Ankara Avrupa Çalışmaları Dergisi Cilt:21, No:2 (Yıl: 2022), s. 467-495

THE DEVELOPMENT OF EU CYBERSECURITY POLICY: FROM A COORDINATING ACTOR TO A CYBER POWER?♦

Kadri Kaan RENDA*

Research Article

Abstract

The aim of the article is to elaborate on the institutional and normative evolution of the European Union (EU) cybersecurity policy. The article primarily argues that the EU's approach to cyberspace has recently focused on economic and security concerns. Secondly, the article contends that the actorness of the EU in the cyberspace has been evolved from a coordinating role to a more powerful one. The article is structured as follows: In the first part of the article, the literature on the EU's actorness in cyberspace is reviewed. In the second part, the institutional and normative development of EU cybersecurity policy is evaluated. Three strategy papers published by the European Commission in 2013, 2017, and 2020 are elaborated, respectively.

Keywords: *Cyber-power, Cybersecurity, Cyberspace, European Union, Digital Technologies.*

Avrupa Siber Güvenlik Politikasının Gelişimi: Eşgüdümcü Rol'den Siber Güce?

Öz

Makalenin amacı, Avrupa Birliği (AB) siber güvenlik politikasının kurumsal ve normatif evrimini derinlemesine incelemektir. Makale, AB'nin siber uzaya yaklaşımının ekonomik ve güvenlik ile ilgili kaygılara odaklandığını ileri sürmektedir. İkinci olarak, AB'nin siber uzaydaki aktörlüğünün eşgüdümcü bir

♦ An earlier version of this paper was presented at UACES 2021 Virtual Conference, 6-8 September 2021.

* Dr. Öğr. Üyesi, Hacettepe Üniversitesi / Uluslararası İlişkiler Bölümü, E-mail: kadri.renda@hacettepe.edu.tr, ORCID: 0000-0002-1170-4631.

Makalenin Gönderilme Tarihi: 29/04/2022 Kabul Edilme Tarihi: 26/12/2022

rolden siber güce doğru evrildiği makalede iddia edilmektedir. Makalenin içeriği şu şekildedir: İlk kısımda AB'nin siber uzaydaki aktörlüğü üzerine yapılmış olan araştırmalar üzerine bir değerlendirme yapılmaktadır. İkinci kısımda AB siber güvenlik politikasının kurumsal ve normatif gelişimi ele alınmaktadır. Makalenin geri kalanında Avrupa Komisyonu tarafından sırasıyla 2013, 2017 ve 2020'de yayımlanan üç siber güvenlik strateji belgesi ayrıntılı olarak incelenmektedir.

Anahtar Kelimeler: *Siber Güç, Siber Güvenlik, Siber Uzay, Avrupa Birliği, Dijital Teknolojiler.*

Introduction

In today's world, states have to address various threats posed by other states as well as non-state actors such as terrorist organisations, criminals, hackers and even social media trolls. Perpetrators are anonymous, sources and types of threats are ambiguous in a world where the speed, scale and intensity of such threats pertain to the scope, range and complexity of technological advancements. The more technologically advanced, connected and savvy our societies have become, the more they are open to cyber threats. Predicting when and how a cyber-attack would emerge and who would carry out it is a challenging task that necessitates full awareness of ordinary citizens, constant attention of responsible bodies and sustained efforts of public institutions to closely survey and verify potential risks and threats in the everyday lives of ordinary people. Given this fact, states or international organisations such as the European Union (EU) have been focusing on addressing such threats by building up their cyber capacities for becoming more aware of and resilient against them. While doing this, the EU particularly has engaged with the legal and moral aspects of cyberspace and cybersecurity. Cyberspace has become an important policy area for which the EU has to develop new regulations and standards. Any kind of activity in cyberspace whether it is benign or malign has an impact on the functioning of European economies and institutions. Not only do public institutions encounter cyberattacks but also private companies and ordinary citizens have to protect their day-to-day transactions and data against cyber criminals. Hence, the EU cybersecurity policy entails a multidimensional approach to providing cybersecurity for Europeans.

This article aims at delving into the development of EU cybersecurity policy. The establishment of new EU institutions and the emergence of European values and principles will be the primary focus of this article. The

main argument is that cyberspace as a new policy domain provides the EU with a unique opportunity to carve out a new role and enhance its influence concerning cybersecurity matters. The article is structured as follows: In the first part of the article, the literature on the EU's international actorness in general and particularly its actorness in cyberspace is reviewed. In the second part, the emergence and development of the EU cybersecurity policy is explored. This part, particularly, examines the EU's cybersecurity strategies of 2013, 2017, and 2020, respectively. Objectives, priorities and policy recommendations of three strategies are to be discussed in detail. A comparison of these policy papers also will help us to illustrate the rise of the EU's actorness in the field of cybersecurity. The article concludes with a discussion on different aspects of its actorness.

I. A Review of the Literature on the EU's Actorness in Cyberspace

With the commencement of the treaty of Lisbon in 2009, the EU's international actorness gained a legal basis and the treaty produced new institutional structures which would enable the EU to respond to the new crises of the 21st century. Cyber-attacks were seen as new threats to the security of the EU and its member states. Concerns about the single market and internal security shaped the EU's approach toward cybersecurity in the 1990s and early 2000s.[1] For instance, some recent research contends that the European Commission utilized a market-centred approach while addressing cyber-attacks in order not to be superseded by member states' security concerns.[2] The attention of the US and NATO to cyber threats and risks, particularly threats triggered by cyber-attacks conducted or ordered by rival great powers, namely Russia and China in the first decade of the 21st century forced the EU to alter its approach to cybersecurity. Hence, cyberspace has become a new domain of security where the EU has to protect itself and also act as a coordinating player among member states.

