Working paper series No.1

September 2019

CYBERSECURITY IN THE EU

Threats, Frameworks and future perspectives

Laboratory of Intelligence & Cyber-Security

Prepared by Dominika Giantas
Approved by Dr. Andrew N. Liaropoulos

ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ
UNIVERSITY OF PIRAEUS

About the Laboratory

The Laboratory of Intelligence & Cyber-Security was founded in 2015 and provides the Department of International and European Studies, in University of Piraeus, with research and expertise on the fields of intelligence studies and the politics of cyberspace. The Laboratory focuses mainly on the topics of intelligence reform, economic espionage, intelligence, democracy and ethics, oversight of intelligence agencies, cyber-security, cyber-terrorism and cyberspace governance. The Laboratory aims to independently or in cooperation with other higher educational and scientific-research institutions, public institutions, enterprises and civil-society organizations to organize and conduct academic and scientific-research activities in the fields of intelligence and cyber-security.

About the Author

Dominika Helena Giantas graduated from the University of Piraeus with a Bachelor's in International and European Studies. She is a researcher for the Laboratory of Intelligence and Cyber-Security. Among her interests are cybersecurity, terrorism studies and energy security.

Contact: DomiGiantas@outlook.com

List of Abbreviations and Acronyms

ASEAN	Association of South East Asian Nations
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
CEPOL	European Police College
CoE	Council of Europe
CSDP	Common Security Defense Policy
CSIRT	Computer Security Incident Response Team
ECSO	European Cyber Security Organisation
ENISA	European Network and Information Security Agency
EU	European Union
EUROPOL	European Police Office
GDPR	General Data Protection Regulation
ICT	Information and Communication Technology
IPCR	Integrated Political Crisis Response
ISO/ IEC JTC 1	Joint technical committee of the International Organization for Standardization
IT	Information Technology
ITU	International Telecommunication Union
NATO	North Atlantic Treaty Organization
NCCs	National Coordination Centres
NIS Directive	Network and Information Security Directive
OAS	Organization of American States
OASIS	Organization for the Advancement of Structured Information Standards
OECD	Organisation for Economic Co-operation and Development
OSCE	Organisation for Security and Co-operation in Europe
PESCO	Permanent Structured Cooperation
PCJ	Police and Judicial Cooperation
UN	United Nations

Table of contents

Introduction

For several years now, as technology integrates into our lives, security of individuals, organizational and states is challenged by high-profile cyber incidents. Particularly, as the digital era began, it brought new possibilities and positive prospects for communication, trade and businesses. It provided easier and faster access, alleviated transport and several services. More and more daily activities and transactions are conducted through the use of Internet and technological devices. Soon challenges, threats and risks developed in the cyber space, rooted in the acceleration of technology. Virtual attacks are threatening government institutions, critical infrastructure. Sensitive information or personal data are exposed. The digitalization overall can create more fragile and exposed to dangers societies. Obviously, with the utilization and expansion of cyberspace, its security has been addressed as highly important for governmental and non-governmental actors.

Over the past years, the European Union has acknowledged the increasing threats deriving from the nature of our digitally driven world, the reliance on automation and the connection to data. Thus, the EU wants to take the responsibility of cyber security in its own hands by shaping a comprehensive and integral cyber security strategy for its member states as an effort to strengthen the resilience of cyberspace, mitigate the cyber threats and explore all the benefits of digital transformation.

This paper explores the territory of cyber security in the European Union. In the first place, it reflects on the challenge of defining "cybersecurity" by the European Union. Secondly, it maps the cyber security threats which pressed EU to shape a cyber security strategy. Then, it aims to identify the main cyber security capabilities, frameworks and tools of the EU. The last section features the future steps of the European Union towards cyber security and reveals some challenges that the EU member states face in order to achieve a common cyber security policy and cyber security management at the EU level.

1. Cybersecurity: What does it mean to the European Union?

The emergence of cyberspace in the 21st century has been pivotal for our everyday lives, for businesses and services, but has also affected the perception of security, among others in the EU. The continuous innovation, technological advancements, progress of Information and Communication Technologies (ICT) have been merging the fabric of security, by inserting new digital possibilities but also cyber threats and challenges.

In fact, cyberspace constitutes a new arena, complex, multidimensional and not fully explored. Under these circumstances, the effort to conceptualize the term “cyberspace” and thus “cyber security” too, has been ongoing. There is no concise, broadly acceptable definition, which captures the global and multidimensional nature of the term.[1] Although, the existing literature offers a variety of definitions of “cyber security” and several actors including governments, international organizations and institutions have come up with a definition[2], the European Union does not have a shared definition, unified understanding or/ and a collective vision on the “cyber security”.[3] Many EU member states have their own cyber-security strategies and their own conceptualizations of cyber-security.[4]

The EU Cyber Security Strategy: An Open, Safe and Secure Cyberspace does not entail a definition. The same applies for the Cyber security strategy Resilience, Deterrence and Defence: Building strong cybersecurity for the EU, reviewed and adopted in 2017, In 2015, ENISA sought to define cyber security. In its report “Definition of Cybersecurity – Gaps and overlaps in standardization” explored how different actors and numerous stakeholders determine cyber security. For instance, the report *mentions* that ISO/IEC JTC1 defines cyber security as “the preservation of confidentiality, integrity and availability of information in the Cyberspace”. Committee on National Security Systems views cyber security as the” Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” The report includes definitions among others by military, standards developing organizations and industry forums. Therefore, the report does not give one definition of the term “cyber security”, while highlights the plurality of existing definitions. At the

[1] (Craigen, Diakun-Thibault, & Purse, 2014, p. 1)

[2] (Craigen, Diakun-Thibault, & Purse, 2014, p. 1) and (Luiijf, Besseling, & de Graaf, 2013, pp. 5-7)

[3] (Sliwinski , 2014 , p. 3)

[4] (Sliwinski , 2014 , p. 3)

same time, ENISA identifies the several domains encompassed within the word "cybersecurity".Particularly, it entails communications security, operations security information security, physical security and finally national/public security.

For its own purposes, ENISA defines cybersecurity as "the protection of information, information systems, infrastructure and the applications that run on top of it from those threats that are associated with a globally connected environment".[5]The agency uses a pyramid to illustrate the layers of cybersecurity protection. It denotes that the EU has to ensure all of the aspects of cyberspace and thus, a holistic and multifaceted approach towards cyber security. As the figure 1. depicts, the fundament of the cybersecurity pyramid refers to the basic protection measures, such as cyber hygiene[6], education, awareness which aim to enhance the safety and security of users in cyberspace.

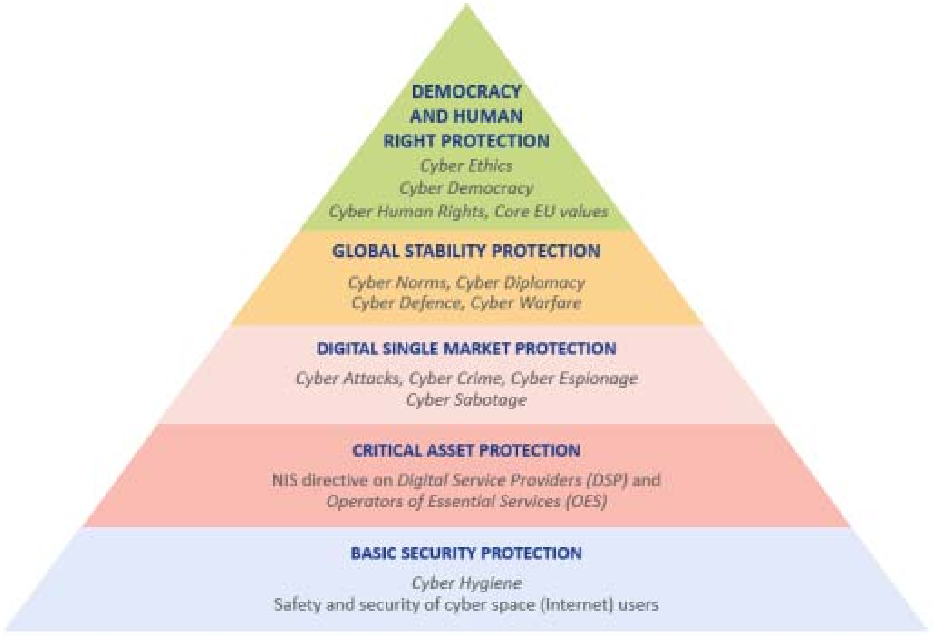
DEMOCRACY
AND HUMAN
RIGHT PROTECTION
Cyber Ethics
Cyber Democracy
Cyber Human Rights, Core EU values
GLOBAL STABILITY PROTECTION
Cyber Norms, Cyber Diplomacy
Cyber Defence, Cyber Warfare
DIGITAL SINGLE MARKET PROTECTION
Cyber Attacks, Cyber Crime, Cyber Espionage
Cyber Sabotage
CRITICAL ASSET PROTECTION
NIS directive on Digital Service Providers (DSP) and
Operators of Essential Services (OES)
BASIC SECURITY PROTECTION
Cyber Hygiene
Safety and security of cyber space (Internet) users

Figure 1. The layers of cybersecurity, Source: [7]

Above this, there is the layer of critical asset protection. The protection of essential services and digital services in sectors such as energy, transport or finance, is enhanced through the NIS Directive, so that the proper functioning of societies and the economic growth are secured.

The third layer, namely the digital single market protection entails measures which protect businesses from cyberspace-related threats such as cybercrime,

[5] (Helmbrecht, Purser, & Ritter Klejn, 2012, p. 13)

[6] Cyber hygiene covers several practices that should be implemented and carried out regularly to protect users and businesses online(ENISA, 2016b, p. 6)

[7] (ENISA, 2017c, p. 4)

cyber espionage and cyber sabotage. This could help EU member states to make up the most from new technologies, and at the same time achieve a safe and trustworthy digital world.

