goals"*.[118] It is especially problematic in the case of cybercrime since a common and coherent conceptualization is required to proceed further; giving the Member States leeway to adjust their laws is likely to resume the fragmentation. These conceptual uncertainties create a certain ambiguity that is deleterious to a unified AFSJ policy being developed and followed by the EU and its composite Member States.[119] Another restriction can be found in paragraph 3 of the respective article which allows members of the Council to suspend the ordinary legislative procedure if a directive would affect fundamental aspects of its criminal justice system. Only in cases of a consensus in the European Council will the ordinary legislative procedure be reopened. If the European Council does not achieve consensus the directive will be suspended; if at least nine member states wish to establish enhanced cooperation on the draft directive this possibility shall be granted for the Member States concerned referring to Article 20(2) TEU and Article 329(1) TFEU. This obvious

[117] H. Carrapiço and B. Farrand, *supra* note 8, at 467.
[118] The distinction of EU legal acts is available at <https://europa.eu/european-union/eu-law/legal-acts_en>.
[119] H. Carrapiço and B. Farrand, *supra* note 8, at 466.

intergovernmental supplement allows finally for sovereign control over an EU provision on cybercrime.

Regarding provisions on cybercrime prevention Article 84 TFEU is applicable which enables the ordinary legislative procedure to *"establish measures to promote and support the action of Member States in the field of crime prevention, excluding any harmonization of the laws and regulations of the Member States"*. While the EU has not clarified which concrete measures fall under the cybercrime prevention realm its competence to act is hereby confined to support the work of Member States. Without the option to harmonise minimum prevention standards prevention under the AFSJ provisions is clearly limited.

Other instrument to further enhance the cooperation in serious criminal matters is the involvement of the two bodies Europol and Eurojust. Europol is referred to among Chapter V on police cooperation and shall support and strengthen action by the Member States' police authorities (Art. 88 TFEU) while Eurojust, established as a judicial coordination unit by Council Decision 2002/187/JHA,[120] is being mentioned in primary law with the mission "*to support and strengthen coordination and cooperation between national investigating and prosecuting authorities in relation to serious crime affecting two or more Member States […]*" (Art. 85 TFEU). Relating to Eurojust, a noteworthy provision is given in Article 86 TFEU which enables the creation of an European Public Prosecutor's Office (EPPO) in order to combat crimes affecting financial interests of the Union. The offences which would fall under the ambit of the EPPO would be specified in a regulation adopted by the Council in the special legislative procedure. However, Art. 86(4) TFEU enables the European Council to adopt a decision extending the powers of the EPPO to include serious crimes having a cross-border dimension. Even though the first proposal on the creation of an EPPO was already adopted in 1997,[121] to this day neither the regulation establishing the EPPO nor a decision extending its competences have been adopted.

[120] Council Decision 2002/187/JHA, *OJ* [2002] L 63/1, 6.3.2002.
[121] M. Coninsx, 'Eurojust News on the creation of a European Public Prosecutor Office', 8 *Eurojust News Issue* (Brussels, May 2013), available at <http://www.eurojust.europa.eu/doclibrary/corporate/Pages/newsletter.aspx>.

On 7 February 2017, the Council registered the absence of the required unanimity in support of the proposal for a regulation creating an EPPO.[122] Member States may proceed with the regulation under the principle of enhanced cooperation but the final decision on this possibility is yet to come. Naturally a decision extending the powers of an EPPO will not be considered before its actual creation. Whether an EPPO would be competent in prosecuting cybercrime is another unknown since the Commission proposal defines financial interest in Article 2(c) as

"all revenues, expenditures and assets covered by, acquired through, or due to the Union budget and the budgets of institutions, bodies, offices and agencies established under the Treaties and budgets managed and monitored by them"

relating only to the EU budget.[123] Still, the provision is worth considering since it could establish the first EU body with prosecutorial and not just coordinating powers allowing the EU to directly defend its own financial interests.[124] A decision by the Council extending the scope of an EPPO to the financial interest of businesses and organisations within Europe might allow for the prosecution of cybercrime. Not least since the attack of *Wannacry* in May 2017[125] European businesses have experienced their subjection to ransomware and subsequent financial losses which might stipulate further efforts to take actions against it.

3.3.1 Instruments derived from AFSJ Provisions

Even in the light of the existence of a competence to harmonise national laws in the realm of computer crime the EU decided to legislate different types of cybercrimes separately, distinguishing effectively between criminal offences which can have a cyber dimension and CIA-crimes. The former type of crimes is regulated in the traditional way with solely single provisions referring to crimes related to ICT. An example for regulating content-related crimes

[122] Council of the EU, 'European Public Prosecutor's Office: Council takes first step towards a possible enhanced cooperation', Press Release (7.2.2017), available at < http://www.consilium.europa.eu/en/press/press-releases/2017/02/07-epo-enhanced-cooperation/?utm_source=dsmsauto&utm_medium=email&utm_campaign=European+Public+Prosecutor%27s+Office+%3a+Council+takes+first+step+towards+a+possible+enhanced+cooperation%3E>.

[123] European Commission, 'Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office' COM (2013) 534 final, 17.7.2013. Since cybercrime up to now mainly entail financial loss for businesses and individuals, these costs would not fall under provisions relating to the EU budget.

[124] B. O'Reilley, ,The European Public Prosecutors Office: An institution built on sand?', *The Boolean,* 2015, available at <http://publish.ucc.ie/boolean/2015/00/OReilly/35/en>.

[125] *WannaCry* is a certain type of ransomware which prevents or limits users from accessing their systems or devices, demanding they pay a ransom, using certain online payment methods and by a set deadline, in order to regain control of their data. In May 2017, it affected a variety of organisations and businesses across Europe and beyond, for example by partially paralyzing rail services in Germany. For further information see for instance Europol at <https://www.europol.europa.eu/wannacry-ransomware>.

can be found in Directive 2011/92/EU on combating the sexual abuse and sexual exploitation of children and child pornography in Article 5.[126] Similarly, Council Framework Decision of 28 May 2001[127] combating fraud and counterfeiting of non-cash means of payment includes provisions on computer-related offences in Article 3. (However, the Commission assessed that many Member States claimed that their national jurisdiction already guarantees that offences related to computers within the meaning of Article 3 are punishable and most Member States used a broad definition of fraud which clearly fail the achievement of concrete definitions of cybercrimes.[128]) Measures taken in the law enforcement realm adopted on Article 83 TFEU are reflecting a patchwork of crime rules risking to leave loopholes with for instance no single EU legislation containing the term 'phishing'. Determination and prosecution of crimes is therefore fragmented and subject to uncertainties.

Even when focusing on the narrow definition of cybercrime as CIA-crimes there are significant challenges to the development of a unified legal position, which the EU is now seeking to rectify[129] as in the 2005 Framework Decision, one of the primary legally binding regulations on attacks against information systems.[130] It clearly refers to the provisions in Title V TFEU on judicial cooperation in criminal matters, explicitly Art. 67, 83(1) TFEU as legal bases.[131] The objective is to *"improve cooperation between judicial and other competent authorities, including the police and other specialised law enforcement services of the Member States, through approximating rules on criminal law in the Member States in the area of attacks against information systems."*[132] But the objectives were not achieved sufficiently for the Commission noted in a review that Member States had implemented the obligations differently impeding comparisons between legal concepts and expressions used and thereby failing to achieve a uniform approach to cybercrime (narrowly defined).[133] Substantial differences between Member States on the interpretation of the Directive combined with general

[126] Directive 2011/92/EU, *OJ* [2011] L 335/1, 17.12.2011.
[127] Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, *OJ* [2001] L149/1, 2.6.2001.
[128] Commission of the European Communities, 'Report from the Commission. Second report based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment' COM (2006) 65 final, 20.2.2006.
[129] H. Carrapiço and B. Farrand, *supra* note 8, at 471.
[130] Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ* [2005] L 69/67, 16.3.2005.
[131] Since the Framework Decision was adopted in 2005, the articles it refers to are not the same as in the Post-Lisbon version of the treaties of 2009. Still, Article 82 in the Lisbon Treaty explicitly names ex. Art. 31 which is also mentioned in the Framework Decision.
[132] Council Framework Decision 2005/222/JHA, *supra* note 124, para (1).
[133] H. Carrapiço and B. Farrand, *supra* note 8, at 471.

uncertainty regarding the definition of cybercrime are impacting upon legal certainty and the protection of individuals, so the European Parliament judged.[134]

Framework Decision 2005/222/JHA was replaced by Directive 2013/40/EU on attacks against information systems.[135] This Directive brought EU efforts closer to the criminal law provisions laid down by the Budapest Convention reproducing and amplifying offences set out in the 2005 Framework Decision and enabling the infliction of penalties.[136] With 83(1) TFEU identified as the appropriate legal basis the EU is competent to establish minimum rules concerning the definition of criminal offences and improving the cooperation of Member States in this domain. Since the different levels of criminalisation and the lack of definitions of cybercrime are of the main challenges, this Directive is of great relevance since it aims at tackling exactly this issue. Especially Articles 2-11 are crucial since these include definitions of important terms used in the Directive and thereby approximate the provision of legal certainty for the Member States.[137] However, based on the definition of cybercrime elaborated in section 2.2 the Directive applies a narrow definition of cybercrimes focusing solely on cyberattacks against information systems: *illegal access to information systems (Article 3), illegal system interference (Article 4), illegal data interference (Article 5) and illegal interception (Article 6).* In fact, the EU refers to measures needed to be taken "*in order to fight cybercrime effectively*" (para. 26) but omits to define what is conceived as cybercrime and subsequently limits itself to provisions on CIA-crimes excluding cyber-enabled crimes. While cybercrime in general is mentioned as a threat it is broken down in subcategories endorsing once again a fragmented approach.