Even after the Treaty of Lisbon entered into force the EU did not have a comprehensive strategy that would provide it with strategic objectives in the field of security and defence. This gap was filled with the announcement of

---

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

2 Ana Paula Brandão, and Isabel Camisão, "Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy," *Journal of Common Market Studies*, 60 no 5 (2022), Accessed date: December 16, 2022, https://doi.org/10.1111/jcms.13158.

the EU Global Strategy (EUGS) in 2016.[3] The fragmented nature of the EU's international actorness is addressed by this new strategy paper. Despite the fact that the EU's first cybersecurity strategy was published in 2013, the EUGS elevated the status of cybersecurity by integrating it into the EU's grand strategy. The EUGS compiles different policies of the EU with regard to world trade, energy security, conflict management, migration, international terrorism, and cybersecurity. According to the strategy, the EU will advocate for an international order founded on rules, with multilateralism as its guiding principle. To address the underlying causes of violence and poverty, as well as to advance human rights, the EU assumes a global role and acts in line with the logic of principled pragmatism.[4] Not only does the strategy underline the importance of the EU's distinct yet coherent way of handling several issues and its coordinated response to crises, but also it aims at enhancing effectiveness in different domains of which cyberspace has given particular attention.

In line with the newly carved-up international role of the EU, the EUGS also pinpoints the importance of cybersecurity. Under the title of cybersecurity, the Strategy stresses that the EU would work in collaboration with member states in order to "maintain open, free and safe cyberspace."[5] Three objectives concerning the EU's actorness in cyberspace are prioritized by the strategy. These are: i) developing technological capabilities for the sake of technological independence and strategic autonomy, ii) maintaining the resilience of critical infrastructure, networks and services, and iii) addressing cybercrime by the legislative initiatives and institutions of the EU.[6] Furthermore, the EUGS also offers a comprehensive approach that referred to the combination of external and internal security policies of the EU.[7] The comprehensive approach highlights the coherent and effective application of EU policies in the field of (cyber) security.

The burgeoning literature on the EU's cybersecurity policies and actorness corresponds to the development of coherent policy, effective

---

[3] Council of the European Union, *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*', June, 2016. [hereinafter EUGS] Accessed date: April 25, 2022, http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

[4] *EUGS*, 8.

[5] *EUGS*, 21.

[6] *EUGS*, 21-22.

[7] *EUGS*, 9.

capabilities and coordinated institutions.[8] Sliwinski contends that the EU's actorness in the cyber domain was vague and not well-defined.[9] This vagueness limits the EU's competencies in cyberspace to defensive and civilian purposes. With the announcement of the EUGS, the debate on the development of EU cybersecurity policy has shifted from economic interests and criminal matters to strategic issues and normative concerns. The EU's approach toward cybersecurity initially rested on the purpose of detecting and addressing risks. Yet, this risk-based approach was replaced by a threat-based understanding of cybersecurity.[10] Given the comprehensive approach advocated by the EUGS, Helena Carrapico and André Barrinha indicate that the central concept around which the EU's cyber policies have been revolving is primarily coherence. According to the authors, coherence implies "institutional coordination and the existence (or not) of shared views on security, threats and potential responses."[11] They scrutinize the coherence among the EU's cybersecurity practices. Fulya Köksoy, in her article, explores the evolution of EU cybersecurity policy since the 1990s from a historical institutionalist perspective and she claimed that the EU could not pursue a coherent cybersecurity policy due to member states' unwillingness to delegate decision-making power to the EU even though the institutionalization of EU cybersecurity policy has been accelerated after the Lisbon treaty.[12]

As part of the discussion on coherence and effectiveness, some other scholars have tried to give answers to the questions of whether the EU has cyber-power, what kind of power the EU exerts in cyberspace, and to what

---

[8] Helena Carrapico and André Barrinha, "European Union cyber security as an emerging research and policy field", *European Politics and Society*, 19 no 3 (2018), Accessed date: December 16, 2022, doi:10.1080/23745118.2018.1430712.

[9] Krzysztof F. Sliwinski, "Moving beyond the European Union's Weakness as a Cyber-Security Agent," *Contemporary Security Policy*, 35 no 3 (2014): 468–486, Accessed date: December 16, 2022, doi: 10.1080/13523260.2014.959261.

[10] Sarah Backman,"Risk vs. threat-based cybersecurity: the case of the EU. European Security," *European Security*, Online first publication, Accessed date: December 16, 2022, doi: 10.1080/09662839.2022.2069464.

[11] Helena Carrapico and André Barrinha, "The EU as a Coherent (Cyber)Security Actor?" *Journal of Common Market Studies*, 55 no 6 (2017): 1257, Accessed date: December 16, 2022, doi: 10.1111/jcms.12575.

[12] Fulya Köksoy, "Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı?", *Güvenlik Stratejileri Dergisi*, 16 (2020), Accessed date: December 16, 2022, doi: 10.17752/guvenlikstrtj.807014.

extent the EU acts as an influential actor in cyberspace.[13] By drawing on these studies one can conclude that the EU has positioned itself as a new player which not only complements existing cybersecurity policies of member states and coordinates their practices but also it has been enhancing its capabilities in order to secure a prominent role in the field of cyberspace. Ultimately, the EU may supplant member states in the near future.

Alongside debates on the coherence and effectiveness of the EU, the literature on the EU's cybersecurity policy can be grouped into three strands. The first group of studies has been addressing the legal and institutional development of EU response to cybercrimes in the form of identity theft, fraud and other illegal activities over the Internet since the 1990s. In the 1990s, the EU was aware of economic problems caused by the misuse of the Internet. Information security was at the centre of the EU's policies vis-à-vis cybercrime.[14] For the last two decades, the EU has been building up its institutional capacity through the adaption of new rules and the establishment of new institutions such as the European Cybercrime Centre. As a result, the internal and external dimensions of cybersecurity have been intertwined while making new rules related to cybercrime.[15]

Cyberterrorism and cyber-attacks on critical infrastructures are the central concepts of the second strand as they pay attention to the protection of society and the economy and the maintenance of public services and public order.[16] Protecting critical infrastructures against cyber-sabotage and

---

[13] Myriam Dunn Cavelty, "Europe's cyber-power," *European Politics and Society*, 19 no 3 (2018), Accessed date: December 16, 2022, doi: 10.1080/23745118.2018.1430718; Constant Pâris, *Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace*, EU Diplomacy Articles, College of Europe, 2021, Accessed date: December 16, 2022, https://www.coleurope.eu/sites/default/files/research-paper/edp_1_2021_paris_0.pdf

[14] George Christou, "The challenges of cybercrime governance in the European Union," *European Politics and Society*, 19 no 3 (2018): 360–361, Accessed date: December 16, 2022, doi: 10.1080/23745118.2018.1430722.