Afterwards, the fourth layer introduces the task of global stability protection, which can be achieved through cyber norms, cyber diplomacy, cyber defense, measures and international agreements to face the challenges of cyber warfare of cyber espionage and thus, contribute to the international order and stability.

Finally, at the top of the cybersecurity pyramid, as conceptualized by ENISA, is the democracy and human rights protection. An integral part of cybersecurity protection is the promotion of EU core values and freedoms in cyberspace, too. In other words, human rights, liberties, democracy and values that EU upholds offline should also apply online.

All in all, ENISA underlines that cybersecurity comprises of two elements: Information security and Network and Information security. This means that cybersecurity covers all aspects of prevention, forecasting; tolerance; detection; mitigation, removal, analysis and investigation of cyber incidents. Additionally, it should cover attributes such as availability, reliability, safety, confidentiality, Integrity, Confidentiality, Maintainability, Robustness, Survivability, Resilience Accountability, Authenticity and Non-repudiation. [8]

However, the understanding of cybersecurity provided by ENISA is not an official and commonly accepted and utilized definition of cybersecurity across the EU. It constitutes one of the many efforts taken in order to determine the term. As a result, many EU member states define individually the meaning of cyber security. For example, Germany defines cyber security as the "the availability of cyberspace and the integrity, authenticity and confidentiality of data in cyberspace".[9]

At the same time, several EU member states have not given a clear definition of the concept (e.g Poland[10]), or have shaped a national cyber security strategy not long ago. For example, Denmark developed its first national cyber security strategy just in 2015 and then review it in 2018.[11] The same delayed response to cyber security incidents applies for some Balkan countries such as Croatia (2015)[12], Bulgaria (2016)[13] and Greece (2017)[14]. The major point is that there exists a significant gap in the EU referring to mutual signification and common standardization and terminology used, among others, the cyber security concept.

[8] (ENISA, 2017c, p. 6)

[9] (Federal Ministry of the Interior, 2011, p. 2)

[10] (Ministry of Digital Affairs, 2017 , p. 7)

[11] (ENISA , 2018a)

[12] (ENISA , 2015)

[13] (ENISA , 2016a)

[14] (ENISA , 2017a)

2. Cyber Incidents which shaped EU cyber security

The gradual involvement of the European Union in the cyber security issues was shaped by some cyber incidents, which constituted unprecedented challenges and had a significant impact on the way in which the EU member states perceived the cyber domain.

To begin with, in 2007 Estonian's Presidency and Parliament, government ministries, political parties, media channels, banks and communication infrastructure [15]were victims of a sustained cyber-attack, believed to be launched from Russia. At that time, Estonia, a country of 1.4 million people and member of both NATO and the European Union, was one of the most wired and advanced societies in Europe and a tech-savvy nation, which fast developed "e-government" services. The country used internet technology for example for voting, education, security and banking.[16] Several government societies were joined together in the virtual world, in the X-road platform[17]. Pernik with Tuohy (2013) notice that the critical infrastructure on which E-stonia relied on was heavily linked with cyberspace, but the government had not shaped a national strategy to protect the cyberspace.[18]

The attacks against Estonian IT infrastructure has been named the world's first cyber war [19], was the first known instance of an entire country being attacked via a massive cyber-offensive.[20] Russ indicates that "it was the first time that a sustained, wholesale and politically motivated e-assault was launched to wreak havoc on a country's entire digital infrastructure".[21]

Until the attack in 2007, the government of Estonia despite being a leading and an advanced e-society, had no big concerns about national cyber security. But the attacks gave the world a wake-up call, by showing that IT systems could be used as an alternative way to spread terror and disruption, that "Internet has become a powerful asymmetric tool for transnational groups who view themselves as disenfranchised and seek to intimidate the nation-states and other actors presumably responsible for their grievances."[22] Cyber-attacks are serious threat to the national security and sovereignty, are not restricted by geographical boundaries and can have high social, political and social impact, by threatening the resilience, functioning and the development of the modern

[15] (Saleem& Hassan, n.d , p. 2)
[16] (Ashmore, 2009, p. 1)
[17] (E-stonia , n.d)
[18] (Pernik & Tuohy, 2013, p. 2)
[19] (Ruus, 2008, p. 1)
[20] (Gordon, 2015, p. 8)
[21] (Ruus, 2008, p. 1)
[22] (Ruus, 2008, p. 1)

state and economy. Nation states received a wake-up call on the new threats emerging from cyber space, alongside with new types of opponents.

All in all, the cyber-attacks which occurred on the government on Estonia were significant, involved a member-state of the EU, but did not result in a common Cyber Security Strategy at the EU level. They progressively captured EU member-states' interest in cyber security issues and provoked discussions, mainly at the national level. This notion is linked mainly to the lack of mutual trust among the EU countries, but also towards the EU institutions and, secondly to the sensitive nature of security related issues, which the EU member states choose to tackle on their own rather than convey as EU competence.

The cyber incidents during the first decade of 21st century (such as the cyber-attack on Estonia, the attacks during the Kosovo war and the Russia-Georgia war) demonstrated that cyber conflicts were becoming commonplace around the world, including Europe and highlighted the emerging need for the national security strategies and policies to competently factor the cyber threat and conflict into all stages of security planning. No longer is the human conflict attached only to physical world. It also occurs in the new domain of cyber space. The cyber threats can often be undetected for a long time, become more and more sophisticated, can have substantial impact on the economy and society, the modern way of life and the national security. Despite the emergence if the cyber threats, the European Union did not have the necessary policies and frameworks to deal with them on a collective EU level. On the contrary, the development of cyber security strategy took place at the national level, of some EU member states.

Specifically, one of the first EU member states to introduce a plan for cyber security was Germany. In 2005, Germany adopted the "National Plan for Information Infrastructure Protection (NPSI)".[23] According to Schallbruch and Skierka (2018), the NPSI was the first IT security-related national strategy in Germany.[24] Moreover, Sweden introduced the "Strategy to improve Internet security in Sweden" and noticeably became the first EU member state to publish a broad national cyber security strategy after the Estonian cyber-attack. [25] The attack on Estonia sparked some attention of several EU countries for policies on cyber security.

In particular, Estonia, the victim of the 2008 attack, shaped a strategy which "sought primarily to reduce the inherent vulnerabilities of cyberspace in the nation as a whole". [26] The Estonian government acknowledged the fact that the

[23] (ENISA , 2012, p. 5)

[24] (Schallbruch & Skierka, 2018, p. 18)

[25] (ENISA , 2012, p. 5)

[26] (Ministry of Defence Estonia , 2008 , p. 3)

coordinated cyber-attacks against national institutions, banks, and media and telecommunication companies clearly demonstrated that, by that time, the security measures undertaken were not sufficient for that purpose and thus, the government needed a new approach and comprehensive plan in order to tackle with vulnerabilities and achieve a better protection of country's cyber assets.

In 2008, Finland and Slovakia shaped a national cyber security plan[27]. Finland perceives cyber security as "a data security issue and as a matter of economic importance that is closely related to the development of the Finnish information society". [28] In Slovakia, the National Strategy for Information Security (NSIS) was implemented until 2013.[29] During the next years, more and more EU member states introduced national strategies and policies for cyber security. For example, in February 2011, the National Cybersecurity Agency of France (ANSSI) published France's Cyberdefence and Cybersecurity Strategy. France also presented a new "French National Digital Security Strategy" in 2015.[30] Germany published its first "Cyber Security Strategy for Germany" in 2011 and updated a new one in 2016. [31]Other member-states such as Poland, Italy, Hungary shaped national cyber security strategies in 2013. Ukraine, in response to the large-scale cyber-attacks on its infrastructure in recent years, adopted in 2016 a National Cyber Security Strategy.[32]

At the EU level, member states witnessed some first steps towards a more comprehensive approach to cyber security issues. Specifically, EU's European Network and Information Security Agency (ENISA) offered expert technical assessments of the developing situation[33]. Moreover, EU member states began to debate new directions for cyber security and the appropriate punishments for states found to have engaged in digital warfare. What is more, as it is mentioned in the European Parliament resolution of 24 May 2007 on Estonia, "the European Parliament calls on the Commission and all the Member States to assist in the analyses of the cyber-attacks on Estonian websites and to present a study on how such attacks and threats might be addressed at EU level; calls on Russia to assist in these investigations to the full"". [34]

In 2008, the Commission launched a public consultation exercise on network and information security policy in Europe. It highlights the need for "a strong, coordinated European response" since, the ICT is the "nervous system of our

[27] (ENISA , 2012, p. 5)

[28] (Dunn, 2005, p. 16)

[29] (Hricikova&Kaska, 2015 , p. 5)

[30] (Gouvernement de la Républiquefrançaise , 2015 , p. 1)

[31] (Federal Ministry of the Interior , 2011 , p. 1)

[32] (Government of Ukraine , 2016)

[33] (Herzog, 2011, p. 54)

[34] (European Parliament , 2007)

modern society" and each country on its own can be very vulnerable. [35] Moreover, the cyber security issues are being addressed under the Third Pillar of EU, namely Police and Judicial Cooperation (PJC). For example, the European Police Office (EUROPOL) may be involved in cyber security tasks at the operational level.[36] In 2009 the European Commission highlighted the importance of the smooth functioning of communications infrastructures for the European economy and society and called for action to protect these critical information infrastructures by making the EU more prepared for and resistant to cyber- attacks and disruptions and welcomed several stakeholders, both public and private bodies to work on issues such as preparedness detection and response to cyber-attacks. [37]

It becomes clear that cyber-attacks, such as the cyber-attack on Estonian government, demonstrated the new international threats emerging from the cyberspace and the difficulties in maintaining order and security in the cyberspace. However, these cyber incidents did not spark a collective interest and effort of EU member -states to propose an EU cyber security strategy and act at a supranational level rather than only individually at a national level. Since the attack in 2007, the cyber security landscape has continued to evolve, welcoming new types of cyber-attacks, new tools and methods of malicious cyber activity, and new cyber actors-threats with different motives, capabilities, targets and tools. In the light of this, the European Union acknowledged that electronic communication services and networks provide the backbone of European economy, that more and more Europeans use actively the Internet and communication infrastructure underpins the functioning of key areas such as energy distribution, water supply, transport, finance and other critical infrastructure. The growing digitalization and cyber-dependency creates greater vulnerability of the infrastructure to cyber-attacks and thus, resulted in EU's effort to prevent and respond to cyber-disruptions and attacks. The Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, introduced in 2013, clarifies EU's vision in the domain of cyber security, clarifies roles and responsibilities and sets out the actions required based on strong and effective protection and promotion of citizens' rights to make the EU's online environment the safest in the world.[38] The 2013 Strategy was accompanied by a proposal for a Network and Information Security (NIS) Directive, namely measures for a high common level of security of network and information systems across the Union.