The assessment of this approach reflected in the Directive is varying within the academic discussion. Haase argues that the splitting-up of cybercrime for the pursuance of a fragmented approach will in fact be more effective than a holistic approach since Member States are more likely to approve separate measures instead of a comprehensive cybercrime model law which might easily constitute conflicts with any country's criminal law tradition.[138] Adding to that, advocates of civil liberties object a 'cover-all' approach since this would presumably infringe upon the freedom of expression for the sake of a comprehensive security approach. However,

[134] DG for Internal Policies, 'Fighting cyber crime and protecting privacy in the cloud', PE 462.509 (October 2012).
[135] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against Information systems and replacing Council Framework Decision 2005/222/JHA, *OJ* [2013] L 218/9, 14.8.2013.
[136] M. Fletcher and E. Herlin-Karnell, 'Is there a transatlantic security strategy?', in M. Fletcher et *al.* (eds.), *The European Union as an Area of Freedom, Security and Justice* (Abingdon: Routledge 2017), at 426.
[137] A. Haase, *supra* note 25, at 1.
[138] A. Haase, *supra* note 25, at 5.

a global framework for cybercrime legislation in every conceivable aspect of the term is favored by several scholars arguing that it is the only way towards avoiding the dangers of inconsistent implementation and closing security loopholes.[139] Additionally, as explained in section 2.2 a clear demarcation between distinct types of cybercrimes is not always possible since CIA-crimes might imply concurrent traditional crimes as fraud. Nevertheless, the Directive is a step in the direction of clearing uncertainties towards the conceptualization of cyberattacks and is binding upon Member States to be adopted in their national legislation, reinforced by the possibility to inflict penalties. Also, an additional improvement is the provision to make the reporting of significant cyber incidents defined by the Directive mandatory as well as to collect statistical data on the offences and transmit those to the Commission (Art. 13,14). An effective implementation might minimize the lack of knowledge and help to augment the sparsely documented pool of data on cybercrimes in the EU which was also identified as a threat in section 2.4. A Commission report on the implementation of the Directive's provisions in Member States is due in September 2017.

Beside legislation, one must acknowledge the work of Europol and Eurojust. Within Europol the European Cybercrime Centre (EC3) was launched in 2013 to act as a focal point in responding to cybercrimes through strengthening law enforcement and enhancing intelligence systems as proposed in the EU Internal Security Strategy.[140] Within the institutional structure cybercrime therefore was already prioritized in 2013 and the mandate to tackle cybercrime has been extended since. Even though EC3 remains a supportive coordination hub its work appears to be promising based on two main observations. Firstly, all agencies and bodies created or extended in the realm of cybersecurity are increasingly interconnecting as is Europol with CERTs, internet and financial services companies, anti-malware industry, ENISA and Interpol to name only a few.[141] This network might help to merge different approaches (cybercrime, law enforcement, police cooperation, private security strategies, etc.) into a comprehensive strategy without loopholes. Secondly, the actual work of EC3 produces success with for example the exposure of a Polish organized crime network suspected of online payment scams which was made possible through cooperation among national law enforcement agencies alongside EC3

[139] *See* for example: J.P. Kesan and C.M. Hayes, 'Creating a "Circle of Trust" to further Digital privacy and Cybersecurity Goals', 1475 *Michigan State Law Review* 2014; and H. Carrapico and A. Barrinha, 'The EU as a Coherent (Cyber)Security Actor?', *Journal of Common Market Studies* 2017.
[140] European Commission, '*Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe',* COM (2010) 673 final, 22.11.2010.
[141] European Cybercrime Center – Europol, 'First Year Report', at 32, available at <https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report>.

in May 2017.[142] Similarly, when the ransomware *WannaCry* affected the Union the responsibility to engage with the investigations was taken by ENISA and EC3 in cooperation.

3.3.2 Evaluation

While the assessment of cyber defence within the CSDP indicated the external dimension of security and the absence of EU legislation the AFSJ was given a distinct priority. Among AFSJ the focus is laid on prosecuting cybercrime and law enforcement measures which embodies one EUCSS-pillar. The effectiveness of this pillar shall be evaluated in the following. The admission of a shared competence in the field of AFSJ to facilitate actions of cooperation and coordination up to the explicit competence to establish minimum rules to harmonise national criminal law in Article 83 TFEU basically makes the EU a legislator in the field of computer crime. However, as the limitations to this power have been elaborated above this does not provide for the establishment of a comprehensive cybercrime policy. In fact, the gap between expectations and outcomes caused scholars to question the very existence of the Area of Freedom, Security and Justice in the field of cybercrime.[143] While the statutory provisions seem to be promising the concrete action is marked by reluctant Member States to cede power and consequential litigations in front of the EUCJ[144], long-standing conceptual ambiguity on essential terms and therefore legal uncertainty and the fragmentation of computer crime preventing coherence.

As a result, the EU has made some progress in the field of cybercrime legislation and law enforcement mainly through Directive 2013/40/EU. The main strength of the EU can be seen in its efforts to link the different national judicial systems, harmonize minimum standards and enhance cooperation to close loopholes for criminals. Also, bodies which were launched under the pillar of law enforcement are supporting the EU approach despite limited mandates which might be extended in the future when debating the creation of an EPPO within Eurojust. Despite these efforts a coherent law enforcement strategy is not in sight yet which is mainly due to restricted statutory provisions and the principle of Member States maintaining the monopoly in

[142] Europol, '9 arrested for online payment scams in joint operation with polish police and Europol', *Press Release* (2 June 2017), available at <https://www.europol.europa.eu/newsroom/news/9-arrested-for-online-payment-scams-in-joint-operation-polish-police-and-europol>.
[143] H. Carrapiço and B. Farrand, *supra* note 8, at 461.
[144] *See* for example Case C-176/03 Com vs Council [2005] ECR I-7879, "neither criminal law nor the rules of criminal procedure fall within the Community's competence".

the area of law enforcement.[145] Additionally, the AFSJ faces the criticism of an excessive *securitisation* of policies disregarding fundamental rights concerns.[146] Critics often perceive the incremental subjection of freedom and justice to security and in fact their definition through the security lens as violating the rights of the individuals guaranteed by the EU Treaties.[147] Measures taken within the AFSJ must therefore always be judged by their protection of fundamental rights and data protection.

3.4 Conclusions and Assessment of the EU Security Paradigm

What can be concluded from the assessment of the existing measures within the EU security paradigm above is a fragmented picture on cybersecurity.[148] Despite the Lisbon Treaty and increasing efforts for coherence among policy fields the area of security is still divided within the security paradigm of CSDP and AFSJ and even beyond. The defence realm within CSDP seems to be the weakest regarding concrete cybersecurity measures adopted. Even though the adoption of the strategies in 2003 and 2016 indicated a shift in the security focus which now includes transnational crimes among the threats which shall be covered by CSDP policies, it remains an area with a dominant external dimension and limited internal security provisions. Deliberations on effective defence against cyber threats is mainly focused on the protection of infrastructures belonging to CSDP operations or the global emergence of cyber-warfare and cyber-espionage which are not covered in this thesis. The adoption of the EUCSS is commonly perceived as an essential step assigning cybersecurity to CSDP even though it is confined to 'voluntary cooperation' 'among Member States' limiting the EU to soft instruments as the pooling of information or enhanced cooperation supported by a network of bodies and agencies. Policies are determined by the European Council deciding unanimously. As analysed in section 3.2, the defence part appears to be the most deviant in cybersecurity with efforts for coherence more successful on the informal level through agencies than through common legislation. Moreover, CSDP might serve as a linkage between external and internal security which is intended by the Union including the cooperation with NATO which remains the foundation for collective defence.