[15] Elaine Fahey, "EU's Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security,' *European Journal of Risk Regulation*, 5 no 1 (2014), Accessed date: December 16, 2022, http://www.jstor.org/stable/24323486; Laviero Buono, "Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (Ec3)," *New Journal of European Criminal Law*, 3 no 3-4 (2012), Accessed date: December 16, 2022, https://doi.org/10.1177/203228441200300307

[16] Christer Pursiainen, "The Challenges for European Critical Infrastructure Protection", *European Integration*, 31 no 6 (2009), Accessed date: December 16, 2022, doi:

cyber-espionage is of great importance for Europe in order to preserve public order and maintain public services. Resisting and deterring cyber-attacks are associated with societal and state-level readiness and preparedness to return to a normal state after a serious cyber-attack. Hence, the idea of resilience has become more relevant within the EU's security policy due to hybrid threats and cyber-attacks.[17] The concept of resilience has been widely used by scholars and practitioners alike. The concept not only entails the idea of being prepared and ready to defend Europe against cyber-attacks but also suggests having abilities at the levels of society and state to recover quickly in the case of a cyber-attack.[18] Quick recovery renders any kind of attack a futile attempt to inflict damage upon the target.

The last group of studies has cast some light on the development of technological capabilities. Since cyberspace is highly related to the development of information and communication technologies, more attention has been paid to research and development projects and public-private partnerships supported by the EU in order not to lag behind the rest of the world in acquiring new technologies. Since the EUGS underlined that the EU should have strategic autonomy, technological independence/sovereignty has become the key to comprehending the EU's approach toward acquiring defensive technologies in the domain of cyberspace.[19] André Barrinha and George Christou elaborate on the concept of technological sovereignty by unravelling "the EU's discursive understandings of technological sovereignty".[20] They conclude that the EU is establishing its technical sovereignty in connection to its internal

10.1080/07036330903199846; Raphael Bossong, "The European Programme for the protection of critical infrastructures – meta-governing a new security problem?", *European Security*, 23 no 2 (2014), Accessed date: December 16, 2022, doi: 10.1080/09662839.2013.856307.

[17] Wolfgang Wagner and Rosanne Anholt, "Resilience as the EU Global Strategy's new leitmotif: pragmatic, problematic or promising?", *Contemporary Security Policy*, 37 no 3 (2016), Accessed date: December 16, 2022, doi: 10.1080/13523260.2016.1228034.

[18] Nathalie Tocci, "Resilience and the role of the European Union in the world," *Contemporary Security Policy*, 41 no 2 (2020): 178, Accessed date: December 16, 2022, doi: 10.1080/13523260.2019.1640342.

[19] Raluca Csernatoni, *The EU's rise as a defense technological power: from strategic autonomy to technological sovereignty*, Carnegie Europe, 2021. Accessed date: December 16, 2022, https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty/$

[20] André Barrinha and George Christou, "Speaking sovereignty: the EU in the cyber domain," *European Security*, 31 no 3 (2022): 357, Accessed date: December 16, 2022, doi:10.1080/09662839.2022.2102895.

competencies and laws as well as its external relations with those it constructs as the others who oppose its standards, interests, and values.[21] Richard Youngs, from a different point of view, criticizes the EU's discourse on technological sovereignty since it rests on the assumption that the EU is either sovereign or not, yet for Youngs, mutual interdependence shapes the advancement in information and communication technologies.[22]

The next section will delve into the historical evolution of EU Cybersecurity policy. Beginning with early initiatives, the next section will provide a comparative analysis of three cybersecurity policy papers of the EU. The analysis will demonstrate the changing nature of the EU's actorness in the domain of cybersecurity.

II. The Development of EU Cybersecurity Policy

Digitalisation and interconnectedness have created a new world. This new world has brought opportunities as well as threats. The threat landscape has evolved and thus, hybrid and cyber threats have forced the EU and its members to develop new policies and institutions that address new threats. Cyber-attacks not only threaten economies, critical infrastructures or public order but also may cause damage to the European way of life, European values, and the functioning of European institutions. These new circumstances compelled the EU to produce policies that would address cyber threats.

A. Early Initiatives

Cyberspace cannot be restricted to national borders. Even though cyberspace depends on the physical presence of computer hardware and energy supplies, cyberspace is a new domain where defence against cyber threats necessitates collaborative action. In 1998 the European Commission produced a paper on globalisation and the information society. The paper highlighted the growing importance of telecommunication and digital technologies. Particularly, the European Commission paid attention to the soaring electronic commerce. The paper stressed that new rules were

[21] Barrinha and Christou, "Speaking sovereignty," 37.

[22] Richard Youngs, *The EU's strategic autonomy trap*, Carnegie Europe, 2021. Accessed date: December 16, 2022, https://carnegieeurope.eu/publications/83955.

necessary to regulate the Internet as an electronic marketplace and it also recommended an international charter which would further coordination among different stakeholders.[23] Notably, there was no mention of cyberspace or cybersecurity in the paper. In the same year, Ulrich Sieber wrote a report on the legal aspects of computer-related criminal activities for the European Commission.[24] Sieber provided a comprehensive legal framework for addressing new crimes generated by cyber activities. The European Commission published another communication titled "Network and Information Security", which specified that a network and information system must be able "to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems."[25] The paper also gave a list of threats to information systems. Malicious interception of the internet and communication, unauthorized access to computers and computer networks, network disruption, malicious modification of data or computer networks, and misrepresentation of the trusted institution were listed as threats to information systems.[26]

At the institutional level, the European Network and Information Security Agency (ENISA) was founded in 2004. It was tasked to develop a culture of network and information security and foster coordination among member states. In its 2006 strategy for the maintenance of a secure information society, the Commission proposed three measures to protect information systems, namely dialogue, partnership, and empowerment.[27]

---

[23] Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Globalisation and the Information Society: The Need for Strengthened Coordination*, COM(1998) 50 final, (Brussels, February 04, 1998), 12, Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51998DC0050&from=EN.

[24] Ulrich Sieber, *Legal Aspects of Computer-related Crime in the Information Society (COMCRIME Study) prepared for the European Commission* (Würzburg, January 1, 1998).