[35] (Cornish, 2009 , p. 25)

[36] (Cornish, 2009 , p. 25)

[37] (European Commission , 2009)

[38] (European Commission, 2013a, p. 3)

The attack on Ukraine’s power grid in 2015 is the first publicly acknowledged cyberattack against the energy sector, which caused a major power outage[39]. It also highlighted the importance of cyber security specifically in the energy sector, since it constitutes one of the most crucial national infrastructure sectors, correlated to the energy security, but also to the resilience, functioning and the development of the modern state and economy. Some other cyber incidents which took place in the recent years created more serious concerns about the security in the cyber domain at the EU level and enhanced the flare of interest in stronger cooperation of EU member states. Examples of such cyber incidents are major data breaches (e.g from Yahoo), DoS attacks on media platforms such as Twitter and Facebook and on infrastructure in Finland [40] , cyber-attack on German government with malware which infiltrated both the Foreign Ministry and the Defense Ministry, suspicions of Russian involvement in elections and cyber espionage of Norway, Denmark, Netherlands or Italy. [41]

Despite the several serious cyber-attacks with victims EU countries, such as Ukraine, the EU suffered from lack of a cooperation and common stance on cyber security issues. Cyber security incidents have been increasing in frequency, magnitude and sophistication and becoming more complex and threatening to safety and economy. However, the efforts of the EU Member States to cooperate, prevent and respond to cyber-attacks have been fragmented and not consistent enough to deal with the cyber challenges. However, EU showed some signs of more collective approach to the cyber security issues. On July, 2016 the European Parliament adopted the Directive on security of network and information systems or NIS Directive. In brief, the Directive is a set of measures for a high common level of security of network and information systems across the EU[42] and is described as the first piece of EU-wide legislation on cybersecurity.[43] What is more, the General Data Protection Regulation (GDPR) is another piece of legislation passed on an EU level, which completes the European framework for handling cyber security and data protection in the EU. Specifically, the GDPR aims to strengthen citizens' fundamental rights in the digital age and facilitate business by simplifying rules for companies in the Digital Single Market.[44]

Furthermore, the EU adopted the European Agenda on Security 2015-2020 highlights the cybercrime as one of the core priorities, requiring immediate

[39] (Pernik , 2018, p. 61)

[40] (ESET , 2016)

[41] (Limnell, 2018 , p. 69)

[42] (European Parliament , 2016 , p. 1)

[43] (European Commission, 2018f)

[44] (Energy Expert Cyber Security Platform , 2017, p. 5)

action and cross-border and cross sectorial cooperation and coordination. [45] The Digital Single Market Communication of 6th May 2016 stresses the need for a stronger personal data protection and a “partnership with the industry on cybersecurity in the area of technologies and solutions for online network security”. [46]

The landmark for a Cyber Security Strategy for the European Union is the WannaCry attack, and soon after the notPetya attack. The Wannacry attack is perceived as the first ever case of cyber cooperation at the EU level. [47]

In May, 2017 multiple variants of a ransomware named WannaCry have been spreading globally, affecting hundreds of thousands of users, organizations, including users in the European Union. [48] The attack occurred across a wide range of sectors, including health care, government, telecommunications and gas[49], affected more than 150 countries and resulted in damages of up to \$1 billion in one week. [50] Soon after the WannaCry attack, the world witnessed another major cyber-attack known as the notPetya. The attackers used a sophisticated backdoor which was embedded into the Ukrainian accounting software M.E.Doc [51] and soon spread not only across Europe but also infections were observed in another 64 countries, such as Russia, China, India and United States. [52]

The WannaCry attack, one of the largest and most damaging attacks in the history of cybercrime[53], was the first time when Member States of the EU exchanged information on cybersecurity incident within the mechanism for operational cooperation under the NIS Directive.[54] In President Juncker's State of the Union address on 13 September 2017, the Commission and the High Representative proposed to reinforce the EU's resilience and response to cyber-attacks by strengthening the European Union Agency for Network and Information Security (ENISA) and reforming ENISA into a stronger EU Cybersecurity Agency with a permanent mandate, greater operational resources and a stable footing for the future. , creating an EU-wide cybersecurity certification framework, a Blueprint for how to respond to large-scale cybersecurity incidents and crises, and a European Cybersecurity Research and Competence Centre.

[45] (European Commission, 2015b, p. 2)

[46] (European Commission , 2015c)

[47] (ENISA , 2017b)

[48] (ENISA , 2017b)

[49] (EY , 2017 , p. 2)

[50] (Askarifar , Rahman , & Osman, 2018 , p. 25)

[51] (Cherepanov , 2018, p. 2)

[52] (CERT-MU , 2017 , p. 1)

[53] (Askarifar , Rahman , & Osman, 2018 , p. 25)

[54] (Council of the European Union, 2017a, p. 1)

At the same time, EU proposed to develop firstly, a new Directive on the combatting of fraud and counterfeiting of non-cash means of payment to welcome a more efficient criminal law response to cyber–attacks, and secondly, a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and thirdly, some measures which would strengthen the international cooperation on cybersecurity issues. [55] What is more, Europol, via the European Cybercrime Centre put much focus on spreading awareness, through creating information website, disseminating flyers and materials via Europol social media channels. [56] Most importantly, the attack resulted in the formulation of the Cyber Security Strategy for the EU.

To sum up, the WannaCry attack had a great impact on EU's cyber security strategy. It challenged the EU Member States and provoked them to adapt their reaction to the reality of the growing digitalization and interconnectivity of the world and the fast-evolving sophisticated cyber-attacks, to introduce new approaches and measures for stronger private-public partnerships and more effective criminal justice in cyberspace.

The cyber-attacks of notPetya and WannaCry tested the EU operational cooperation and the EU's response to ransomware outbreaks which occurred in 2017, while featured clues of a more synchronized cross-border cooperation and information flow, fast incident response and better recognition and understanding of the cyber threats and the risk management. Most importantly, the attacks were a "wake-up" call for the EU Member States for a new cyber security policy which would bolster EU capabilities to address cyber threats.

In the upcoming years, ENISA assesses that the main trends in the cyber threat landscape could be the increasing complexity and sophistication of the cyber-attacks, malicious actors will become more and more advanced in obfuscation and infrastructure for cyber actions will exploit more the anonymization, encryption and detection evasion, while the financial gains will evolve into the primary motive for malicious cyber actors, usually state-sponsored. Finally, ENISA estimates that the security from cyber risks is robustly becoming linked to skills and capabilities acquisition, to training and education programs within organizations across the EU. [57] Furthermore, ENISA's Executive Director Udo Helmbrecht said: "Global ransomware damage costs are predicted to exceed $11.5 billion annually by 2019, the human attack surface is expected to reach 6 billion people by 2022".[58] These facts highlight the growing concerns of the EU for its security in the cyber domain and, alongside with the cyber events, such

[55] (European Commission , 2017d)

[56] (European Commission , 2017a, p. 2)

[57] (ENISA , 2018b, pp. 112,113)

[58] (Centre for Cyber Security Belgium , 2018)

as the WannaCry ransomware, have shaped significantly the framework and triggered the development of tools and initiatives at the EU level.

3. What has the European Union done so far? Frameworks, policies, tools and initiatives

For the past decade, but especially since 2013, the European Union has developed several policies and tools towards cyber threats and has achieved some success in the cybersecurity governance. The cyber security ecosystem of the EU is based upon the 2013 EU Cyber Security Strategy and the updated Cyber Security Strategy of 2017. The EU focuses on priorities such as achieving cyber resilience, reducing cybercrime, developing cyber defence policy and capabilities related to the Common Security and Defense Policy (CSDP), developing the industrial and technological resources for cybersecurity and finally, establishing a coherent international cyberspace policy for the European Union and promote core EU values.[59]

As cited in Lester cyber resilience refers to "the ability to prepare for, respond to and recover from a cyber-attack." [60]He further explains that cyber resilience is not only prevention of a cyber-attack, but it is also the concern for continuous operation during an attack and the ability to adapt and recover. Towards this goal, the EU is constantly promoting the development of its capabilities and the effective cooperation of both private and public sector, at a national and EU level. Moreover, the UE acknowledges the essential role of information and experiences exchange and coordination and cooperation between sectors. For this reason, the EU established the CSIRTs Network which aims to facilitate the exchange of information and good practices and even explore and identify forms of operational cooperation.