Regarding the law enforcement realm among the AFSJ mandate a shared competence is attributed to the EU for constituting an Area of Freedom, Security and Justice which is however

[145] B. van Vooren and R.A. Wessel, *supra* note 63, at 478.
[146] B. van Vooren and R.A. Wessel, s*upra* note 63, at 478.
[147] K. Tuori, *European Constitutionalism*, (Cambridge: Cambridge University Press 2017), at 296.
[148] R.A. Wessel, *supra* note 65, at 419.

constrained by the subsequent provisions (*see* section 3.3). The primary provision to regulate by means of directives is found in Article 83(1) TFEU to establish minimum harmonisation in computer crime. Adopted through the ordinary legislative procedure the basic cybercrime legislations enabling crime prosecution in the EU are based on the AFSJ. Especially Directive 2013/40/EU has to be emphasized in that regard even though it might already constitute the maximum achievable since strong national interests clearly dilute exceeding proposals. Also, the use of Article 83(1) as legal basis addresses the fundamental weakness of the European cyber policy which is the absence of a coherent European understanding of what the concepts of cybersecurity and cybercrime should include.[149]

3.4.1 Prospects for the use of a dual legal basis

Respecting the choice of the correct legal basis and the separation of policy provision is in a legal sense imperative for EU policy making guided by the principle of conferral.[150] Content-wise the stretching of one policy too far in the sphere of influence of the other is clearly prohibited by Article 40 TEU stating that the implementation of one policy shall not affect the application of other EU competences. One might therefore argue that the provisions of primary law deliberately design a fragmented approach including varying policies with clear divisions of responsibilities. Certainly, one might argue that the use of different legal basis provisions lays at the nature of EU action and is applied in other areas as well.[151] Nevertheless, the ongoing effort to achieve coherence between CSDP and AFSJ poses the question whether a dual legal basis might be an option when the measure *"simultaneously pursues a number of objectives or has several components that are indissociably linked without one being secondary and indirect in relation to the other".*[152] However, since the EU itself demarcated defence and law enforcement in the EUCSS, thereby contesting the 'indissociable'- claim, and more importantly is characterized by highly diverging rules and procedures as well as responsible actors and possible instruments within CSDP (*see* section 3.2) and AFSJ (*see* section 3.3) a dual legal basis seems unrealistic. Consequentially, the EU's complex division of powers with its diverging procedures and rules for different policy areas as well as the ongoing struggle with Member States for competences seem to hamper not only the realization of combined AFSJ and CSDP

[149] K. F. Sliwinski, *supra* note 110, at 472.
[150] The constitutional significance of the proper legal basis has been reaffirmed by the EUCJ, see for example: Opinion 1/08 Amendments to EU Schedules of Commitments under GATS [2009] ECR I-11129, para. 110.
[151] One example might be the possibility of dual CFSP-development legal bases, *see* B. van Vooren and R.A. Wessel, supra note 63, at 332.
[152] C-178/03 *Commission* v *Parliament and Council*, paragraph 43.

measures but even of a comprehensive body cybersecurity law.[153] Sliwinski even attests that inconsistencies on the European and between the national levels prevent an effective implementation of cybersecurity strategies and appear *"more than likely to leave the EU toothless in the future".*[154]

Still, it cannot be disputed that the EU has proceeded in the realm of cybersecurity and acknowledged the relevance of efficient policies in the EUCSS. The CSDP's main contribution can be seen in its linkage to external policy and international cooperation as well as improved technical capabilities covered by defence spending. Within the AFSJ the scope of conferred competences has been used to adopt necessary legislation and enhance cooperation even though flaws within the regulations remain. Moreover, the possibility of creating an EPPO for a centralized guidance on criminal investigations as well as increasing participation of agencies indicate first signs of increased effort and coherence. Starting from these limited but still existent possibilities for the EU to act the next chapter shall serve to identify existent provisions outside the traditional security paradigm. The loopholes existent in the security domains and the incorporation of the economic rationale within the cybersecurity structure in the EUCSS raise questions whether other policy areas might complement the current framework.

[153] R.A. Wessel, *supra* note 65, at 425.
[154] K. F. Sliwinski, *supra* note 110, at 472.

4 CYBERSECURITY PROVISIONS BEYOND THE SECURITY PARADIGM

The analysis of the cybersecurity provisions regarding law enforcement and cyber defence within the EU security paradigm gives a mixed impression on the current situation. While the Union certainly has augmented efforts to tackle cyber threats a comprehensive and adequate approach is far from in sight due to the respective limitations inherent to the security areas of CSDP and AFSJ. Still, the EU disposes of further possibilities to implement action which shall be analysed in the following chapter. Under consideration shall be the applicability of internal market measures in complementing EU cybersecurity action and the connections to security policies. Therefore, it is firstly essential to analyse the respective statutory framework to elaborate possible competences. Secondly, measures taken in the field by the EU shall be analysed regarding their setup and impact. Concretely this chapter focuses on two measures, answering *SQ4 'How does Directive 2016/1148 and its application add to the regulatory framework on enforcing cybersecurity?'* which considers a regulatory approach. Additionally, *SQ5 'Which mandate and possible instruments are awarded ENISA in order to combat cybercrime?'* approaches institutional efforts. Since these are evaluative sub-questions an extensive assessment follows the analysis which shall conclude on the contribution of non-security-based policies to the cybersecurity framework. This chapter is based on the appropriate legislative documents and scientific assessments as well as internet sources and commentaries to infer conclusions.

4.1 The Economic rationale as a Complement to the Security Paradigm

Some existing instruments referred to as frontline action for effective cybersecurity are not covered among defence provisions in CSDP nor cybercrime provisions within AFSJ. This third pillar tackles the security of NIS for the economic and societal well-being. The European Commission opts for defining the security of network and information systems in Directive 2016/1148 as 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" (Article 4(2)).

Similar to the economic motives boosting cybersecurity considerations in the 1990s, NIS appeared on the EU's agenda with the beginning of the 21th century.[155] Again, the increasing reliance of the economy on digital infrastructure and the fear of potential disruptions of the smooth functioning of the internal market motivated initial attempts to secure NIS and the development of an Information Society in Europe. Later, the efforts in this field augmented due to reinforced *security* considerations for the development of critical infrastructure protection, closely linked to counter-terrorism.[156] In this sense, Article 114 TFEU has been applied increasingly as a legal basis for NIS instruments which allows for *"measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market"*. Two instruments which refer to this Article shall be analysed in the following.

4.2 The NIS-Directive

Characterized by these considerations is one of the most recent measures adopted in the field of cyberspace. The NIS-Directive[157] concerning measures for a high common level of security of network and information systems across the Union explicitly identifies Article 114 TFEU as the correct legal basis which belongs to Title VII on Common Rules on Competition, Taxation and Approximation of Laws. This provision is geared towards the achievement of the objectives set out in Article 26 TEU allowing for the approximation of national provisions for the proper functioning of the internal market. These objectives which would allow for the usage of Article 114 are the functioning of the internal market comprising an area without internal frontiers and with the free movements of goods, persons, services and capital (Art. 26(2)). Therefore, the Directive refers to the connection to the internal market in the very first paragraph and adds in (3) that *"Network and information systems, and primarily the internet, play an essential role in facilitating the cross-border movement of goods, services and people".* The necessity and applicability of Article 114 is adequately justified.

Similar to the state of law enforcement across Member States the Directive acknowledges the very different levels of preparedness and security as the main reasons leading to a fragmented

[155] One of the first documents on NIS: Commission of the European Communities, *'Communication from the Commission to the Council, European Parliament, EESC and Committee of the Regions: Network and Information Security: Proposal for A European Policy Approach'*, COM (2001) 298 final, 6.6.2001.
[156] DG for External Policies, *supra* note 106, at 32.
[157] Directive (EU) 2016/1148 *OJ* [2016] L 194/1, 19.7.2016.

approach across the Union and therefore insufficient protection of consumers and businesses. Consequentially, the EU demands in this Directive a "*global approach at Union level covering common minimum capacity building and planning requirements, exchange of information, cooperation and common security requirements for operators of essential services and digital service providers"*. It constitutes a juncture of national and Union level measures: In chapter II of the Directive Member States are demanded to create a national framework on the security of network and information systems including a national NIS-strategy and a National Competent Authority (NCA) to monitor the application of the strategy in their territory. However, the Directive is open on how the NCA shall ensure a consistent application of national NIS-strategies requiring states only to provide 'adequate resources' to work in an effective and efficient manner. To ensure cross-border cooperation the creation of a 'single point of contact' is required in every state exercising a liaison function with other Member States authorities, the Computer Security Incident Response Teams (CSIRTs network) and a 'Cooperation Group'. The establishment of national CSIRTs is another requirement in the Directive which shall support early warning mechanisms and the handling of incidents or risks. Member States shall ensure the cooperation and division of tasks between these bodies.

Chapter III initiates the formation of a cooperation network at Union level to coordinate against risks and incidents affecting NIS through the creation of a Cooperation Group and a CSIRTs network.[158] The CSIRTs network will consist of all national CSIRTs which monitor incidents, provide early warning and risk analysis, respond to incidents and cooperate with the private sector and shall exchange information on CSIRTs' services, operations and cooperation capabilities as well as security incidents up to the exploration of further forms of operational cooperation. Alongside the CSIRTs network, a Cooperation Group is established in order to support and facilitate strategic cooperation and the exchange of information as well as to build trust and confidence among Member States. This Cooperation Group will be composed of representatives of the Member States, the Commission, and ENISA with a variety of tasks assigned to it from providing strategic guidance for the activities of the CSIRT to exchanging information and best practises as well as preparing a report assessing the experience gained with the strategic cooperation. The establishment of a cooperation network addresses the need to involve all actors, public and private, within and across Member States to effectively deal

[158] P. Ryan et *al*., 'EU Network and Information Security Directive', *The IT Law Community*, available at <https://www.scl.org/articles/3224-eu-network-and-information-security-directive>.

with cyber threats in a coherent manner.[159] However, the involvement of a variety of stakeholders is at risk of blurring divisions of tasks and even though references to some intersections with ENISA are clarified in the Directive its overall success will be contingent on cooperation efforts and (informal) arrangements between the bodies involved to avoid uncertainties in a threat situation.