[25] Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach*, COM(2001) 298 final, (Brussels, June 6, 2001), 9, Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF.

[26] COM(2001) 298, 10–15.

[27] Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the*

According to the strategy, dialogue among multi-stakeholders which consisted of public authorities and private companies might facilitate better implementation of network and information security. In addition to dialogue, partnerships between member states and other stakeholders, and partnerships between the research community and private entities would contribute to tackling computer-related crimes. Lastly, raising awareness through training, exercises and educational activities was regarded as an instrument to develop a security culture.[28]

Bearing in mind the changing threat environment and increasing incidents of cyber-attacks such as the 2007 cyber-attack to Estonia, the European Commission urged member states to come up with an action plan to mitigate risks that would cause a failure in the functioning of critical infrastructures such as information communication technologies.[29] In this new security environment, "A Digital Agenda for Europe" published in May 2010 raised issues regarding trust and security in cyberspace.[30] The Agenda provided a blueprint for an EU strategy in the digital age. The strategy underlined that the development of the digital single market and the prosperity of European economies depended on gaining users' confidence and trust in cyberspace and digital services.[31] The Agenda recommended the establishment of the European Cybercrime Centre and Cybercrime platform as well as Computer Emergency Response Teams (CERTs) for the EU and member states as part of the EU's strategy for preventing cybercrime.[32] A permanent Computer Emergency Response Team (CERT-EU) for the EU institutions, agencies and bodies was set up on 11 September 2012. The team

Committee of the Regions A strategy for a Secure Information Society – "Dialogue, partnership and empowerment", COM(2006) 251 final, (Brussels, May 31, 2006), Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF.

28 COM(2006) 251, 8–9.

29 Commission of the European Communities, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection,* COM(2009) 149 final, (Brussels, March 30, 2009), Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF.

30 European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe,* COM(2010) 245 final, (Brussels, May 19, 2010), Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

31 COM(2010) 245, 16.

32 COM(2010) 245, 17.

consists of IT security experts and aims at enhancing cooperation with other CERTs at the national level and with specialized IT security companies.

Cybercrime was described as an internal threat against which the EU had to establish an institution to police cyberspace in the Internal Security Strategy published in 2010. The Strategy listed cybercrime as a growing threat to the internet-mediated economies of EU member states.[33] Since the main objective of the EU was defined as promoting and protecting the market economy, criminal activities at the cyber level have been considered as threats to the EU and its member states.[34] The strategy paper recommended that a new cybercrime centre should be established by 2013.[35] The European Cybercrime Centre (EC3) opened on 11 January 2013. It is established at the European Police Office, Europol at The Hague. The EC3 monitors illegal online activities such as attacks targeting e-banking and other online financial activities, online child sexual exploitation and attacks on the critical infrastructure and information systems in the EU.[36] The objectives of the EC3 demonstrate that the institutionalisation of EU cyber policy had begun owing to an internal security concern emanating from criminal activities.

B. The 2013 Cybersecurity Strategy of the EU

The European Commission prepared a comprehensive cybersecurity strategy in 2013. Due to the increasing digitalisation and automation in some sectors such as transport, finance, energy, and even health and education, the economies of EU member states have become more dependent on information technologies. As digitalisation in several sectors and the number of connection points to the internet increase, cyber threats have varied, too. This point was highlighted in the introductory part of the 2013 Cybersecurity Strategy of the EU.[37] The strategy underlined that cybersecurity and cyber

---

[33] European Commission, *Communication from the Commission to the European Parliament, the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, COM(2010) 673 final, (Brussels, November 22, 2010), 4, Accessed date: April 25, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673& from=EN.

[34] COM(2010) 673, 2.

[35] COM(2010) 673, 9.

[36] "Key Objectives," The European Cybercrime Centre, March 01, 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

[37] European Commission and High Representative, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the*

defence were inextricably intertwined. The EU Cybersecurity Strategy pinpointed the intentional and unintentional/accidental characteristics of cyber threats.[38] Therefore, reinforcing cybersecurity measures through the diversification of detection and protection capabilities, formation of new EU institutions on cybersecurity, and provision of education to European firms and citizens were listed as priorities. The strategy did not provide an official definition of cybersecurity, yet in a footnote, it was noted that "cybersecurity commonly refers to the safeguards and actions that can be used to protect the cyber domain, both in the civilian and military fields."[39] In a similar vein, instead of providing a new definition of cybersecurity, an article published by the European Network and Information Security Agency distinguishes five domains of cybersecurity, namely communications security, information security, operations security, physical security, and public/military security.[40] While cybercrimes were considered as threats to the internet-based economies of member states and the functioning of EU institutions,[41] the cyber defence was mentioned as part of capability development for Common Security and Defence Policy (CSDP) operations.[42] The Cybersecurity Strategy of 2013 emphasized that not only maintaining "the reliability and interoperability of the Internet" but also protecting "fundamental rights, democracy and the rule of law" in cyberspace is of great importance for the freedom and prosperity of Europeans.[43] It was also noted that the EU would strive to protect and promote freedom and fundamental rights online even in third countries where authoritarian regimes exploit cyberspace in order to keep a close watch on the activities of their citizens.[44]

Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace, JOIN(2013) 1 final, (Brussels, December 7, 2013), Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

38 JOIN(2013) 1, 3.

39 JOIN(2013) 1, 3, fn.4.

40 European Union Agency for Network and Information Security, *Definitions of Cybersecurity: Gaps and Overlaps in Standardisation*, v1.0, (Brussels, 2015), 11–12, Accessed date: April 25, 2022, https://www.enisa.europa.eu/publications/definition-of-cybersecurity/view/++widget++form.widgets.fullReport/@@download/Cybersecurity_Definition_Gaps_v1_0.pdf.