At the heart of the cybersecurity ecosystem of the EU are ENISA and NIS Directive. ENISA (European Network and Information Security Agency) was founded in 2004 as a center of expertise for cyber security in Europe. [61] ENISA is an agency with an important contribution to better understanding the dynamics of cyber security culture. The Agency provides good practices, methodological tools and step-by-step guidance on how to enhance cyber security in the private and public sectors. It is a body of expertise in cyber security, keen to share it within the EU. It also initiated cooperation and information exchange between the Members States and between governments and agents active in the field of NIS. In other words, ENISA has evolved into a

[59] (Hogan Lovells, 2016, p. 5)
[60] (Hogan Lovells, 2016, p. 3)
[61] (European Union, n.d)

broker of knowledge and a switchboard of information. [62] At the same time, ENISA's mandate does not extend to the domains of operational national security, law enforcement and defense, but remains in the prevention field. This means that national bodies and some EU or intergovernmental bodies such as NATO, remain responsible on an operational level for cyber security issues. Even in the light of the extension of its mandate, ENISA remains an agency with limited responsibilities regarding cyber security. [63]

Various stakeholders still see NATO as a more appropriate partner in terms of military aspects of cybersecurity and are sceptic of the benefits of collaboration or see some barriers to the cooperation such as the reluctance and lack of trust from some Member States and, finally, the uncertainty on about ENISA's mandate and capabilities. The opportunities for international cooperation do not limit on NATO or ENISA. Various stakeholders and countries can develop cooperation with UN/ITU, OASIS, Europol or standard developing organizations.

According to Attström, Ludden and Lessmann[64] ENISA's voice in the press, media and general public is weak and not enough heard. The agency also has limited self-assertion and lacks long-term vision as it is too constrained by its mandate and the dominance of the different wills and priorities of EU member states. At the same time there are several structural weaknesses too, which affect ENISA's effectiveness in the EU cybersecurity landscape. ENISA lacks sufficient human and financial resources to complete its various activities at the highest level, while the level of the professionalism, training and skills is not high enough to handle effectively all the task entrusted to the agency. Thus, the role of ENISA in cybersecurity is limited and solely supportive in nature. Operational cyber defence, in practice and on paper, remains the purview of member states.[65]

"The Directive on the Security of Network and Information Systems (the "NIS Directive") is the first EU-wide cybersecurity law. [66]The NIS Directive is at the heart of the EU cyber resilience and a cornerstone of the EU's effort to enhance its cyber security. It can be interpreted as a set of minimum standards for the EU member states regarding cyber security. What is more, this law can result in upscaling cyber capabilities, preparedness, and effective risk management, and enhance cooperation and exchange of information and good practices for cyber security between the EU member states, both the private sector and public

[62] (ENISA, n.d)

[63] (European Commission , 2017c)

[64] (Attström, Ludden, &Lessmann, 2017 , p. 112)

[65] (Attström, Ludden, &Lessmann, 2017 , p. 115)

[66] (European Commission , n.d c)

authorities. [67]It is a tool which could result in a high common level of security of NIS in the EU and avoidance of fragmentation of cyber security measures and practices.

Referring to the cybercrime (According to European Commission's Department of Migration and Home Affairs, "Cybercrime consists of criminal acts that are committed online by using electronic communications networks and information systems".), the borderless and often highly profitable, low-risk danger which becomes increasingly sophisticated and widespread due to the interconnected, digitalized and cyber dependent world, the EU tries to address this issue mainly through legislation (e.g Directive on combating the sexual exploitation[68]) but also through the acquisition of some operational capabilities to combat cybercrime. Specifically, the EU shall provide EU member states with necessary funding, so that they can identify gaps and strengthen their capability to investigate and combat cybercrime. [69] What is more, EU promotes the cooperation with the European Cybercrime Centre (EC3), within Europol, European Police College (CEPOL) and with Eurojust. [70] This can lead to improved coordination at the EU level, by bringing close law enforcement and judicial authorities and public and private stakeholders.

At the same time, the EU recognizes that the aspect of cybersecurity must be included in the spectrum of its market, commerce and economic relations, both internal and external. The innovative ICT products and services produced in the EU and in third countries and used in critical services, infrastructure and mobile devices are trustworthy, secure and guarantee the protection of personal data.[71] This can also contribute to the growth and competitiveness of the EU economy and lead to greater public and private spending on cybersecurity Research and Development (R&D). [72] For these reasons, the EU has come up with the initiative of Digital Single Market, to ensure the free movement of goods, persons, services and capital is ensured and where individuals and businesses can seamlessly access and exercise online activities under conditions of fair competition, and a high level of consumer and personal data protection, irrespective of their nationality or place of residence. [73]

What is more, the EU has approved the European cybersecurity certification framework, which will provide EU-wide certification schemes as a comprehensive set of rules, technical requirements, standards and procedures

[67] (European Commission , 2018b)

[68] (European Commission Migration and Home Affairs , n.d)

[69] (European Commission, 2013a, p. 9)

[70] (European Commission, 2013a, p. 10)

[71] (European Commission, 2013a, p. 12)

[72] (European Commission, 2013b)

[73] (Eurostat , 2019b)

for ICT products and services.[74] This initiative is an important step towards a common EU framework applying in the Digital Single Market. It could also be seen as the first EU law that refers to cyber security of digital products and services, such as Internet of Things devices and that incorporates several security restrictions and characteristics in the design, development and distribution of digital services and goods. For sure, common certification frameworks within the EU can progressively give an end to the fragmentation of legislations and policies among the EU member states and, give space for unified standards and procedures for ICT products and services, which all the EU member states have to comply with.

At present, there is no self-standing policy mechanism for responding to cyberattacks on or within the EU. However, there are two potential policy mechanisms which can be leveraged for a collective EU response to an emerging cyber crisis: the Cyber Diplomatic Toolbox and the Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises.

In 2017, the Council of the EU adopted the draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities namely the Cyber Diplomacy Toolbox. Its aim is to strengthen EU's ability to deter and respond to cyber threats. The toolbox constitutes a set of measures within the Common Foreign and Security Policy, which could be used against malicious operations and threats in cyberspace. Although the Council does not clarify what kind of measures could be taken as diplomatic response to cyber incidents, it highlights that the measures can be "restrictive", if such a necessity occurs.This means that EU has a wide range of instruments, including diplomatic tools such as condemning statements, summoning ambassadors, or declaring diplomats persona non grata[75] , as well as more coercive tools such as imposing sanctions. [76]

As the communication mentions "The EU reminds that attribution to a State or a non-State actor remains a sovereign political decision based on all-source intelligence and should be established in accordance with international law of State responsibility. In that regard, the EU stresses that not all measures of a joint EU diplomatic response to malicious cyber activities require attribution to a State or a non-State actor."[77] This means that the public attribution of a cyber operation is upon the decision of the victim state, while it is not required for the toolbox to be used.

[74] (European Commission , n.d d)

[75] (van der Meer , 2017, p. 1)

[76] (NATO Cooperative Cyber Defence Centre of Excellence, 2017)

[77] (Council of the European Union , 2017b, p. 5)

The initiative of the EU and its member states to adopt such a toolbox of measures can be interpreted as an effort of unifying their diplomatic response to malicious cyber activities and creating a common and comprehensive approach for cyber diplomacy. At the same time, it is a demonstration of encouraged cooperation, greater matchmaking of interests and goals among the EU countries. Finally, it is a new instrument of the EU aspiring to enhance the cyber security within the EU, create more stability in the cyberspace and contribute to threat mitigation and conflict prevention.

The "Blueprint for Coordinated response to large-scale cross-border cybersecurity incidents and crises" within the Integrated Political Crisis Response (IPCR) describes and sets out the objectives and modes of cooperation and coordination between the Member States and EU Institutions, bodies, offices and agencies when responding to large scale cybersecurity incidents and crises, and how the existing Crisis Management mechanisms can make full use of existing cybersecurity entities at EU level. [78] The Blueprint does not cover the full crisis management lifecycle, namely prevention/mitigation, preparedness, response, recovery. It focuses on response at three levels, strategic/political, operational and technical. However, it is the will of the EU member states the decisive factor for the activation of the Blueprint and the Crisis Response Mechanism.[79]

The EU has also prioritized the establishment of a coherent international cyberspace policy for the European Union and thus it promotes dialogue and strong bonds with international actors, organizations, active in the field of cyber security such as NATO[80], OECD and UN[81], as well as with civil society, private sector.[82] In fact, "The EU will seek to promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international laws in cyberspace".[83] Clearly, EU is determined to promote social responsibility, transparency, to illustrate cyberspace as an area of freedom and fundamental rights and launch international cooperation and initiatives in the cyber security domain. [84]

Among the many cooperation schemes that EU has launched in the fields of cyber security and defense, the most prominent is the EU-NATO cyber cooperation. It was shaped recently, just in 2016 with the Joint Declaration. It foresees cooperation between the two institutions in several critical areas, two of which related directly to the cybersecurity, namely countering hybrid threats

[78] (European Commission , n.d a)
[79] (European Commission , 2012 , p. 5)
[80] (European Parliament , 2018)
[81] (International Business Publications , 2013 , p. 123)
[82] (International Business Publications , 2013 , p. 123)
[83] (European Commission, 2013a, p. 15)
[84] (International Business Publications , 2013 , p. 123)

and cyber security and defence.[85] For instance, NATO and EU cyber incident response teams are regularly exchanging policy updates and best practices. They are also increasingly involved in each other's exercises, such as NATO's annual CMX exercise or the Cyber Coalition exercise.[86]

In the light of the changing security environment, the EU pursued its cyber defense under the Permanent Structured Cooperation (PESCO). The participation is voluntary and not EU-wide. [87] The two projects "Cyber Rapid Response Teams and Mutual Assistance in Cyber Security"[88] and "Cyber Threats and Incident Response Information Sharing Platform"[89] promote interstate initiatives for a common cyber defense and crisis management of cyber-attacks. However, they do not address the full spectrum of cyber defense strategies from deterrence to preparedness.[90] Finally, the PESCO projects clearly illustrate a persistent demand for tactical and operational solutions and deeper intestate coordination to effectively handle cybersecurity challenges.[91]

On bilateral basis, EU has opened dialogue and has created cyber partnerships with strategic partners such as US[92], China[93] and India[94], but at the same partnerships with Brazil or South Korea are also in plans.[95] Close relations have also been established with international organizations such as OSCE, CoE, ASEAN and OAS [96] and with CEN CENELEC and ECSO.[97]

According to Renard[98] the EU is interested in developing and extending a network of bilateral cyber-partnerships with key countries, in order to pursue the objectives set by its cyber-strategy, namely strengthening of the EU's own

[85] (European Union External Action, 2018b, p. 1)

[86] (NATO , 2018, p. 1)

[87] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 35)

[88] (European Union External Action , 2018a, p. 1)

[89] (PESCO , n.d)

[90] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 35)

[91] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 35)

[92]The oldest and most developed partnership relies primarily on the Working Group on Cyber-security and Cyber-crime (WGCC), some joint exercises. (Retrieved from: (Renard , 2018 , p. 9)). Recently, it added the AEGIS project on US-EU cybersecurity and privacy dialogue.