In chapter IV and V obligations for security and incident notifications to certain operators are determined. Firstly, market operators of essential services are addressed which shall be identified by Member States along common guidelines. These operators are public or private entities operating in the energy, transport, banking, financial market infrastructures, health, drinking water supply or digital infrastructure sector[160] which provide an essential service for the maintenance of critical societal and/or economic activities dependent on network and information systems and whose services would significantly be disrupted by an incident. All entities which meet these criteria are now obliged to manage the risks posed and "*prevent and minimize the impact of incidents affecting the security of the network and information systems (…) with a view to ensuring the continuity of those services"*.[161] Furthermore, these operators are obliged to notify the competent authority or CSIRT of incidents having a significant impact on the continuity of their services, which was one of the most contested parts of the Directive,[162] and thereby initiating cooperation and coordination within the Union. If the operators of essential services fail to provide information or to implement security policies the competent authority may issue binding instructions which gives importance to the provisions in the Directive. Still, the obligations of chapter IV have been subject of intense debates during the legislative process especially due to the question whether 'key Internet enablers' should be covered by the scope of the Directive.[163][164] In the end, these providers were excluded which limits the impact of the Directive. Chapter V deals with digital service providers (DSPs) who are automatically covered by the Directive if they provide online marketplaces, online search engines and cloud computing services. Similar to the operators of essential services, the DSPs have to take technical and organizational measures to manage the risks posed and prevent and

[159] P. Ryan et *al*., *supra* note 158.
[160] This list of operators of essential services is non-exhaustive and shall be reviewed regularly, *see* Directive (EU) 2016/1148 Art. 23.
[161] Directive (EU) 2016/1148 *OJ* [2016] L194/1, 19.7.2016, Art. 14.
[162] NATO Cooperative Cyber Defence Centre of Excellence, 'Developments in the European Union: NIS Directive, Data Protection Reform, EP's response to U.S. surveillance', *Incyder news* (31 March 2014), available at <https://ccdcoe.org/developments-european-union-nis-directive-data-protection-reform-eps-response-us-surveillance.html>.
[163] P. Ryan et *al*., *supra* note 158.
[164] 'Key Internet enablers' include among others social networks, cloud services and search engines.

minimise the impact of incidents ensuring the continuity of those services as well as notify the competent authority or CSIRT of incidents having a substantial impact on the provision of their services. However, a lighter approach for DSPs is chosen since the Commission will determine the security criteria and Member States will not be able to impose additional more stringent requirements for harmonisation purposes. But besides that, the Directive further enables Member States to proceed beyond minimum harmonisation leaving room for a higher level of security than what is settled as common ground in the Directive. Importantly, the final provisions include the adoption of effective, proportionate and dissuasive penalties in cases of infringement which shall be defined by the Member States. This demands businesses to take the protection of NIS more seriously and fosters an effective enforcement and the Directive's objective to achieve a high common level of security in NIS.

4.2.1 Evaluation of the NIS-Directive

While the European Commission Vice-President Andrus Ansip was praising the NIS-Directive as the "*first comprehensive piece of EU legislation on cybersecurity and a fundamental building block for our work in this area"*[165] it is strictly speaking mainly contributing to the work of the NIS-pillar which is only in combination with law enforcement and cyber defence forming the EU cybersecurity strategy. Still, the NIS-Directive is an ambitious measure providing for a high level of harmonisation of definitions and norms across Member States which has been under-developed throughout cybersecurity in the Union so far. Importantly, it complies with the requirements made in the EUCSS in 2013 on the achievement of cyber resilience ensuring that Member States take the necessary steps to deal with cybersecurity threats, involving the private sector and facilitating information sharing across Member States. The disclosing of security incidents is improved through binding instructions on essential service operators which had been identified as a weakness of the EU's cybercrime agenda.[166] EU action in this field is of importance since the absence of common regulation would enable a 'privatization' of security since providers of essential services are usually private operators. The provisions on the introduction of binding penalties in cases of infringements attaches further importance to the objective.

[165] European Commission, 'Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity', 6 July 2016, available at <http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm>.
[166] H. Carrapiço and B. Farrand, *supra* note 8, at 473.

Given the quite recent adoption of the Directive Member States have time to implement provisions until 9th of May 2018 which is why several questions remain around the implementation. It remains to be seen among other things whether the new setup of bodies will complement or hamper the network of actors in cybersecurity and whether true coherence between Member States concerning the definition of how 'critical' an operator of critical infrastructure is can be achieved. Certainly, varieties in the translation in national law and efforts taken by the Member States as well as the reluctance to share sensitive data will complicate the achievement of harmonisation; nevertheless, if implemented accordingly, the NIS-Directive can be seen as an important step towards the highest possible common security level of network and information systems. Indeed, strengthening the resilience of infrastructures under this Directive might prevent crimes in the future rather than any measures adopted within the limited provisions on crime prevention in Article 84 TFEU on AFSJ. The Directive constitutes a principle instrument for the effective implementation of the Cybersecurity Strategy and its existence is even more remarkable given the highly contested and complex discussion on its adoption in the preparatory stage.[167]

4.3 The European Network and Information Security Agency

When it comes to network and information security issues the creation of the European Network and Information Security Agency (ENISA) was probably the most illustrative and advanced measure taken in the field. ENISA is working with EU Member States to protect Europe's Information Society mainly as a neutral information collecting and sharing platform bridging the gap between policy and operational requirements.[168] The founding document of ENISA is Regulation (EC) No. 460/2004[169] referring in particular to the primary law provision to "*adopt the measures for the approximation of the provisions laid down by law, regulation or administrative action in Member States which have as their object the establishment and functioning of the internal market"*.[170] From the beginning, ENISA was therefore established to improve the security level of NIS to support the smooth functioning of the internal market. To meet the growing requirements on the technical and organisational level Member States

[167] J. Fleming, 'Cybersecurity directive faces uncertain fate in Parliament', *euractiv special report* (7 March 2013), available at <http://www.euractiv.com/section/cybersecurity/news/cybersecurity-directive-faces-uncertain-fate-in-parliament/>.
[168] U. Helmbrecht et *al.,* 'Cyber security: future challenges and opportunities', at 16, available at <https://www.enisa.europa.eu/>.
[169] Regulation (EC) No 460/2004, *OJ* [2004] L 077, 13.3.2004.
[170] European Union Consolidated Versions of the Treaty on European Union and of the Treaty establishing the European Community, *OJ* [2002] C 325/1, 24.12.2002. (Art. 95(1) is now post-Lisbon Article 114 TFEU).

were to be supported by the provision on guidance, advice and assistance within its objectives.[171] In effect, ENISA was established primarily to function as a point of information exchange and enhanced cooperation between stakeholders. Its mandate was further extended firstly by the Regulation (EC) No 1007/2008 and later by Regulation 580/2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.[172] The latest extension was adopted in 2013 which contains the valid provisions for the agency.[173] This latest Regulation shows progress since 2004 due to changing challenges in network and information security and therefore updates and strengthens the work of ENISA.[174] Firstly, the provisions on the concrete tasks show that ENISA's role as an actor was increased. Generally, the tasks have changed from the former focus on the facilitation of cooperation and supporting research to an extended version comprising the support and development of Union policy and law, support the capability building, foster voluntary cooperation and awareness raising among competent public bodies and between stakeholders, support research and development and standardisation, cooperate with Union institutions, bodies, offices and agencies to foster the emerging NIS community as well as contribute to the Union's efforts to cooperate with third countries and international organisations.[175] Especially the objective to "*assist the Union institutions, bodies, offices and agencies in developing policies in network and information security"* is significant since it has no comparable mentioning in 2004 and enables ENISA to assume an active role in the development of Union policy and law by representing its interests and positions.[176] And even the conversant tasks of cooperation are extended by for example expressly proposing cooperation efforts across cybersecurity pillars with law enforcement bodies as Europol. Additionally, the scope can be extended by conferring new tasks to ENISA by legal acts of the Union. These tasks are reflected in the actual initiatives taken by ENISA which comprise among others numerous publications on current incidents, info notes for the public[177] or strategic concepts as well as organising events such as meetings, conferences and workshops, active social media representation and a regular openly accessible newsletter.[178] For the achievement of the tasks and to reflect ENISA's enhanced role the regulation provides for increased financial

[171] Regulation (EC) No 460/2004, *OJ* [2004] L 077, 13.3.2004, at (10).
[172] ENISA, 'About ENISA', available at <https://www.enisa.europa.eu/about-enisa/regulatory-framework>.
[173] Regulation (EU) 526/2013, *OJ* [2013] L 165/41, 18.6.2013.
[174] Regulation (EU) 526/2013, *OJ* [2013] L 165/41, 18.6.2013, at (11).
[175] ENISA, see < https://www.enisa.europa.eu/about-enisa/mission-and-objectives>.
[176] Regulation (EU) 526/2013, *OJ* [2013] L 165/41, 18.6.2013, at Art. 2(2).
[177] One example is the cybersecurity info not on the WannaCry Ransomware with detailed explications and recommendations for individuals affected, see < https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst>.
[178] All this is accessible via the homepage of ENISA, *see* < https://www.enisa.europa.eu/>.

and human resources allocated to ENISA. For the same purpose, the institutional structure is supplemented by the creation of an Executive Board for administrative and budgetary tasks to ensure greater efficiency and effectiveness and the achievement of its strategic objectives.