41 JOIN(2013) 1, 3.

42 JOIN(2013) 1, 11.

43 JOIN(2013) 1, 2.

44 JOIN(2013) 1, 3.

The strategy paper prioritized four fundamental principles of cybersecurity, namely protecting human rights, freedom of expression, personal data and privacy; safe access for all; democratic and efficient multi-stakeholder governance; shared responsibility among public authorities, the private sector and individual citizens to ensure cybersecurity.[45] The EU would champion these fundamental principles at the international level.[46] Building upon these principles, the strategy is concerned with five strategic issues. First, the EU and its member states would be cyber-resilient. Cyber resilience would be achieved in two ways. Initially, the strategy recommended that new legislation on cyberspace, namely Network and Information Security Directive (NIS) should be adopted. Such a directive would give more responsibilities and authority to the European Network and Information Security Agency (ENISA) to coordinate national authorities and enhance collaboration among several other regulatory bodies.[47] The strategy also suggested that for a resilient Europe cybersecurity awareness should be raised through "publishing reports, organising expert workshops and developing public-private partnerships."[48]

The second strategic priority is fighting cybercrime through "strong and effective legislation", "enhanced operational capability" at the national level, and "improved coordination at the EU level". The stance of the EU for tackling cybercrime originated from the Budapest Convention. Alongside its emphasis on the Convention, the strategy underscored the importance of two EU directives; one directive on combating the sexual exploitation of children online and child pornography, and the other one on attacks against information systems.[49]

The third strategic priority listed in the strategy is concerned with the development of a cyber defence framework and capabilities. According to the strategy, detecting cyber threats, responding to them effectively and speed recovery after a cyberattack are the main goals of EU cyber defence. The strategy underlined the importance of synergies between civilian and military authorities as well as cooperation and coordination with NATO while enhancing cyber defence capabilities.[50]

---

45 JOIN(2013) 1, 4.
46 JOIN(2013) 1, 3.
47 JOIN(2013) 1, 6.
48 JOIN(2013) 1, 8.
49 JOIN(2013) 1, 9.
50 JOIN(2013) 1, 11.

The fourth strategic priority is related to research and development investments in cybersecurity and technological innovation, especially in the information and communication sectors. The strategy urged public and private authorities to pay more attention to "transparency about security in ICT products", to the adoption of "EU-wide voluntary certification schemes" for ICT products, and to the security of the supply chain in critical economic sectors.[51]

The last priority is about international cooperation. The strategy stressed that "open, free and secure cyberspace" could not be maintained without the help of international partners.[52] The strategy openly stated that the EU would "promote openness and freedom of the Internet, encourage efforts to develop norms of behaviour and apply existing international law in cyberspace."[53] These norms about cyberspace would be respected by not only individuals and private corporations but also by states. However, on the same page, it was also underlined that the EU would not champion a new international legal instrument for cyber issues. The EU would continue to abide by existing conventions and charters concerning cybercrime, cyber defence and human rights[54] For the EU, dialogue, coordination and cooperation with "like-minded" third countries is the major element of fighting cybercrime and maintaining cybersecurity. Such international cooperation was deemed to generate trust, transparency, and a sense of responsibility.[55]

In line with the priorities of the Cybersecurity Strategy of 2013, a plan for developing cyber defence capabilities was published in 2014. The Cyber Defence Policy Framework (CDPF) described cyberspace as a new military domain alongside land, sea, air and space on which the success of military and civilian operations/missions is increasingly dependent.[56] In the framework, the Council of the European Union set five priorities concerning the development of cyber defence capabilities. These five priorities are supporting member states to develop their cyber defence capabilities,

---

51 JOIN(2013) 1, 12–13.
52 JOIN(2013) 1, 14.
53 JOIN(2013) 1, 15.
54 JOIN(2013) 1, 15.
55 JOIN(2013) 1, 15.
56 Council of the EU, *EU Cyber Defence Policy Framework*, 15585/14, (Brussels, November 18, 2014), 2, Accessed: April 25, 2022, https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf.

enhancing the defence of networks used by EU institutions, promoting civil-military and private-public partnerships, providing training and education opportunities to national experts, and fostering cooperation with international partners. The CDPF of 2014 paved the way for the development of capabilities, provision of training, education and cyber exercise facilities, and cultivation of a cyber defence culture. As part of the capability development plan, the Cyber Ranges Federation Project – the first cyber defence project of the European Defence Agency (EDA) – was launched in 2017.[57] Austria, Belgium, Estonia, Finland, Germany, Greece, Ireland, Latvia, the Netherlands, Portugal and Sweden participated in the project. The aims of the project include: "increasing the availability of existing and emerging cyber range facilities; increasing the occupation rate and efficiency of cyber ranges and platforms; mainstream and improve cyber defence training, exercises and testing at European level."[58]

After the launch of Permanent Structured Cooperation (PESCO) in 2017, two projects on cyber defence were initiated. These are "Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity" and "Cyber Threats and Incident Response Information Sharing Platform." Whereas Lithuania, Romania, Croatia, Poland, the Netherlands, and Estonia are the participating members of the first project[59], the second project is an initiative of Greece, Spain, Italy, Cyprus, Hungary, Austria, and Portugal.[60] In addition, "EU Cyber Academia and Innovation Hub (EU CAIH)" led by Portugal and "Cyber and Information Domain Coordination Center (CIDCC)" led by Germany are launched. CIDCC is described as a "standing multinational military element". Participating member states (Germany, France, Hungary, and the Netherlands) have the sole authority to decide case-by-case on the matter of how they will contribute to the operations of

[57] "Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States," European Defence Agency, May 12, 2017, Accessed date: April 25, 2022, https://eda.europa.eu/news-and-events/news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states

[58] "Cyber Ranges," para. 1.

[59] "PESCO Projects: Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity (CRRT)," Permanent Structured Cooperation, Accessed date: April 25, 2022, https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

[60] "PESCO Projects: Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)," Permanent Structured Cooperation, Accessed date: April 25, 2022, https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/

the Centre.[61] These PESCO projects notwithstanding, an EU Cyber Command has not been formed, yet.[62] Despite the EU's prioritization of cyber defence, the EU lacking a centralized cyber command undermines its cyber defence capabilities and curtails its ambitions to become more influential in this new policy field.

Published in June 2016, A Global Strategy for the European Union's Foreign and Security Policy counted cybersecurity as a priority of the EU's external action.[63] In September 2017, in his speech on the state of the union, former president of the Commission Jean-Claude Juncker drew attention to cybersecurity by stressing that "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."[64] Against this backdrop and with the rising awareness of cybersecurity issues, the Juncker Commission proposed establishing the European Cybersecurity Agency (formerly ENISA), and the European Cybersecurity Research and Competence Centre. The Commission also proposed the establishment of an EU-wide cybersecurity certification scheme, a framework for a Joint EU Diplomatic Response to Malicious Cyber Activities and last but not least a cyber defence training and education platform.