[93]The cooperation includes a common cyber taskforce, dialogue on IT, telecommunications and informatisation (From: (Renard , 2018 , p. 10)) , EU-China Information Society Project (EUCISP) (from: (Pawlak & Sheahan, 2014 , p. 4)) and lately the Digital 3 Seas Initiative (from: (Kosciuszko Institute , 2018 , p. 1))

[94]In 2015, EU and India upgraded their consultations to the level of Cyber Dialogue, within the framework of the bilateral Security Dialogue. They also launched the EU-India Agenda for Action 2020 for stronger cooperation among others in cybersecurity ((EU-India Think Tank Twinning Initiative, 2016, p. 1))

[95] (Pawlak & Sheahan, 2014 , p. 1)

[96] (European Commission , 2018a, p. 35)

[97] (CEN-CENELEC , 2018)

[98] (Renard , 2018 , p. 3)

diplomatic and cyber agency and increasing EU's cyber actorness and reaffirming EU's global status and recognition.[99] They also promote global norms of the cyberspace. [100] These cyber-partnerships are necessary for the EU to become a global strategic actor. They favor the integration process of EU's cyber policy and a more coherence and cohesive foreign policy and a common European cybersecurity agenda.

4. The future of cyber security in the European Union

The European societies and economies are more efficient, among others due to the progress of digitalization. More and more sectors, industries, entities and/or individuals adopt digital solutions, introduce new technologies and become interconnected. The Internet has reshaped the structure and functioning of media, energy sector, financial services, manufacturing, agriculture, transport and public services. The Digital Single Market has the potential to improve the access to goods and services, facilitate the growth and innovation. It is estimated that the Digital Single Market can contribute even 415 billion € per year to Europe's economy. [101]

It is clear that technologies give plenty of opportunities. However, the reliance on automation, the escalating digitalization and the integration of technologies in our lives create new unprecedented challenges and vulnerabilities to individuals, entities and governments. Actually, they create a new and constantly changing threat landscape and new entry points for cyber-attacks. Cyber threats have become one of the main security issues for EU and its member states, which acknowledge the danger of technologies and digitalization to their societies, economies, the proper functioning of states and national security. There were more 4,000 ransomware attacks per day in 2016, 80% of European companies experienced at least one cybersecurity incident last year, Security incidents across all industries rose by 38% – the biggest increase in the past 12 years, while in some Member States 50% of all crimes committed are cybercrimes. [102]According to the EU's cyber security factsheet, published in 2018, cyber incidents and attacks are reportedly on the rise. Since 2016, every day there are more than 4,000 ransomware attacks and have increased by 300% since 2015. "Cyber-attacks can be more dangerous to the stability of democracies and economies than guns and tanks. [...] Cyber-attacks know no borders, and no one is immune. highlighted the European

[99] (Renard , 2018 , p. 15)

[100] (Renard , 2018 , p. 3)

[101] (European Commission, n.d b)

[102] (European Commission , 2018g, p. 1)

Commission President Jean-Claude Juncker. That is the reason why, EU and member states have been vigorous in its response to the challenge of cyber security. They have created several EU bodies and agencies, adopted new frameworks, but they do not stop here, since they come up with new initiatives. For example, in the nearest future, EU plans to establish the Network of National Coordination Centres (NCC), a Cybersecurity Competence Community and a European Cybersecurity Industrial, Technology and Research Competence Centre.

As towards a common cyber security management at the supranational level, the strategies, tools and proposed laws, highlight the growing potential of EU as an actor active in the cyber security domain, constitute signs of a common determination and commitment of the EU member states to address cyber security issues at a collective level of EU, and a demonstration the EU and its member states are becoming increasingly interested and involved in common approaches, cooperation and coordination initiatives, as they put more and more emphasis on cyber related topics in the agenda of the EU.

Even the national cyber security strategies of several EU member states have defined the cooperation at the EU level as one of the key objectives for greater cyber security. The best example is Spain. One of the six objectives of its national cyber security strategy is "to contribute to improving cyber security, supporting the development of a coordinated cyber security policy in the European Union and in international organisations, and to collaborate in the capacity building of States that so require through the development cooperation policy". At the same time, it is highlighted that "the National Cyber Security Policy will be aligned with initiatives similar to those of the countries in our neighborhood and with the European and international organizations with responsibilities in this area, particularly the EU Cyber Security Strategy."[103]

Another example is Italy. In its national cyber security strategy, the government refers to the participation in ENISA's cyber security exercises to improve the national preparedness, the goal of reinforcing the protection of critical and strategic ICT communications, supporting the single market, achieving a common cyber resilience capability, developing a cyber defense policy and related operational capabilities, in line with goals and means of the Common Security and Defense Policy and implementing of the objectives pursued by the European Digital Agenda. [104]

The national cyber security strategy of Estonia, clearly mentions "With the goal of promoting the European Union's common cyber security and its policies, joint efforts will be made to raise the cyber capability of Member States and to improve their readiness and ability to deal with new threats." Additionally, "To

[103] (Gobierno de España, 2013 , pp. 4, 22)

[104] (Presidency of the Council of Ministers , 2013 , pp. 22, 23)

ensure collective defense in an international environment, information exchange and cooperation are enhanced with NATO, European Union cyber instances and other partners. Efforts are made concerning the creation and development of NATO joint cyber security capabilities, standards, training and training opportunities."[105]

Despite the progress being made, the EU faces serious obstacles in its effort to achieve in the future a common cyber security policy and cyber security management at the EU level.

Firstly, a significant factor which impedes these ambitions is that cybersecurity issues are linked to national security and sovereignty. They also touch upon the most conceivable aspects of societal, commercial and private life. Therefore, some EU member states assume that those issues should stay within their national security agendas and policies and not become an issue of jurisdiction of EU authorities. They want to limit EU's involvement in the tasks of security and defense and are skeptical towards common responses and collective vision on cyber security. Moreover, they suggest that certain aspects of EU should be stopped or adversed and they should opt out from greater integration in specified areas. On the contrary, some countries push for greater cooperation and even integration in the areas of cyber security and defense. Specifically, they are in favor of a common defense approach and common responses to crisis, since the digital and cyber security matters are globalized and do not respect borders and national sovereignty. In brief, the EU cyber security is at the center of the national vs supranational conflict. And conflicts of how EU member states view the role of EU.

Secondly, common cyber security management at the EU level faces the issue of capabilities gap among EU member states. Member states are at different levels of cyber security development.

Some are immature and at a initial phase when it comes to capabilities, infrastructure, research and development of technologies, cyber security awareness and skills. Christou highlights that some member states have not defined a cyber security strategy or face with problems in developing cyber defense doctrines, organization and training, and obtaining the facilities and infrastructure necessary for effective cyber defense. [106] Other member states, such as France[107], aims to invest more financial and human resources in the national cyber defense and have cyber weapons in their armory. Even when it comes to the implementation of EU frameworks and strategies, many member states fall back. For example, the implementation of NIS Diretive is still in progress for several EU members. In July, 2018 send a letter of formal notice to

[105] (Ministry of Economic Affairs and Communication, 2014, pp. 10,12)

[106] (Christou , 2016, p. 180)

[107] (Mackenzie, 2019, p. 1)

17 member states (such as Poland, Hungary, Netherlands, France etc.) to fully transpose into national law the NIS Directive. [108]According to the Global Cybersecurity Index [109], EU encloses countries both highly committed to cyber security requirements (e.g. Estonia 5th globally, Finland 16th, Netherlands 15th and France 8th) and still maturing (e.g. Austria, Luxemburg, Greece, states of Central and Eastern Europe). In addition, the levels of Internet use still vary greatly across the EU. Particularly, according to Eurostat, in 2017 while more than half of EU citizens access the Internet every day (63%), a substantial minority (24%) say that they never use the Internet or do not have access. The highest levels of Internet use can be seen in Sweden (96%), the Netherlands (95%) and Denmark (94%).[110] Netherlands is also the EU member state to enjoy the biggest Internet access both in 2017 and 2018 (98%). High percentages were also recorded in Denmark (97% and 93%),, Luxemburg (97% and 93%) , Sweden (95% and 92%), Germany (93% and 94%) and Finland (94% in 2017 and 2018). [111] On the contrary member states such as Romania, Greece (76% in 2018), Bulgaria and Lithuania (78% in 2018) have recorded lower levels of Internet use and Internet access. The lowest rate of Internet access among all the EU member states, according to Eurostat was observed in Bulgaria, namely 72% in 2018. [112] At the same time Romania stands out for the largest proportion of respondents who never access the Internet, at over four in ten (41%) of those polled.[113]

The highest proportion (98 %) of households with internet access in 2017 was recorded in the Netherlands, while Denmark, Luxembourg, Sweden, Finland, the United Kingdom and Germany also reported that more than 9 out of every 10 households had internet access in 2017, while the lowest rates have been recorded in among others Bulgaria (67%) , Greece, Croatia and Cyprus. [114]

Respondents in Denmark (76% jointly very well and fairly well informed), Sweden (67%) and the Netherlands (65%) consider themselves to be 'well informed' about cybercrime. By contrast, only 27% of respondents from Bulgaria feel either fairly of well-informed about cybercrime. [115]

[108] (European Commission , 2018e)

[109] Is a reference of International Telecommunications Union which measures the commitment of countries to cybersecurity at a global level to raise awareness of the importance and different dimensions of the issue along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Building, and (v) Cooperation – and then aggregated into an overall score. Retrieved from: (International Communications Union , 2018)

[110] (European Commission, 2015a, p. 7)

[111] (Eurostat, 2018)

[112] (Eurostat, 2018)

[113] (European Commission, 2017b, p. 14)

[114] (Eurostat, 2019a, p. 2)

[115] (European Commission, 2017b, p. 52)

The EU is a union of different speeds and levels of development, knowledge and skills among others in the cyber domain. This disproportion and fragmentation contributes to the fact that EU is not a collective actor in the cyber domain. It also results in unequal level of protection of consumers and businesses, in lack of common requirements on operators of essential services and digital service providers and scar in the overall level of security of network and information systems within the Union

A strong cyber security in the EU overall, requires all member states to be harmonious, to have a common stride, and to keep pace not only with the technological advancements in the cyber domain, but also with each other in order to guarantee a high level of cyber security and an effective management common for the whole Union. Through this way, the EU could reduce or even avoid policy fragmentation, disparities and disadvantages for some EU member states and achieve a common approach and policy of cyber security.