Still, ENISA remains a body of expertise supporting the crime prevention field in cybersecurity without competence to inspect, directly operate or regulate in contrast to other EU-agencies.[179] It lacks not only formal decision- making power concerning policy issues but also concrete, technical means to improve EU cybersecurity with tasks reduced to *assist, advice, offer, provide, analyze, support, promote* and *facilitate.*[180] *Frontex* as another agency in the field of internal security promotes, coordinates and develops European border management with tasks including among others vulnerability assessments (similar to ENISA's threat landscape assessment) or developing technical standards but also the coordination and organisation of joint operations and rapid border interventions. Much more than providing expertise *Frontex* has operational capabilities at hand drawing on staff which is seven times as large as in the case of ENISA.[181] Similarly, with a budget reaching €322 million in 2020 compared to around €11.1 million for ENISA in 2016 *Frontex*'s impact and capabilities easily exceed ENISA.[182] Also, the mandate of ENISA is still timely limited and dependent on the evaluation whether assigned objectives, mandates and tasks have been achieved which impedes long-term planning and the creation of reliability. Furthermore, the selected location in Greece is not conducive to the aim of enforce cooperation with other bodies settled in Brussels (EDA) or The Hague (EC3).

4.3.1 Evaluation of the work of ENISA

The shortcomings of ENISA can mainly be tied back to the EU itself. While the principle of not prejudicing competences of Member States and especially not affecting activities concerning public security is comprehensible given the delicate division of competences between the Union and its Members other restrictions are harder to justify. The abundance of tasks does not belie the fact that ENISA remains an advisory agency in support of Member States and Institutions which was often concealed by political rhetoric.[183] Furthermore, with

[179] ENISA, *see* <https://www.enisa.europa.eu/faq-on-enisa/general-faqs-on-enisa>.
[180] J. Ruohonen et *al.,* 'An outlook on the institutional evolution of the European Union cyber security apparatus', 33 *Government Information Quarterly* 2016, at 750.
[181] There are around 60 staff members working for ENISA, *see* <https://www.enisa.europa.eu/faq-on-enisa/general-faqs-on-enisa>.
[182] ENISA, *see* <https://www.enisa.europa.eu/about-enisa/accounting-finance>.
[183] J. Ruohonen et *al., supra* note 180, at 750.

ENISA's Management Board composed of representatives by the Member States and the Commission its action will most likely follow the interests of national governments. The reluctance to establish a permanent network and information security agency and invest an appropriate level of financial and human resources creates reasonable doubts on the seriousness of the EU to strengthen cybersecurity arrangements. Regarding the protection of EU borders by *Frontex* the efforts and means allocated are to a considerable degree higher than the protection of network and information systems which is irrational given the imminent risk. Comparing only the financial resources allocated to cybersecurity to the USA European efforts appear extremely weak: ENISA's annual budget worth €11 million is just a fraction of the proposed US budget including a $ 3.1 billion Information Technology Modernization Fund enabling agencies to modernize IT infrastructure and networks.[184] The insufficiency of allocated resources has been a recurring point of criticism and leads to the current needs in improving NIS in Europe exceeding by far what ENISA can provide with its current remit and available resources.[185]

Still, with the existent resources ENISA has managed to develop itself to an essential actor in the cybersecurity strategy of the EU and is referred to in all relevant EU publications. It actively pursues its tasks and documents the work transparently and extensively on its homepage fostering the awareness raising of the public.[186] The last external evaluation report published in 2015 generally considered that ENISA is positively contributing to the strengthening of NIS.[187] Especially since the creation of EC3 within Europol and the extended mandate of ENISA in 2013 these two agencies have played a major role in the field. With both agencies focusing on different aspects of cybersecurity their cooperation[188] strengthens the institutional architecture.[189] This would further be enhanced if ENISA was assigned an implementing and operational capacity in 2020 similar to the tasks of Europol.[190]

---

[184] The White House, 'Fact sheet: Cybersecurity National Action Plan', Factsheet (09 February 2016), available at <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>.

[185] ENISA, 'Annual Incident Reports 2015', at 57, available at <https://www.enisa.europa.eu/publications/annual-incident-reports-2015>.

[186] ENISA, see <https://www.enisa.europa.eu/>.

[187] K. Attström et *al*., 'External Evaluation of ENISA – 2015 Final Report' (Ramboll May 2016), available at <https://www.enisa.europa.eu/about-enisa/annual-ex-post-evaluation-of-enisa-activities/2015/external-evaluation-of-enisa-2015/view>.

[188] Cooperation includes producing joint papers, exercising such as *CyberEurope*, producing good practice guide for CERTs etc.

[189] H. Carrapiço and B. Farrand, *supra* note 8, at 475.

[190] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Agency for Law Enforcement Cooperation (Europol), *OJ* [2016] L 135/53, 24.5.2016, Art. 4(c).

4.4 Conclusion and Assessment

Even though the measures highlighted in this chapter are not covered by the traditional security policies they still contribute considerably to the regulation of cybersecurity. In line with the underlying idea of the EU being an economic project the smooth functioning of the internal market is serving as a strong motive to foster network and information security. It is even included in the EUCSS as an equal pillar besides defence and law enforcement. In fact, contrary to the fields of CSDP and AFSJ the vertical division of competences within the internal market is not that highly contested which allows for substantive EU action. If the NIS-Directive is implemented correctly by the Member States monitored by the Commission (*see* chapter VII of the NIS-Directive) it will constitute the most advanced regulation in the cybersecurity realm without belonging to the security paradigm. Additionally, it fosters cooperation and mutual trust between Member States. Similarly, ENISA successfully accomplishes its objectives within the bounds of possibility of an advisory body. Only due to the reluctance of Member States and Institutions it has not yet developed into a serious cybersecurity agency with operational capacities as *Frontex* in the realm of border management. This chapter has revealed that NIS issues can be regulated from internal market measures not only to complement the security-based initiatives of the EU, but rather that this approach forms an indispensable part of cybersecurity with neither defence nor law enforcement responding adequately to the resilience of networks.

Still, the realm of the internal market, given that it is in fact an *economic* policy area, does not provide unlimited opportunities to regulate security. Since Article 114 TFEU is the only applicable provision the measures based upon it have to be legitimized adequately to not violate the scope of competences. Especially in this domain, the EU will have to create a balance between enhancing security and thereby economic certainty without imposing additional burden to businesses.

5 CONCLUSION AND FUTURE PERSPECTIVES

In May 2017, European citizens experienced what had been put off as science fiction when rail services in Germany were paralysed and British doctors were blocked from gaining access to patient files:[191] The unknown masterminds behind the ransomware attack *WannaCry* were able to encroach upon fundamental rights of citizens and internal security with minimal logistical efforts. The attack left not only those affected with immense financial losses but also illustrated the serious harm that can be potentially done to the whole of society.

The ever-increasing threat of cybercrime challenges the values and fundamental objectives of the EU among which are the rule of law and the security of the citizens. Moreover, it affects Human Rights and strategic functions of the states and the EU which is why effective action in the field is imperative. Therefore, this thesis wishes to assess the extent to which the existing EU cyberspace framework is contributing to a coherent and effective cybersecurity policy of the Union by assessing certain EU policy areas. With the introductory chapter reflecting on the background and societal relevance of the topic it became evident that the impact of digital revolution is twofold between advancement and threat potential. Furthermore, the requirements for cybersecurity approaches are complex which challenges governments and law enforcement. A review of relevant scientific publication revealed persistent uncertainties concerning the conceptualization of cybercrime and the ongoing struggle for an effective and coherent cybersecurity approach.

In that regard, the second chapter conceptualized and demarcated the terms of cybercrime, cybersecurity and critical infrastructure as an essential step before assessing the threat potential of crimes and the weakness of related responses. Cybercrimes cover CIA-crimes, computer-related and content-related crimes which are challenging due to the lack of clear definitions, their borderless nature, the quick technical changes as well as the minimal resources needed to cause damage. Since traditional crime law is ill-fitted to face these crimes effective cybersecurity policies are in need to prevent crimes harming the critical infrastructure of Europe.

Within the third chapter the two traditional security policy areas of the CSDP and the AFSJ were analysed respectively in terms of their statutory provisions in primary law and the

[191] R. Goldman, 'What We Know and Don't Know About the International Cyberattack', *The New York Times,* 12 May 2017. The British and the German case are only two of many examples of affected services worldwide.

measures that were taken on that basis responding to sub-question 2 and 3. While it is acknowledged that the EU is taking cybersecurity seriously and has put forward ideas and strategies for Union Policy of which the EUCSS is identified as the most important one the limitations within these policies are equally obvious. While the defence-driven and externally oriented focus of the CSDP is primarily concentrating on cyber-warfare and the protection of military infrastructures its main contribution can be seen in merging the internal cybersecurity efforts of the Union with the external dimension and cooperation with international partners such as NATO. Otherwise, defence within Europe remains a nationally determined area. Even though this is also visible within the AFSJ, the provisions underlying allow for more EU action up to the approximation of criminal laws based on Article 83(1) TFEU which was translated into action with Directive 2013/40/EU. While this contributed to a harmonised approach towards attacks against information systems certain flaws remain. Importantly, operating on a criminal law rationale, the uncertainties regarding a common definition of cybercrime or cyberattacks are obstructive. Adding to that, while still some progress has been made regarding substantive cybercrime law especially in the realm of law enforcement the dominance of national influence is visible and disturbing coherence. Furthermore, the merging of the two policy areas within common measures seems unlikely due to diverging provisions as for example the disregarding of the European Parliament and the EUCJ among CSDP.