C. The 2017 Cybersecurity Strategy of the EU

The joint communication of the European Commission and High Representative to the European Parliament and the Council titled "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU" pinpointed the seriousness and urgency of developing a secure cyberspace for Europe that has been in a rapid digital transformation.[65]

---

61 "PESCO Projects: Cyber and Information Domain Coordination Center (CIDCC)," Permanent Structured Cooperation, Accessed date: April 25, 2022, https://www.pesco.europa.eu/project/cyber-and-information-domain-coordination-center-cidcc/

62 In contrast, the US Cyber Command was formed in 2010.

63 *EUGS*, 22–23.

64 Jean Claude Juncker, *State of the Union Address 2017*, Transcript of Speech delivered at the European Parliament, Brussels, September 13, 2017, Accessed date: April 25, 2022, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

65 European Commission and High Representative, *Joint Communication to the European Parliament, the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU,* JOIN (2017) 450 final, (Brussels, September 13, 2017), 2,

Secure cyberspace was deemed to be indispensable for European economies, democracies and values.[66] The strategy accentuated the shift from an interconnected world to a hyper-connected world with the introduction of the Internet of Things (IoT) devices.[67] The strategy also warned of serious damage caused by the widespread use of IoT devices without a built-in cybersecurity design on economies and societies across Europe. Similar to the 2013 Strategy, the 2017 strategy put emphasis on resilience, deterrence and international cooperation. According to the strategy, the EU could provide economic incentives and support for member states, and could facilitate coordination among them while developing its own cybersecurity capacity.[68] Similar to the Cybersecurity Strategy of 2013, this strategy also rested on a multifaceted and comprehensive approach toward cybersecurity, which entailed coordinated actions of several public authorities and private corporations. Such a comprehensive strategy was complemented by a proactive approach in the new strategy. For instance, the strategy welcomed the screening of foreign direct investment in the cybersecurity sector across Europe as acquiring and maintaining strategic autonomy for the EU was considered vital for cyber deterrence.[69] The strategy took geopolitical shifts in international politics into consideration and acknowledged that geopolitical rivalry continues in cyberspace, too. The influence of the Global Strategy for the EU's Foreign and Security Policy on the EU cybersecurity strategy of 2017 is obvious. Alongside raising awareness, enhancing resilience and building trust, the EU would strive for strategic autonomy and technological leadership both of which contribute to the EU's power in cyberspace.

As part of efforts to enhance resilience, the strategy suggested strengthening the ENISA, setting up an EU cybersecurity certification framework, adopting a "security by design" approach for not only digital devices used in critical sectors such as health, transportation, and energy, but also for mass consumer digital devices and services.[70] Furthermore, the strategy underlined the importance of implementing the Directive on

Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en.

66 JOIN (2017) 450, 2.

67 JOIN (2017) 450, 2.

68 JOIN (2017) 450, 3.

69 JOIN(2017) 450, 6.

70 JOIN(2017) 450, 5.

Network and Information Systems for better coordination and information sharing. Sharing information between the private and public sectors would restore consumer trust in digital services.[71] It is noteworthy that in the event of large-scale cybersecurity incidents a member state could request the initiation of the solidarity clause.[72] By invoking the solidarity clause, a Union-level response would be requested by a member state.

In the next subsection of the strategy paper, research and development in critical digital technologies such as artificial intelligence, quantum computing, and encryption were noted as one of the EU's strategic interests.[73] Investing in new digital technologies, generating a cyber workforce trained with much-needed cybersecurity skills, and spreading cyber hygiene and awareness in public and private sectors in order to reduce cyber incidents caused by human mistakes were given particular attention as part of the EU's proactive approach in building a resilient Europe against cyber-attacks.[74] For the strategy, cybersecurity is a mixture of security-by-design and security-by-user. This is why spreading cyber hygiene and awareness is necessary for cyber resilience.

Under the title "Creating Effective EU Cyber deterrence", the strategy focused on developing more effective law enforcement, a more prompt investigation, better identification of perpetrators via cross-border electronic evidence sharing, and adoption of common standards for cyber forensics.[75] It is noted that one of the goals of the EU's strategy is to promote online accountability as a general principle to deter cybercrime.[76] The strategy furthermore stressed the importance of enhanced public-private cooperation against cybercrime and forming a political response (e.g. sanctions on individuals and corporations) to malicious cyber activities via the utilization of the cyber diplomacy toolbox. Last but not least, enhanced cooperation among member states for the development of cyber defence capabilities is of great importance for the EU's cyber deterrence.[77]

[71] JOIN (2017) 450, 7.
[72] JOIN (2017) 450, 8.
[73] JOIN (2017) 450, 8–9.
[74] JOIN (2017) 450, 10–12.
[75] JOIN (2017) 450, 13–14.
[76] JOIN (2017) 450, 15.
[77] JOIN (2017) 450, 17.

The fourth section is devoted to the EU's international actorness in maintaining and promoting "global cyber stability."[78] The EU's global cybersecurity policy had two objectives. First, the EU would promote global cyber stability. Second, the EU would cooperate with third countries in the area of cybersecurity if such cooperation contributed to Europe's strategic autonomy. In order to achieve these objectives, the EU would continue to support the development of international practices and laws related to cybersecurity, would benefit from cyber dialogue with other countries, give assistance to third countries to enhance their national capabilities against cyberattacks and deepen cooperation with NATO.[79] The strategy concluded with an emphasis that the EU's cybersecurity policy would be an integral part of the Digital Single Market and Security and Defence Union.

D. The 2020 Cybersecurity Strategy of the EU

Prior to the 2020 strategy, the Cybersecurity Act was accepted by the European Parliament and the Council. The Act is a new regulation which lays down new rules concerning the cybersecurity of digital products and assigns new duties to the ENISA.[80] The Act acknowledges the significance of digital technologies for the economic growth of Europe. The Act defines cybersecurity as "activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats."[81] The Cybersecurity Act is a binding document for all member states and therefore, it is a manifestation of the growing EU role in the civilian aspect of cybersecurity.