Thirdly, due to the borderless and information-based nature of cyber security, its effective management requires information sharing and exchange of good practices and experiences among EU member states. However, it is inevitable that issues with trust, confidentiality and sensitive cyber security- information sharing may arise. This comes from the fact that cyber domain has become a considerable element of national security strategies of EU member states, and thus, they endeavor to protect any information, procedures and practices which have substantial impact on the security of their societies, economies and governments. The lack of trust can impede any steps towards a common cyber security approach at the EU level and keep the management of cyber security and threats mainly at the level of national strategies and policies.

Additionally, for a few years now, EU is facing unprecedented challenges, which are seen as more urgent and requiring EU immediate action. For instances, the ongoing immigration crisis, the economic difficulties of several EU members, austerity measures and Eurozone crisis, or/and the Brexit and the outcome of the negotiations have overshadowed cyber security topics and absorbed most of the EU' attention. Other trends which have significantly complicated EU's ability to progress as a collective actor in the cyberspace are a heightened terrorism threat, democracy and rule-of-law concerns in some EU member states such as Poland and Hungary and the rise in support for populist, nationalist, antiestablishment, "euroskeptic" parties[116]. Over the last few years, the environment in the EU has changed significantly. The EU experiences serious repercussions and struggles with simultaneous challenges in its security environment. Even the legitimacy, the structure and the character of the EU are questioned by some member states. All these challenge the EU's abilities to

[116] (Archick, 2018, p. 7)

forge common cyber security policies and to further integration in the area of the cyber security, and concurrently render the EU and its institutions politically fragile, economically weak and with uncertain future.

Finally, at the present time the EU has to accept the superiority of NATO in the cyber security and defense domain. NATO's mission is focused on security and defense aspects of cyber security, namely the defense of the Allies, by executing its core tasks: collective defence and deterrence, crisis management, and cooperative security through partnerships. Its primary tasks also encompass the protection of member states and its own organisations, infrastructures, and operations against cyber-attacks.[117]

While each Ally is responsible for its own cyber defences NATO supports its members in boosting these defences. NATO has launched Cyber Coalition, one of the largest cyber defence exercises in the world, and has created the NATO Computer Incident Response Capability and the Cyber Defence Pledge. [118] According to the Alliance, the existing regimes of international law apply to cyberspace and that cyber defense is part of the Alliance's core task of collective defense.[119] This means that an Ally can invoke Article 5 of NATO Treaty, namely the collective self-defense should a cyber-attack have a comparable effect to that of a conventional armed attack. What is more, during the Warsaw Summit in 2016, NATO declared cyberspace as a domain of its operations, similarly to air land and sea.[120] Although NATO has several common actions with the European Union in the field of cyber security, the Alliance has its own cyber security policy and strategy

On the contrary, the EU does not have operational and strategic assets to face cybersecurity issues on EU level. The operational and strategic realities of cyber defense remain located within member states.[121] Moreover, there is no standing model for or independent power to respond to cyberattacks at the EU level.[122] The cooperation within the Common Foreign and Security Policy is essentially intergovernmental. Major decisions of the European Council and the Council of the European Union are taken either by consensus or by unanimity respectively. For the time being, the European agency responsible for the cyber security is ENISA. Its objectives are rather moderate and reactive[123]

The EU's approach is not as security-centered and military-related as NATO's. In fact, the main areas of interest and responsibility for cyber security concerns constitute mainly, some internal security issues, such as data protection, cyber-

[117] (Pernik , 2014 , p. 1)

[118] (NATO , 2019, p. 1)

[119] (De Zan, 2017 , p. 5)

[120] (NATO , 2019, p. 1)

[121] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 42)

[122] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 3)

[123] (Sliwinski , 2014 , p. 6)

crime, internal market, online rights, cyber diplomacy and critical infrastructure protection, and secondly the international cyber cooperation and initiatives. [124] The core responsibilities of defense and security lie with the member states themselves while EU institutions assist, advise, facilitate and support. [125] Thus, EU has rather an advisory role and is a regulator and law-maker. Its role focuses on coordination and cooperation between its member states, the harmonization of policies, and locating resources and capabilities among states and institutions.

The core mandates of both institutions differ and could provide interlocking or complementary functions in increasing European cyber defense capabilities.[126]In terms of cyber defense and offense, states can depend on NATO's capabilities, since the EU does not have a cyber defense posture on its own. The EU' common defense is at an embryonic stage and a work in progress. NATO is successfully integrating cyber defence into operational and contingency planning and exercises, as well as establishing methods and tools to ensure interoperability of cyber capabilities. [127] Compared to NATO, the EU is lagging behind in capabilities, resources, tools and the development of a comprehensive cybersecurity policy. The EU faces the issues of fragmentation across many institutions and actors, lack of trust among member states, EU institutions, various stakeholders and public and private sectors regarding security and finally, the absence of a cohesive strategic vision for security and defense.

To sum up, in the area of cyber domain, the EU plays an advisory rather than a strategic or operational role. The cyber security and defense policies remain in the hands of the EU member states. What is more, existing capabilities are fragmented across the EU member states and resources such as funding, professional staff and facilities are lacking. At the same time, EU member do not a share a common view on the EU's role and future. Subsequently, they are opposed to steps towards supranational management in specific areas touching the sovereignty and national security. This obviously entails the cyber security issues. Besides this, cyber security is not the only challenge that worries theEE. Simultaneously, many crises have arisen in the security environment of EU member states. Notably, the economic crisis and crisis of the Eurozone, the immigration and refugee crisis, the escalating threat of terrorism and nationalist waves in the European countries are the hot concerns for the EU, requiring its immediate response and action. Finally, NATO seems to be a more

[124] (Pernik , 2014 , p. 4)

[125] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 41)

[126] (Pupillo, Griffith, Blockmans, & Renda, 2018, p. 35)

[127] (Pernik , 2014 , p. 5)

valuable asset for member states regarding defense and security in the cyberspace, compared to the limited non-military role of the EU.

5. Concluding remarks

Cyber security is nowadays a very serious issue for individuals, businesses, public and private organizations, governments and states. The digital development of our modern societies has been explosive. In a very short time, our way of life has become unseparated to the technology. Economies, health services and national security and the modern lifestyle are now defined by the technology. The world is digitally driven and confined by data. As technology continues to evolve so also do the opportunities and challenges it provides. The EU is not immune to these threats and becomes a new focal point for cybercrime, industrial espionage, or/and cyberattacks. The security gaps in the EU are large. This has been highlighted by several cyber incidents. Attacks on Estonian government, on Ukraine's power grid, and especially the WannaCry and notPetya provoked an impetus for the introduction of new security measures, the establishment of new agencies and the formulation of a coordinated crisis response at the EU level.

In fact, the EU is following a three-edged approach towards boosting its cyber security. On the one hand, the EU is developing common rules, giving guidance to all EU member states, proposing new regulations and establishing new institution and agencies at the EU level. The best example is the NIS Directive, which is the first piece of EU-wide legislation on cybersecurity. After cyber-attacks on critical infrastructure, democratic institutions and businesses, and the massive ransomware threats of WannaCry and notPetya, it became clear that the EU needed to adapt to the new reality and take a more pro-active approach to cyber threats. As a result a reviewed cyber security strategy was adopted in 2017, together with a package of new proposals. What is more, recently, the EU agreed on the Cyber Security Act and the ambitious plan of upgrading the ENISA and setting up a certification framework. This is very important since it constitutes a standard-setting activity which enhances unity and coherence in the EU territory. In its effort addressing the current cyber security skills gap, the EU focuses on training, education and awareness campaigns.EU also passed in 2017 a framework for joint EU diplomatic response to malicious cyber activities, namely the Cyber Diplomacy Toolbox.