Based on the analysis of the EU security paradigm chapter 4 was meant to highlight a policy approach which might complement a coherent cybersecurity strategy, namely efforts along an economic rationale. The corresponding sub-questions 4 and 5 were answered by framing Directive 1148/2016 and the agency ENISA within their internal market background. Since the security of NIS is inevitably connected to the smooth functioning of the EU economy which is increasingly reliant on digital services Article 114 TFEU is identified as a legitimate legal basis. Proposed by the EUCSS the NIS-Directive was adopted on that Article and constitutes a successful measure on the way to more coherence within the EU. In fact, the internal market provisions are more suitable for the resilience of networks than the limited provisions among AFSJ on the prevention of crime in Article 84 TFEU. For the same objective ENISA was created in 2004 which produced modest accomplishments due to constraints in its construction by the EU itself. While regulations among the internal market are overall successfully contributing to enhanced cybersecurity, an extended usage of these provisions should be eyed discerningly: They should not have the primary purpose of reinforced security entailing the *securitisation* of the economic logic. This is because the concerns raised by Member States and

business operators on interference with business growth and competition due to top-down regulation at European level have to be responded deliberately. Moreover, internal market provisions were initially adopted for the aim of increased *free* movement within the EU.[192] Restricting freedoms for the sake of cybersecurity regulation violates fundamental EU principles.

The purpose of this study was to give answers to the research question: *To what extent is the existing EU regulatory framework on cybercrime contributing to the security of the Union?* In general, the view expressed by EU Commissioner Julian King can be endorsed:

"To conclude, we have done a lot to improve the resilience of our critical infrastructure, thanks to the NIS Directive, but there is still much more to be done to make sure that cybercrime and cyber attacks are no longer an attractive option."[193]

Clearly, there is neither a European 'cover-all' approach to cybersecurity nor the mandate to pursue it. This is not necessarily negative since EU has already proven the ability to successfully tackle issues combining several policy areas. Also, scholars see certain advantages in not pursuing a top-down regulatory approach by the Union. The Union itself acknowledges that *"centralised, European supervision is not the answer*".[194] Still, a purely voluntary, industry-led information-sharing and harmonisation approach as pursued by the USA[195] and proposed by certain scholars is hardly recommendable given what is at stake: Cybersecurity encompasses more than a tool to prevent individuals from financial losses in the virtual domain. The infringement of cybersecurity can also have serious implications up to threatening national security which makes mandatory regulation beneficial. The EU therefore pursues a multi-stakeholder approach spanning across the defence logic within CSDP, law enforcement within the AFSJ and NIS within the Internal Market (*see* Table 2 in section 3.2.1). Even though this might be the first step towards a comprehensive approach it is not coherent in itself, leading to fragmentation and inconsistencies. Especially the diverging provisions on the horizontal level

[192] European Commission on the Internal Market, *see* < https://ec.europa.eu/commission/priorities/internal-market_en>.
[193] European Commission, 'Commissioner King's remarks at the Cyber-security Summit Hessen 2017, 21 June 2017, available at < https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-cyber-security-summit-hessen-2017-cybersicherheits-gipfel-hessen-2017_en>.
[194] European Commission, *supra* note 13, at 17.
[195] P. Ryan et *al*., *supra* note 158.

between the CSDP and AFSJ prevent common measures and no legal basis for full participation in cybercrime exists in the EU Treaties leaving the EU with mainly coordinating tasks.[196] Most strikingly might appear the fact that the EU until now has not established a universal and definite definition of cybersecurity and cybercrime applicable within all areas. Similarly, even though legislative instruments have been adopted to approximate national legislation Member States are still far from harmonised cybercrime laws and effective resilience. Adding to that, the very nature of cybercrime enables rapidly changing and innovative crimes which challenge the EU framework to be outdated by technological developments before legislation is even adopted.[197] The latest illustration of these flaws followed the *WannaCry* attack: It became clear that European infrastructures are not shielded from cyberattacks and hence, citizens are threatened.

Still, the fact that the EU has not managed to find a coherent and effective cybersecurity strategy so far does not preclude the possibility to improve in the future. Undeniably, the European Union is ambitious on expanding efforts on the substantive law and on the institutional level. Several options are still open and leave considerable leeway for improvements even if they are adopted only in a gradual manner.[198] Top priority should be the tight control of the implementation process of the NIS-Directive and a considerable increase in investment. Since technological capabilities within the EU are still insufficient plans of the European Commission such as the launch of a new public-private partnership on cybersecurity that is expected to trigger €1.8 billion of investment by 2020 are contributing to improvement.[199]

Also, resources for agencies should be increased to support their work which has been lacking behind so far. Indeed, the merging of efforts by cybersecurity agencies in all fields might lead to more coherence in the cybersecurity approach than legislative instruments. While regulation often reflects trade-offs between policy areas and conflicts on the vertical division of competences, agencies haven proven that they successfully translate objectives into action even though they will not be a panacea for solving cybersecurity challenges.[200] While the adoption of legislative measures on a dual legal basis of CSDP and AFSJ is highly improbable the cooperation of agencies in these fields – EDA and EC3 – has already been exercised. The

[196] R.A. Wessel, *supra* note 65, at 419.
[197] H. Carrapiço and B. Farrand, *supra* note 8, at 473.
[198] R.A. Wessel, *supra* note 65, at 425.
[199] European Commission, 'Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats', *Press Release* (5 July 2016), available at < http://europa.eu/rapid/press-release_IP-16-2321_en.htm>.
[200] F. Trauner, 'New kids on the CFSP block: The JHA agencies', *European Union Institute for Security Studies (EUISS)* (March 2016).

agencies furthermore support the coherence claim of the CSDP being naturally related to the security domain of AFSJ.[201] The EU can therefore not only be considered as a regulatory cybersecurity actor but also as an institutional cyber-power. This presupposes however a serious commitment by the EU Institutions and Member States to support the increasing formation of a EU cybersecurity body. The recent political developments might promote these efforts: Upheavals in European defence and security policy including discussions on increased defence spending combined with regularly occurring cyberattacks might reinforce cybersecurity efforts. For the EU to remain a credible actor who preserves the security of European citizens serious and coherent commitments for cybersecurity are imperative before the next security agenda approaches in 2020.

Finally, cyberspace is constantly evolving and so are related preventive and reactive policies. A vast amount of unanswered question remains for future researchers to approach, of which one is addressed in section 1.1 and 1.3 concerning the involvement of fundamental rights provisions related to the analysis of cybersecurity. Since a detailed assessment would have gone beyond the scope of this thesis, only short references were included on possible competences based on Article 16(1) TFEU on the right to the protection of personal data and Article 7 (respect for private and family life), 8 (right to protection of personal data) and 11 (Freedom of expression and information) of the Charter of Fundamental Rights. Taking this study as a starting point, further research on the possible involvement of data protection norms in the EU cybersecurity framework can add to that knowledge. Especially for students in European Public Administration there is still much room to find governance solutions to newly emerging technical and security challenges.

[201] European Commission, *'Joint Staff Working Paper: Strengthening Ties between FSJ and CSDP Actors. Proposals for a way ahead'*, SEC (2011) 560 final, 5.5.2011, at 3.

6 BIBLIOGRAPHY

Literature

BOOKS

B. Brewster *et al.,* 'Cybercrime: Attack Motivations and Implications for Big Data and National Security', in B. Akhgar (eds.), *Application of Big Data for National Security: A Practitioner's Guide to Emerging Technologies* (Waltham: Elsevier 2015), 108-127.

B. Van Vooren and R.A. Wessel, *EU External Relations Law. Text, cases and materials* (Cambridge: Cambridge University Press 2014).

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

H. Carrapiço and B. Farrand, 'The European Union's fight against cybercrime', in M. Fletcher *et al*. (eds.), *The European Union as an Area of Freedom, Security and Justice* (London: Routledge 2017), 459-481.

H. Jahankhani *et* al., 'Cybercrime classification and characteristics', in B. Akhgar, *et* al. (eds.), *Cyber Crime and Cyber Terrorism. Investigator's Handbook* (Waltham: Elsevier 2014), 149-164.

K. A. DeTardo-Bora and D.J. Bora, 'Cybercrimes: an overview of contemporary challenges and impending threats', in J. Sammons (ed.), *Threatscape and Best Practices* (Waltham: Elsevier 2016), 119-132.

K-D. Borchardt, *Die rechtlichen Grundlagen der Europäischen Union: Eine systematische Darstellung für Studium und Praxis* (Wien: Facultas Verlags- und Buchhandels AG, 6th edition 2015).

K. Tuori, *European Constitutionalism* (Cambridge: Cambridge University Press 2017).

M.-C. Frunza, *Introduction to the Theories and Varieties of Modern Crime in Financial Markets* (Waltham: Elsevier 2016).

M. Chawki *et al.*, *Cybercrime, Digital Forensics and Jurisdiction* (Cham: Springer 2015).

M. Fletcher and E. Herlin-Karnell, 'Is there a transatlantic security strategy?', in M. Fletcher et *al.* (eds.), *The European Union as an Area of Freedom, Security and Justice* (Abingdon: Routledge 2017), 417-438.

M. Portnoy and S. Goodman (eds.), *Global Initiatives to Secure Cyberspace. An Emerging Landscape* (Springer: New York 2009).

M. van Hoecke (ed.), *Methodologies of legal research. Which kind of method for what kind of discipline?* (Oxford: Hart Publishing Ltd 2011).