The Commission in December 2020 issued the latest cybersecurity strategy. The strategy first describes the threat landscape. The 2020 strategy draws attention to geopolitical tensions. Geopolitical tensions are believed to be reflected in cyberspace.[82] According to the strategy, geopolitical tensions

---

78 JOIN(2017) 450, 18.

79 JOIN (2017) 450, 18–19.

80 Official Journal of the European Union, *Regulatıon (EU) 2019/881 of The European Parliament And of The Council on ENISA (the European Union Agency for Cybersecurity) of 17 April 2019 and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, (Brussels, June 7, 2019), Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

81 Regulation (EU) 2019/881, 18.

82 European Commission and High Representative, *Joint Communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade*,

and increased polarisation at the international level not only threaten the openness and safety of the Internet but also continuously undermine European values such as the rule of law, fundamental rights, freedom and democracy.[83] As European economies and societies have become ever more interconnected and digitalized, cyber threats raise serious concerns about the security of critical infrastructures, critical public services, and individual privacy. In the words of the strategy, "Improving cybersecurity is therefore essential for people to trust, use, and benefit from innovation, connectivity and automation, and for safeguarding fundamental rights and freedoms, including the rights to privacy and to the protection of personal data, and the freedom of expression and information."[84] As this quote illustrates, not only have individuals and private businesses adopted "a responsible and security-conscious" approach but also governments have to do the same.[85]

According to the strategy, one of the obstacles in front of addressing cyber threats is the lack of coordination and information sharing among member states.[86] The lack of "limited mutual operational assistance between Member States" and "no operational mechanism between Member States and EU institutions" are compounded by the lack of "collective situational awareness."[87] Forming operational mechanisms and responding collectively during a crisis were highlighted as missing elements of EU strategy.

After describing the threat environment and highlighting the main shortcomings of EU cybersecurity policy, the strategy delineates the principle instruments and policy areas. Regulatory, investment and policy instruments are to be utilized in order for the EU to achieve its objectives. The strategy prioritizes three areas for the EU to act in order to ensure a global and open Internet. The first area consists of measures taken by the EU. These measures aim at enhancing resilience and maintaining technological sovereignty and leadership by increasing investments in technologies such as Artificial Intelligence, encryption and quantum computing. The second area focuses on the development of the EU's

JOIN(2020) 18 final, (Brussels, December 16, 2020), 1, Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

83 JOIN (2020) 18, 2.

84 JOIN (2020) 18, 4.

85 JOIN(2020) 18, 4.

86 JOIN(2020) 18, 3.

87 JOIN(2020) 18, 3–4.

operational capacity in addressing cyber threats. The last area of action covered international cooperation for advancing a global and open cyberspace.[88]

With regards to enhancing resilience across Europe, the strategy initially supports the Commission's proposal for a revised NIS directive which would extend rules to the public sector.[89] It proposes measures to protect critical energy infrastructure, transportation sectors (especially aviation), democratic processes and institutions and lastly, services under the Space programme.[90] Earlier strategies of the EU mentioned the protection of critical infrastructures and the prevention of disruption of digital services used in energy, transportation, and health sectors. The latest strategy pinpoints electricity networks, aviation systems and space programmes. For instance, the strategy stresses the importance of adopting a "network code" for protecting cross-border electricity flows from cyber threats. In addition, democratic resilience is foregrounded in the latest strategy compared to previous strategies. Particularly, the strategy stresses the significance of preventing foreign manipulation of elections and protecting press freedom. As part of enhancing resilience, the strategy proposes that a network of Security Operations Centres (SOCs) across the EU should be established to provide a "cyber shield" for the EU.[91] The cyber shield for the EU consists of SOCs and the Joint Cyber Unit in addition to other EU institutions. While SOCs are tasked with monitoring communication networks and analysing activities in cyberspace, the Joint Cyber Unit functions as part of the European cybersecurity crisis management.[92]

In addition to new institutions, the strategy suggests developing new technologies such as quantum communication infrastructure, encryption, 5G and future generations of mobile networks, and artificial intelligence. For instance, the EU 5G toolbox has been established in order to identify policies and measures to be applied by member states during their transition to future mobile networks.[93] All these technologies must be developed and produced as designed and made in Europe technologies by European companies that are not dependent on high-risk suppliers. The underlying principle is that

88 JOIN(2020) 18, 4.
89 JOIN(2020) 18, 5.
90 JOIN(2020) 18, 6.
91 JOIN(2020) 18, 6–7.
92 JOIN(2020) 18, 7, 11.
93 JOIN(2020) 18, 8.

Europe should minimize its technological dependency on non-EU states and should acquire leadership in the production and use of strategically important technologies.[94] It is believed that maintaining strategic autonomy and technological leadership would ensure the EU's technological independency in the coming age of artificial intelligence and automated systems. Whereas the principle of strategic autonomy already was embedded in the EU's 2017 strategy, in the 2020 strategy technological leadership and sovereignty have been prioritized, too.

In line with its objective of maintaining an open, safe, trusted, global Internet, the strategy underscores the "integrity and availability of the global DNS root system", a strategy for DNS diversification, the development of a "European DNS resolver service", and wide-spread use of key internet standards such as IPv6.[95] These technical standards will make the EU less vulnerable in the incident of a large-scale cyber-attack. Furthermore, it is stated that such key protocols and standards will help the EU to "counteract closed and control-based models of the Internet."[96]

In the area of international security, the strategy puts emphasis on the importance of collective diplomatic response in the event of a cyber-attack. Restrictive measures against malicious activities of third-country organisations and citizens have been used recently by the EU.[97] In addition to sanctions, cyber deterrence can be achieved by establishing EU cyber intelligence working groups and enhancing cyber defence capabilities. The strategy proclaims that the EU Military Committee should declare a "Military Vision and Strategy on Cyberspace as a Domain of Operations.[98]" Such a document will be the first-ever military doctrine of the EU on cyber defence. Despite this new military vision and strategy on cyberspace, there is no mention of a European Cyber Command. Lastly, the strategy notes that the EU should continue its efforts to safeguard and "promote a global, open, stable and secure cyberspace."[99] While striving for this objective the EU not only upholds existing "non-binding international norms, rules and principles of responsible state behaviour", but also facilitates international cooperation