Secondly, the EU strives for innovation, investments in the area of cyber security, capacity building, skills acquisition and technology development. For example, the Commission proposed a total budget of 92 billion € which would be spent on five main areas, namely a) Supercomputers, b) Artificial

Intelligence, c) Cybersecurity and trust, d) Digital skills and e) Ensuring a wide use of digital technologies across the economy and society. [128] Moreover, it proposed to renew the Connecting Europe Facility', with €42.3 billion to support investments in the European infrastructure networks for transport (€30.6 billion), energy (€8.7 billion) and digital (€3 billion).[129]This aims to ensure that all main socio-economic drivers such as schools, hospitals, and transport hubs, main providers of public services and digitally-intensive enterprises have access to future-oriented broadband connections by 2025. [130]
There is a third motion in the EU, the one towards enhanced international cooperation. The cyber international partnerships are a result of two developments at the EU level. Firstly, the EU's ambition and endeavor to become a global strategic actor and increase its presence in the cyber domain too. Secondly, the shaping of an agenda, tools and strategies on cyber issues and the extension of interest, competences and capabilities of the EU in the cyber security. The best example is the Three Seas Initiative, which foresees joint actions and greater cooperation in the cyber domain with NATO or China. Particularly, EU and NATO target at "Active interaction at staff level is proceeding in the field of cyber on concepts and doctrines, existing and planned training and education courses, threat indicators, ad-hoc exchanges of threat alerts and assessments, cross-briefings, including on the cyber aspects of crisis management and regular meetings".[131]

Clearly, the EU has the ambition to play a leading role, both in Europe and internationally. It invests in tools, introduces frameworks, wants to exercise power in the cyberspace, advance EU interests and at the same time stand by its values. However, the EU faces the serious challenges of skills gap and different levels of digital literacy and development across its members, the euro-skepticism towards EU's competences in security and defense issues, the lack of trust and cooperation of its member states, the mix of issues such as Brexit, refugee crisis and economic hardships of some EU countries and the operational and strategic superiority of organization such as NATO, regarding defense and security. All of these create a complex, volatile and unpredictable environment for the EU and baffle EU's effort to have a strong presence in the cyber-related issues. For now, the EU's role in this territory is more formative compared to the dominant powers such as the United States or China, and EU's responses are often diverse, lack coherence and could create conflicts inside the EU.

[128] (European Commission , 2018c)
[129] (European Commission , 2018d)
[130] (European Commission , 2018c)
[131] (European Union External Action, 2018b)

References

Archick, K. (2018, December 3). The European Union: Ongoing Challenges and Future Prospects.*Congressional Research Service*. Retrieved from: https://fas.org/sgp/crs/row/R44249.pdf

Ashmore, W. (2009).Impact of Alleged Russian Cyber Attacks. *Baltic Security &Defence Review. 11* Retrieved from: https://www.bdcol.ee/files/files/documents/Research/BSDR2009/1_%20Ashmore%20-%20Impact%20of%20Alleged%20Russian%20Cyber%20Attacks%20.pdf

Askarifar , S., Rahman , N., & Osman, H. (2018 , July). A Review of Latest WannaCry Ransomware: Actions and Preventions.*Journal of Engineering Science and Technology, 24-33*. Retrieved from: http://jestec.taylors.edu.my/Special%20Issue%20ICCSIT%202018/ICCSIT18_03.pdf

Attström, K., Ludden, V., &Lessmann, F. (2017).*Study on the Evaluation of the European Union Agency for Network and Information Security*. Retrieved from: https://openarchive.cbs.dk/bitstream/handle/10398/9524/EvaluationofENISA-FinalReport.pdf?sequence=1

CEN-CENELEC. (2018, November 13). *Memorandum of Understanding between CEN, CENELEC and the European Cyber Security Organisation (ECSO* . Retrieved from: https://www.cencenelec.eu/News/Press_Releases/Pages/PR-2018-09.aspx

Centre for Cyber Security Belgium. (2018). *CYBERSECURITY IS A SHARED RESPONSIBILITY: 2018 EUROPEAN CYBER SECURITY MONTH KICKS OFF*. Retrieved from: https://www.ccb.belgium.be/en/news/cybersecurity-shared-responsibility-2018-european-cyber-security-month-kicks

CERT-MU. (2017 , June). *THE PETYA CYBER ATTACK* . Retrieved from: http://cert-mu.govmu.org/English/Documents/White%20Papers/PETYA%20CYBER%20ATTACK%20-%20CERTMU%20WHITEPAPER.pdf

Cherepanov , A. (2018, October). GreyEnergy: A successor to BlackEnergy.*ESET White Paper*. Retrieved from: https://www.welivesecurity.com/wp-content/uploads/2018/10/ESET_GreyEnergy.pdf

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

Cornish, P. (2009, February). Cyber-Security and Politically, Socially and Religiously Motivated Cyber-Attacks.*European Parliament*. Retrieved from: http://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/sede090209wsstudy_/SEDE090209wsstudy_en.pdf

Council of the European Union. (2017a, May 31). *Cybersecurity- Information from the Commission*. Retrieved from http://data.consilium.europa.eu/doc/document/ST-9621-2017-INIT/en/pdf

Council of the European Union. (2017b, June 7). *Draft Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")*.nRetrieved from http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014, October). Defining Cybersecurity.*Technology Innovation Management Review.* Retrieved from: https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf

De Zan, T. (2017, September 9). EU-NATO Cyber Cooperation: Who Steps in During a Crisis?.*Cyber Warfare: Challenges and Opportunities,* 7 Retrieved from: https://www.academia.edu/36491546/EU-NATO_Cyber_Cooperation_Who_Steps_in_During_a_Crisis

Dunn, M. (2005, June-July 28-1). A COMPARATIVE ANALYSIS OF CYBERSECURITY INITIATIVES WORLDWIDE.*Center for Security Studies.* Retrieved from: http://www.itu.int/osg/spu/cybersecurity/docs/background_paper_comparative_analysis_cybersecurity_initiatives_worldwide.pdf

Energy Expert Cyber Security Platform. (2017, February). *EECSP Report: Cyber Security in the Energy Sector.* Retrieved from https://ec.europa.eu/energy/sites/ener/files/documents/eecsp_report_final.pdf

ENISA. (2012, May 8). *National Cyber Security Strategies.* Retrieved from https://www.enisa.europa.eu/publications/cyber-security-strategies-paper

ENISA. (2015). *Croatian National Cyber Security Strategy.* Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/croatian-cyber-security-strategy

ENISA. (2016a). *Bulgarian National Cyber Security Strategy.* Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-6

ENISA. (2016b, December). *Review of Cyber Hygiene practices.* Retrieved from https://www.enisa.europa.eu/publications/cyber-hygiene

ENISA. (2017a). *National Cyber Security Strategy of Greece.* Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-cyber-security-strategy-greece/

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

ENISA. (2017c, September). *Overview of cybersecurity and related terminology.* (pp. 4, 6) Retrieved from https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology

ENISA. (2018a). *Danish National Cyber Security Strategy.* Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/national-strategy-for-cyber-and-information-security

ENISA. (2018b, January 15). *ENISA Threat Landscape Report 2017.* (pp. 112-113) Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

ENISA. (n.d). *General FAQ's on ENISA.* Retrieved from https://www.enisa.europa.eu/faq-on-enisa/general-faqs-on-enisa

ESET. (2016 , December 30). *The 10 biggest security incidents of 2016.* Retrieved from https://www.welivesecurity.com/2016/12/30/biggest-security-incidents-2016/

E-stonia.(n.d). *x-road.* Retrieved from https://e-estonia.com/solutions/interoperability-services/x-road/

EU-India Think Tank Twinning Initiative. (2016, December).*Moving forward the EU-India Security Dialogue: Traditional and emerging issues.* Retrieved from https://www.gatewayhouse.in/wp-content/uploads/2016/12/EU-India-Security-Dialogue-Cyber-Security.pdf

European Commission. (2009 , March 30). *Commission acts to protect Europe from cyber-attacks and disruptions.* Retrieved from http://europa.eu/rapid/press-release_IP-09-494_en.htm

European Commission. (2012 , November 14). *A Blueprint to Safeguard Europe's Water Resources.* Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0673:FIN:EN:PDF

European Commission. (2013a, February 7). *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace.*Retrieved from https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission. (2013b, February 7). *Communication on a Cybersecurity Strategy of the European Union – An Open, Safe and Secure Cyberspace.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/communication-cybersecurity-strategy-european-union-–-open-safe-and-secure-cyberspace

European Commission. (2015a, February). *Special Eurobarometer 423: Cybersecurity.*

European Commission. (2015b, April 28). *The European Agenda on Security.* Retrieved from https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf

European Commission. (2015c, May 6). *A Digital Single Market for Europe: Commission sets out 16 initiatives to make it happen.* Retrieved from http://europa.eu/rapid/press-release_IP-15-4919_en.htm

European Commission. (2017a, May 31). *Cybersecurity.*Retrieved from http://data.consilium.europa.eu/doc/document/ST-9621-2017-INIT/en/pdf

European Commission. (2017b, September). *Special Eurobarometer 464a. Report. Europeans' attitudes towards cyber security.* Retrieved from http://data.europa.eu/euodp/en/data/dataset/S2171_87_4_464A_ENG

European Commission . (2017c, September 13). *Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=en

European Commission . (2017d, September 19). *State of the Union 2017: The Commission scales up its response to cyber-attacks.* Retrieved from http://europa.eu/rapid/press-release_MEMO-17-3194_en.htm

European Commission . (2018a). *Operational Guidance for the EU's international cooperation on cyber capacity building.* Retrieved from https://www.iss.europa.eu/sites/default/files/EUISSFiles/Operational%20Guidance.pdf

European Commission. (2018b, May 4). *Questions and Answers: Directive on Security of Network and Information systems, the first EU-wide legislation on cybersecurity.* Retrieved from http://europa.eu/rapid/press-release_MEMO-18-3651_en.htm

European Commission. (2018c, June 6). *EU budget: Commission proposes €9.2 billion investment in first ever digital programme.* Retrieved from http://europa.eu/rapid/press-release_IP-18-4043_en.htm

European Commission. (2018d, June 6). *EU Budget: Commission proposes increased funding to invest in connecting Europeans with high-performance infrastructure.* Retrieved from http://europa.eu/rapid/press-release_IP-18-4029_en.htm

European Commission . (2018e, July 19). *Commission asks Member States to transpose into national laws the EU-wide legislation on cybersecurity.* Retrieved from https://ec.europa.eu/digital-single-market/en/news/commission-asks-member-states-transpose-national-laws-eu-wide-legislation-cybersecurity

European Commission. (2018f, August 24). *The Directive on security of network and information systems (NIS Directive).* Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Commission. (2018g, September 12). *State of Union 2018: Building strong cybersecurity in Europe.* (p. 1) Retrieved from https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-factsheet-cybersecurity_en.pdf