R.A. Wessel, ‘Towards EU cybersecurity law: Regulating a new policy field’ in N. Tsagourias and R. Buchan (eds.), *Research Handbook on International Law and Cyberspace* (Cheltenham: Edward Elgar Publishing 2015), 403-425.

R. Bieber *et al.*, *Die Europäische Union. Europarecht und Politik* (Baden-Baden: Nomos Verlagsgesellschaft, 12th edition 2016).

S. Lorenzmeier, *Europarecht schnell erfasst* (Berlin: Springer, 5th edition 2017).

S. Manacorda (ed.), *Cybercriminality. Finding A Balance Between Freedom And Security* (Milan: ISPAC 2012).

JOURNALS

A. Segura Serrano, ‘Cybersecurity: towards a global standard in the protection of critical information infrastructures’, 6 *European Journal of Law and Technology* 2015, 1-24.

A. Shkëmbi and D. Sina, ‘Cybercrime in the Perspective of the European Legal Framework’, 4 *Mediterranean Journal of Social Sciences* 2013, 327-330.

E. Wennerström, ‘EU-legislation and Cybercrime. A Decade of European Legal Developments’, 47 *Scandinavian Studies in Law* 2004, 451-470.

F. Calderoni, ‘The European legal framework on cybercrime: striving for an effective implementation’, 54 *Crime, Law and Social Change* 2010, 339-357.

H. Carrapico and A. Barrinha, ‘The EU as a Coherent (Cyber)Security Actor?’, *Journal of Common Market Studies* 2017, 1-19.

J. Clough, ‘Cybercrime’, 37 *Commonwealth Law Bulletin* 2011, 671-680.

J. Keller-Noellet, ‘The Solidarity Clause of the Lisbon Treaty’s’, *Note Europe,* June 2011.

J.P. Kesan and C.M. Hayes, ‘Creating a “Circle of Trust” to further Digital privacy and Cybersecurity Goals’, 1475 *Michigan State Law Review* 2014, 1475-1560.

J. Ruohonen et *al.,* ‘An outlook on the institutional evolution of the European Union cyber security apparatus’, 33 *Government Information Quarterly* 2016, 746-756.

K. F. Sliwinski, ‘Moving beyond the European Union’s weakness as a cyber-security agent’, 35 *Contemporary Security policy* 2014, 468-486.

M. Piechowicz, ‘Intergovernmental Cooperation and the Idea of Community in the Institutional and Decision-making Sphere of the EU Common Foreign and Security Policy’, 23 *European Review* 2015.

N. E. Marion, ‘The Council of Europe’s Cyber Crime Treaty: An exercise in Symbolic Legislation’, 4 *International Journal of Cyber Criminology* 2010, 699-710.

N. Tocci, 'The making of the EU Global Strategy', 37 *Contemporary Security Policy* 2016, 461-472.

POLICY DOCUMENTS

Commission of the European Communities, *'Communication from the Commission to the Council, European Parliament, EESC and Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime'* COM (2000) 890 final, 26.1.2001.

Commission of the European Communities, *'Communication from the Commission to the Council, European Parliament, EESC and Committee of the Regions: Network and Information Security: Proposal for A European Policy Approach',* COM (2001) 298 final, 6.6.2001.

Commission of the European Communities, *'Report from the Commission. Second report based on Article 14 of the Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment'*, COM (2006) 65 final, 20.02.2006.

Commission of the European Communities, *'Communication from the Commission to the European Parliament, Council and Committee of the Regions: Towards a general policy on the fight against cyber crime'*, COM (2007) 267 final, 22.5.2007.

Council of the European Union, '*Report on the Implementation of the European Security Strategy'*, S407/08 (2008), 11 December 2008.

Council of the European Union, *'EU Cyber Defence Policy Framework',* 15585/14 (2014), 18 November 2014.

Council of the European Union, *'Cover note on the European Union Concept for EU-led Military Operations and Missions'*, 17107/14 (2014), 19 December 2014.

Council of the European Union, *'Council conclusions on implementing the EU Global Strategy in the area of Security and Defence',* 14149/16 (2016), 14 November 2016.

Council of the European Union, *'Note on the Implementation Plan on Security and Defence', 14392/16 (2016), 14 November 2016*.

DG for External Policies, *'Cybersecurity and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU'*, PE 433.828 (2011).

DG for Internal Policies, *'Fighting cyber crime and protecting privacy in the cloud'*, PE 462.509 (2012).

European Commission, '*Communication from the Commission to the European Parliament and the Council: The EU Internal Security Strategy in Action: Five steps towards a more secure Europe',* COM (2010) 673 final, 22.11.2010.

European Commission, *'Joint Staff Working Paper: Strengthening Ties between FSJ and CSDP Actors. Proposals for a way ahead'*, SEC (2011) 560 final, 5.5.2011.

European Commission, *'Joint Proposal for a Council Decision on the arrangements for the implementation by the Union of the Solidarity clause'*, JOIN (2012) 39 final, 21.12.2012.

European Commission, '*Joint Communication to the European Parliament, Council, EESC and Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace',* JOIN (2013) 1 final, 7.2.2013.

European Commission, *'Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union'*, COM (2013) 48 final, 7.2.2013.

European Commission, *'Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office'*, COM (2013) 534 final, 17.7.2013.

European Commission, '*Commission Staff Working Document on an Overview of natural and man-made disaster risks in the EU',* SWD (2014) 134 final, 8.4.2014.

European Commission, '*Communication from the Commission to the European Parliament, Council, EESC and Committee of the Regions: The European Agenda on Security*', COM (2015) 185 final, 28.4.2015.

European Commission, *'Communication from the Commission to the European Parliament, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe',* COM (2015) 192 final, 6.5.2015.

European Council, '*A secure Europe in a better world European Security Strategy'*, 12 December 2003.

European Council, *'The Stockholm Programme – An Open and Secure Europe serving and protecting citizens', OJ* [2010] C 115/1, 4.5.2010.

European Parliament, *'Cybersecurity in the EU Common Security and Defence Policy (CSDP) Challenges and Risks for the EU',* PE 603.175, *Scientific Foresight Unit (STOA),* May 2017.

F. Mogherini, *'Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy'*, June 2016.

INTERNET SOURCES

A. Haase, 'Harmonizing Substantive Cybercrime Law through European Union Directive 2013/40/EU - From European Legislation to International Model Law?', *IEEE Explore Digital Library – First International Conference on Anti-Cybercrime (ICACC)* (2015), available at <http://ieeexplore.ieee.org/document/7351931/>, assessed 26.04.2017.

A. Segal, 'Guest Post: Two Years Later, the EU's Cybersecurity Strategy Stumbles Forward', *Council on Foreign Relations Blog Post* (3 February 2015), available at < https://www.cfr.org/blog-post/guest-post-two-years-later-eus-cybersecurity-strategy-stumbles-forward>, assessed 3.6.2017.

A. Seger, 'The Budapest Convention on Cybercrime 10 years on: Lessons learnt or the web is a web', 16.2.2012, available at < https://rm.coe.int/16802fa3e0>, assessed 10.5.2017.

B. O'Reilley, ,The European Public Prosecutors Office: An institution built on sand?', *The Boolean,* 2015, available at <http://publish.ucc.ie/boolean/2015/00/OReilly/35/en>, assessed 5.6.2017.

C.A. Theohary and J.W. Rollins, 'Cyberwarfare and Cyberterrorism: In Brief', *Congressional Research Service* (27 March 2015), available at < https://fas.org/sgp/crs/natsec/R43955.pdf>, assessed 25.6.2017.

Council of the EU, 'European Public Prosecutor's Office: Council takes first step towards a possible enhanced cooperation', Press Release (7.2.2017), available at <http://www.consilium.europa.eu/en/press/press-releases/2017/02/07-epo-enhanced-cooperation/?utm_source=dsms-auto&utm_medium=email&utm_campaign=European+Public+Prosecutor%27s+Office+%3a+Council+takes+first+step+towards+a+possible+enhanced+cooperation>, assessed 1.6.2017.

D. McGuinness, 'How a cyber attack transformed Estonia', *BBC News,* Tallinn, 27 April 2017, available at <http://www.bbc.com/news/39655415>, assessed 9.6.2017.

ENISA, 'Annual Incident Reports 2015', available at <https://www.enisa.europa.eu/publications/annual-incident-reports-2015>, assessed 15.6.2017.

ENISA, see <https://www.enisa.europa.eu/>, assessed 1.6.2017.

ENISA, see <https://www.enisa.europa.eu/about-enisa/accounting-finance>, assessed 18.6.2017.

ENISA, see <https://www.enisa.europa.eu/faq-on-enisa/general-faqs-on-enisa>, assessed 18.6.2017.

ENISA, see < https://www.enisa.europa.eu/about-enisa/mission-and-objectives>, assessed 18.6.2017.

ENISA, see <https://www.enisa.europa.eu/publications/info-notes/wannacry-ransomware-outburst>, 20.6.2017.

European Commission, 'Commission signs agreement with industry on cybersecurity and steps up efforts to tackle cyber-threats', *Press Release,* 5 July 2016, available at < http://europa.eu/rapid/press-release_IP-16-2321_en.htm>, assessed 20.6.2017.

European Commission, 'Statement by Vice-President Ansip and Commissioner Oettinger welcoming the adoption of the first EU-wide rules on cybersecurity', 6 July 2016, available at <http://europa.eu/rapid/press-release_STATEMENT-16-2424_en.htm>, assessed 29.5.2017.

European Commission, 'European Defence Action Plan: Towards a European Defence Fund' (30 November 2016), available at < http://europa.eu/rapid/press-release_IP-16-4088_en.htm>, assessed 15.6.2017.

European Commission, 'Commissioner King's remarks at the Cyber-security Summit Hessen 2017, 21 June 2017, available at < https://ec.europa.eu/commission/commissioners/2014-2019/king/announcements/commissioner-kings-remarks-cyber-security-summit-hessen-2017-cybersicherheits-gipfel-hessen-2017_en>, assessed 24.6.2017.

European Cybercrime Center – Europol, 'First Year Report', available at <https://www.europol.europa.eu/publications-documents/european-cybercrime-center-ec3-first-year-report>, assessed 8.6.2017.

European Defence Agency, 'Cyber Defence', Fact Sheet, last updated 10 February 2015, available at <https://www.eda.europa.eu/docs/default-source/eda-factsheets/2015-02-10-factsheet_cyber-defence>, assessed 1.6.2017.

European Parliament, 'Two years until the 2019 European elections. Special Eurobarometer of the European Parliament', *European Parliamentary Research Service* (April 2017), available at <http://www.europarl.europa.eu/pdf/eurobarometre/2017/2019ee/two_years_until_ee2019_synthesis_en.pdf>, assessed 20.5.2017.

European Parliament News, 'EU defence: how Parliament wants to boost cooperation' (6.6.2017), available at <http://www.europarl.europa.eu/news/en/headlines/priorities/20170616TST77649/20170602STO76617/eu-defence-how-parliament-wants-to-boost-cooperation>, assessed 10.6.2017.

European Parliament, 'Common Security and Defence Policy', *Fact Sheets on the European Union*, June 2017, available at <http://www.europarl.europa.eu/atyourservice/en/displayFtu.html?ftuId=FTU_6.1.2.html>, assessed 22.6.2017.

European Union, available at <https://europa.eu/european-union/eu-law/legal-acts_en>, assessed 20.5.2017.

Europol, 'Wannacry Ransomware', available at <https://www.europol.europa.eu/wannacry-ransomware>, assessed 17.6.2017.

Europol, '9 arrested for online payment scams in joint operation with polish police and Europol', *Press Release* (2 June 2017), available at <https://www.europol.europa.eu/newsroom/news/9-arrested-for-online-payment-scams-in-joint-operation-polish-police-and-europol>, assessed 17.6.2017.

Eurostat, available at < http://ec.europa.eu/eurostat/statistics-explained/index.php/Internet_access_and_use_statistics_-_households_and_individuals>, assessed 5.5.2017.

F. Trauner, 'New kids on the CFSP block: The JHA agencies', *European Union Institute for Security Studies (EUISS)* (March 2016), available at <http://www.ies.be/user/233>, assessed 20.6.2017.

F. Wamala, 'The ITU National Cybersecurity Strategy Guide' (September 2011), available at <http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf>, assessed 12.5.2017.

G. Christou, 'The EU's Approach to Cyber Security', *EU-China Security Cooperation: performance and prospects. Policy Paper Series* (Autumn/Winter 2014), available at <http://eusc.essex.ac.uk/documents/EUSC%20Cyber%20Security%20EU%20Christou.pdf>, assessed 14.5.2017.

International Telecommunication Union, <http://www.itu.int/en/about/Pages/default.aspx>, assessed 10.5.2017.

J. Fleming, 'Cybersecurity directive faces uncertain fate in Parliament', *euractiv special report* (7 March 2013), available at <http://www.euractiv.com/section/cybersecurity/news/cybersecurity-directive-faces-uncertain-fate-in-parliament/>, assessed 29.5.2017.

J. Keller-Noellet, 'The Solidarity Clause of the Lisbon Treaty's', *Note Europe,* June 2011, available at < http://www.notre-europe.eu/media/tgae20117fkellernoellet.pdf?pdf=ok>, assessed 14.5.2017.

J. Solana and S. Blockmans, 'EU defence plan is no "game-changer"', *EU Observer* (Brussels, 16 December 2016), available at <https://euobserver.com/opinion/136315>, assessed 14.5.2017.

K. Attström et *al*., 'External Evaluation of ENISA – 2015 Final Report' (Ramboll May 2016), available at <https://www.enisa.europa.eu/about-enisa/annual-ex-post-evaluation-of-enisa-activities/2015/external-evaluation-of-enisa-2015/view>, assessed 16.6.2017.

McAfee, 'Net Losses: Estimating the Global Cost of Cybercrime', *Center for Strategic and International Studies* (June 2014), available at <https://www.mcafee.com/de/resources/reports/rp-economic-impact-cybercrime2.pdf>, assessed 21.6.2017.

McConnell International, 'Cyber Crime… and Punishment? Archaic Laws threaten Global Information' (December 2000), at 2, available at < http://www.witsa.org/papers/McConnell-cybercrime.pdf>, assessed 12.5.2017.

M. Coninsx, 'Eurojust News on the creation of a European Public Prosecutor Office', 8 *Eurojust News Issue* (Brussels, May 2013), available at <http://www.eurojust.europa.eu/doclibrary/corporate/Pages/newsletter.aspx>, assessed 4.6.2017.

M. McGuire and S. Dowling, 'Cyber crime: A review of the evidence', *Home Office* (October 2013), available at <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf>, assessed 5.5.2017.

NATO Cooperative Cyber Defence Centre of Excellence, 'Developments in the European Union: NIS Directive, Data Protection Reform, EP's response to U.S. surveillance', *Incyder*

news (31 March 2014), available at <https://ccdcoe.org/developments-european-union-nis-directive-data-protection-reform-eps-response-us-surveillance.html>, assessed 29.5.2017.

N. Robinson, 'EU cyber-defence: a work in progress', European Union Institute for Security Studies (ISS) Brief No. 10 (14 March 2014), available at < http://www.iss.europa.eu/publications/detail/article/eu-cyber-defence-a-work-in-progress/>, assessed 3.6.2017.

P. Ryan et *al*., 'EU Network and Information Security Directive', *The IT Law Community,* available at <https://www.scl.org/articles/3224-eu-network-and-information-security-directive>, assessed 29.5.2017.

R. Goldman, 'What We Know and Don't Know About the International Cyberattack', *The New York Times*, 12 May 2017, available at <https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html>, assessed 16.6.2017.

S. Gordon and R. Ford, 'Cyberterrorism?', *Symantec Security Response White Paper,* available at <https://www.symantec.com/avcenter/reference/cyberterrorism.pdf>, assessed 24.6.2017.

The White House, 'Fact sheet: Cybersecurity National Action Plan', Factsheet (09 February 2016), available at <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan>, assessed 29.5.2017.

U. Helmbrecht et *al.,* 'Cyber security: future challenges and opportunities', at 16, available at <https://www.enisa.europa.eu/>, assessed 20.6.2017.

W. Röhrig and R. Smeaton, 'Viewpoints: Cyber Security and Cyber Defence in the European Union', European Defence Agency (EDA) Opinion (11 June 2014), available at <https://www.eda.europa.eu/info-hub/opinion/2014/06/11/viewpoints-cyber-security-and-cyber-defence-in-the-european-union>, assessed 29.5.2017.

Legislation

INTERNATIONAL

Council of Europe, 'Convention on Cybercrime', *European Treaty Series* No. 185, 23.11.2001.

Resolution adopted by the General Assembly on 21 December 2009, United Nations A/RES/64/211. Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures, 17.3.2010.

EUROPEAN UNION

Consolidated Versions of the Treaty on European Union and of the Treaty establishing the European Community, *OJ* [2002] C 325/1, 24.12.2002.

Consolidated Versions of the Treaty on European Union and the Treaty on the Functioning of the European Union, *OJ* [2012] C 326, 26.10.2012.

Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (2002/187/JHA), *OJ* [2002] L 63/1, 6.3.2002.

Council Framework Decision of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment, *OJ* [2001] L149/1, 2.6.2001.

Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, *OJ* [2005] L 69/67, 16.3.2005.

Council Framework Decision 2008/919/JHA of 28 November 2008 amending Framework Decision 2002/475/JHA on combating terrorism, *OJ* [2008] L 330/21, 9.12.2008.

Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, *OJ* [2011] L335/1, 17.12.2011.

Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against Information systems and replacing Council Framework Decision 2005/222/JHA, *OJ* [2013] L 218/9, 14.8.2013.

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, *OJ* [2016] L 194/1, 19.7.2016.

ECJ, Case C-178/03 *Commission v Parliament and Council* [2006] ECLI:EU:C:2006:4.

ECJ, Case C-176/03 Commission v Council [2005] ECLI:EU:C:2005:542.

European Parliament, 'Resolution on EU mutual defence and solidarity clauses: political and operational dimensions', *OJ* [2015] C 419/138, 16.12.2015.

Opinion 1/08 of the European Court of Justice on Amendments to EU Schedules of Commitments under GATS [2009] ECR I-11129.

Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, *OJ* [2004] L 077, 13.3.2004.

Regulation (EU) No 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004, *OJ* [2013] L 165/41, 18.6.2013.

Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Agency for Law Enforcement Cooperation (Europol), *OJ* [2016] L 135/53, 24.5.2016.