European Commission. (n.d a). *Digital Single Market: Cybersecurity.* Retrieved from https://ec.europa.eu/digital-single-market/en/cyber-security

European Commission. (n.d b). *Shaping the Digital Single Market.* Retrieved from https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market

European Commission. (n.d c). *The Directive on security of network and information systems (NIS Directive).* Retrieved from https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

European Commission. (n.d d). *The EU cybersecurity certification framework.* Retrieved from https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework

European Commission Migration and Home Affairs.(n.d). *Cybercrime.* Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime_en

European Parliament. (2007, May 27). *European Parliament resolution of 24 May 2007 on Estonia.* Retrieved from http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2007-0215+0+DOC+XML+V0//EN&language=EN

European Parliament. (2016, July). *DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL.* (p. 1) Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ:L:2016:194:TOC&uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

European Parliament. (2018, June 11-14). Stepping up EU cyber defence and cooperation with NATO.*News.* Retrieved from:

http://www.europarl.europa.eu/news/en/agenda/briefing/2018-06-11/7/stepping-up-eu-cyber-defence-and-cooperation-with-nato

European Union External Action. (2018a, June 27). *New tool to address cyber threats: the EU's Rapid Response Force.* Retrieved from https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en

European Union External Action. (2018b, November 22). *EU-NATO ooperation - Factsheet.* (p. 1) Retrieved from https://eeas.europa.eu/headquarters/headquarters-Homepage/28286/eu-nato-cooperation-factsheet_en

European Union. (n.d). *European Union Agency for Network and Information Security (ENISA).* Retrieved from https://europa.eu/european-union/about-eu/agencies/enisa_en

Eurostat. (2018, August 17). *Level of internet access - households.* Retrieved from https://ec.europa.eu/eurostat/tgm/table.do?tab=table&init=1&language=en&pcode=tin00134&plugin=1

Eurostat. (2019b, December). E-commerce statistics for individuals.*Statistics Explained.* Retrieved from: https://ec.europa.eu/eurostat/statistics-explained/pdfscache/46776.pdf

Eurostat. (2019a, June). *Digital economy and society statistics - households and individuals.* Retrieved from https://ec.europa.eu/eurostat/statistics-explained/pdfscache/33472.pdf

EY. (2017, May).*"WannaCry" ransomware attack.* (p. 2) Retrieved from https://www.ey.com/Publication/vwLUAssets/ey-wannacry-ransomware-attack/$File/ey-wannacry-ransomware-attack.pdf

Federal Ministry of the Interior. (2011, February).*Cyber Security Strategy for Germany.* (pp. 1, 2) Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy-for-germany

Gobierno de España. (2013). *National Cyber Security Strategy.* (pp. 4, 22) Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/NCSS_ESen.pdf

Gordon, M. (2015, December). LESSONS FROM THE FRONT:A CASE STUDY OF RUSSIAN CYBER WARFARE.*AIR COMMAND AND STAFF COLLEGE AIR UNIVERSITY.* (p. 8)Retrieved from: https://apps.dtic.mil/dtic/tr/fulltext/u2/1040762.pdf

Gouvernement de la Républiquefrançaise.(2015). *French Digital National Security Strategy.*Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/France_Cyber_Security_Strategy.pdf

Government of Ukraine. (2016). *CYBERSECURITY STRATEGY OF UKRAINE.* Retrieved from https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&ved=2ahUKEwiShpWs8ZXhAhVGalAKHSs9ArkQFjACegQIBRAC&url=https%3A%2F%2Fdefense-reforms.in.ua%2Fen%2Fdownload%3Fpath%3D%252Ffiles%252FPress%252FGeneral%252FInfographics%252FSD_EN_Cyber_Strategy.pd

Helmbrecht, U., Purser, S., & Ritter Klejn, M. (2012). Cyber Security: Future Challenges and Oportunities.*ENISA*.

Herzog, S. (2011).*R*evisiting the Estonian Cyber Attacks:Digital Threats and Multinational Responses.*Journal of Strategic Security 4, no. 2*.Retrieved from: https://scholarcommons.usf.edu/cgi/viewcontent.cgi?referer=https://www.google.gr/&httpsredir=1&article=1105&context=jss

Hogan Lovells. (2016). *Cyber security: A growing threat to the energy sector – An Australian perspective.*Retrieved from https://www.hoganlovells.com/en/knowledge/topic-centers/cybersecurity-solutions/~/media/c14b2cc829b04a6e841237f66882b2df.ashx

Hriciková, L., &Kaska, K. (2015).National Cyber Security Organisation: Slovakia.*NATO Cooperative Cyber Defence Centre of Excellence*. Retrieved from: https://ccdcoe.org/uploads/2018/10/CS_organisation_SLOVAKIA_042015.pdf

International Business Publications. (2013). EU Cyber Security Strategy and Programs Handbook, *Strategic Information and Regulations.Volume 1.*Washington DC: International Business Publications .

International Communications Union. (2018). *Global Cybersecurity Index.* Retrieved from https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Kosciuszko Institute. (2018, June).THE DIGITAL 3 SEAS INITIATIVE:A CALL FOR A CYBER UPGRADE OF REGIONAL COOPERATION.*THE KOSCIUSZKO INSTITUTE POLICY BRIEF.* Retrieved from: https://ik.org.pl/wp-content/uploads/white_paper_the_digital_3_seas_initiative-1.pdf

Limnell, J. (2018). Russian cyber activities in the EU from Hacks, leaks and disruptions Russian cyber strategies.*European Union Institute for Security Studies.* (p. 69) Retrieved from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Luiijf, E., Besseling, K., & de Graaf, P. (2013, January). Nineteen National Cyber Security Strategies.*INTERNATIONAL JOURNAL OF CRITICAL INFRASTRUCTURE PROTECTION.* Retrieved from: https://informationsecurity.report/Resources/Whitepapers/cf8d0895-e0c8-4256-8b12-bdd2eb0f9358_543545380cf2bf1f1f286509.pdf

Mackenzie, C. (2019, January 18). French defense chief touts offensive tack in new cyber strategy.*Fifth Domain.* Retrieved from: https://www.fifthdomain.com/global/europe/2019/01/18/french-defense-chief-touts-offensive-tack-in-new-cyber-strategy/

Ministry of DefenceEstonia .(2008). *Cyber Security Strategy.*

Ministry of Digital Affairs. (2017). *National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022.*Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/govermental-program-for-protection-of-cyberspace-for-the-years-2011-2016-2013

Ministry of Economic Affairs and Communication. (2014). *Cyber Security Strategy 2014-2017.*Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/strategies/cyber-security-strategy

NATO. (2018, February). *NATO – EU Relations.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_02/1802-factsheet-nato-eu-en.pdf

NATO.(2019, February).*NATO Cyber Defence.* Retrieved from https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf

NATO Cooperative Cyber Defence Centre of Excellence. (2017, September 18). *European Union Equipping Itself against Cyber Attacks with the Help of Cyber diplomacy Toolbox.* Retrieved from https://www.google.gr/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwiztIeL95_hAhVGLFAKHQOJB4wQFjAAegQIARAB&url=https%3A%2F%2Fccdcoe.org%2Feuropean-union-equipping-itself-against-cyber-attacks-help-cyber-diplomacy-toolbox.html&usg=AOvV

Pawlak, P., & Sheahan, C. (2014 , March). The EU and its (cyber) partnerships.*European Union Institute for Security Studies.*Retrieved from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief_9_Cyber_partners.pdf

Pernik, P. (2014 , September). Improving Cyber Security: NATO and the EU .*International Centre for Defence Studies*. Retrieved from: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

Pernik, P. (2018, October). Chapter 5 The early days of cyberattacks:the cases of Estonia, Georgia and Ukraine from Hacks, leaks and disruptions Russian cyber strategies.*European Union Institute for Security Studies*. Retrieved from: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf

Pernik, P., & Tuohy, E. (2013, August).Cyber Space in Estonia: Greater Security, Greater Challenges.*International Centre for Defence Studies*. Retrieved from: https://icds.ee/wp-content/uploads/2013/Piret%20Pernik%20-%20Cyber%20Space%20in%20Estonia.pdf

PESCO.(n.d). *CYBER THREATS AND INCIDENT RESPONSE INFORMATION SHARING PLATFORM.* Retrieved from https://pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/

Presidency of the Council of Ministers . (2013 , December). *National Strategic Framework for Cyberspace Security.* Retrieved from https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/italian-national-strategic-framework-for-cyberspace-security.pdf

Pupillo, L., Griffith, M., Blockmans, S., & Renda, A. (2018, November 26). *Strengthening the EU's Cyber Defence Capabilities.*Retrieved from https://ssrn.com/abstract=3300625

Renard , T. (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain.*European Politics and Society*. Retrieved from: http://www.egmontinstitute.be/content/uploads/2018/01/EPS-EU-cyber-partners_RENARD_AM.pdf?type=pdf

Ruus, K. (2008). Cyber War I: Estonia Attacked from Russia.*European Affairs: Volume number 9, Issue number 1-2.*

Saleem, M., & Hassan, J. (n.d)."Cyber warfare", the truth in a real case.*Information Security Course Linköping Universitetet*. Retrieved from: https://pdfs.semanticscholar.org/b0aa/b027865f06f359e23d70a6826042403bc5e9.pdf

Schallbruch, M., & Skierka, I. (2018, July 20). *Cybersecurity in Germany.* (p. 18) Springer .

Sliwinski, K. (2014). Moving beyond the European Union's weakness as a cyber-security agent.*Hong Kong Baptist University HKBU Institutional Repository*.Retrieved from: https://repository.hkbu.edu.hk/cgi/viewcontent.cgi?article=1007&context=gis_ja

van der Meer , S. (2017, June 20). EU Creates a Diplomatic Toolbox to Deter Cyberattacks.*Council on Foreign Relations.*Retrieved from: https://www.cfr.org/blog/eu-creates-diplomatic-toolbox-deter-cyberattacks