94 JOIN(2020) 18, 7–8.
95 JOIN(2020) 18, 10–11.
96 JOIN(2020) 18, 11.
97 JOIN(2020) 18, 16.
98 JOIN(2020) 18, 18.
99 JOIN(2020) 18, 20.

in order to strengthen the cybersecurity capacity of third countries.[100] The strategy urges the EU to "step up its engagement in, and leadership on international standardisation processes" concerning the use of emerging technologies such as artificial intelligence, and quantum computing.[101] This is depicted not only as an urgent need for the EU but also as a strategic interest of the EU since third countries have taken the lead in forming international standards which may contradict European values and policies.[102]

Conclusion

Attacks on hardware as well as software are the new realities of today's security environment. Ransomware, digital theft and fraud on the Internet, leaks of sensitive information, illegal access to and improper usage of personal and private data, disinformation campaigns via social media, and paralysing the functioning of critical infrastructures by damaging computer systems and databases are typical examples of cyber threats. Given the pervasive nature of digital technologies in today's world, the EU has to develop its own policies concerning the new realm of cyberspace. The origins of EU cybersecurity policy can be found in the 1990s. Due to the growing importance of networks and the rapid increase in the usage of the Internet, the EU, was initially, concerned with the smooth adoption of electronic commerce to the Single Market. Later, the EU paid more attention to cyberterrorism, cyber deterrence and cyber defence. This new attention of the EU produced three cybersecurity strategies. The article has delved into the cybersecurity policy of the EU by giving details of three cybersecurity strategies of the EU issues in 2013, 2017, and 2020, respectively.

All three cybersecurity strategies of the EU recommend that the EU should coordinate initiatives and projects, train and educate the personnel of the EU and member states, conduct exercises, regulate markets and ICT and cybersecurity sectors, foster the development of law enforcement capabilities for fighting cybercrime, develop its own cybersecurity teams against cyber-attacks to EU institutions. In the event of a large-scale cyber-attack, EU institutions must be ready to detect and respond to cyber threats. Recently,

[100] JOIN(2020) 18, 20.
[101] JOIN(2020) 18, 20.
[102] JOIN(2020) 18, 20.

the EU has directed its efforts to promote non-binding rules and norms of cybersecurity in third countries. Particularly, the latest strategy stresses the importance of increased global resilience for the maintenance of Europe-wide resilience. Lastly, the EU has also included cyber defence as part of its cybersecurity policy. However, as the EU's cybersecurity strategy demonstrates the EU does not have a military doctrine and a military cyber command when it comes to cyber-warfare since its main concern is law enforcement, crisis management and international cooperation rather than power projection in cyberspace. In conclusion, this article has demonstrated that the EU's actorness concerning cybersecurity has evolved from mere economic and technical concerns to cybercrimes, technological leadership, strategic autonomy and international influence on third countries while the military dimension of EU cybersecurity policy has been lagging far behind its civilian and economic dimensions.

References

Backman, Sarah. "Risk vs. threat-based cybersecurity: the case of the EU." *European Security*, Online first publication. Accessed date: December 16, 2022, doi: 10.1080/09662839.2022.2069464.

Barrinha, André and George Christou. "Speaking sovereignty: the EU in the cyber domain." *European Security*, 31 no 3 (2022): 356-376. Accessed date: December 16, 2022, doi:10.1080/09662839.2022.2102895.

Bossong, Raphael. "The European Programme for the protection of critical infrastructures – meta-governing a new security problem?". *European Security*, 23 no 2 (2014):210–226. Accessed date: December 16, 2022, doi: 10.1080/09662839.2013.856307.

Brandão, Ana P. and Isabel Camisão. "Playing the Market Card: The Commission's Strategy to Shape EU Cybersecurity Policy." *Journal of Common Market Studies*, 60 no 5 (2022): 1335–1355. Accessed date: December 16, 2022, https://doi.org/10.1111/jcms.13158.

Buono, Laviero. "Gearing up the Fight against Cybercrime in the European Union: A New Set of Rules and the Establishment of the European Cybercrime Centre (Ec3)." *New Journal of European Criminal Law*, 3 no (3–4), 2012: 332–343. Accessed date: December 16, 2022,https://doi.org/10.1177/203228441200300307

Carrapico, Helena and André Barrinha. "European Union cyber security as an emerging research and policy field." *European Politics and Society*, 19 no 3 (2018): 299–303. Accessed date: December 16, 2022, doi:10.1080/23745118.2018.1430712.

Carrapico, Helena and André Barrinha. "The EU as a Coherent (Cyber)Security Actor?". *Journal of Common Market Studies*, 55 no 6 (2017): 1254–1272. Accessed date: December 16, 20022, doi: 10.1111/jcms.12575.

Csernatoni, Raluca. *The EU's rise as a defense technological power: from strategic autonomy to technological sovereignty*, Carnegie Europe, 2021. Accessed date: December 16, 2022, https://carnegieeurope.eu/2021/08/12/eu-s-rise-as-defense-technological-power-from-strategic-autonomy-to-technological-sovereignty/$

Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Globalisation and the Information Society: The Need for Strengthened Coordination,* COM(1998) 50 final. Brussels, February 04, 1998. Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:51998DC0050&from=EN.

Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Network and Information Security: Proposal for A European Policy Approach,* COM(2001) 298 final. Brussels, June 6, 2001. Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0298:FIN:EN:PDF.

Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A strategy for a Secure Information Society – "Dialogue, partnership and empowerment*, COM(2006) 251 final. Brussels, May 31, 2006. Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0251:FIN:EN:PDF.

Commission of the European Communities. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection*, COM(2009) 149 final. Brussels, March 30, 2009. Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

Council of the European Union. *Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy*, June, 2016. Accessed date: April 25, 2022, http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review_web.pdf.

Council of the European Union. *EU Cyber Defence Policy Framework*, 15585/14. Brussels, November 18, 2014. Accessed date: April 25, 2022, https://ccdcoe.org/uploads/2018/11/EU-141118-EUCyberDefencePolicyFrame-2.pdf.

Christou, George. "The challenges of cybercrime governance in the European Union." *European Politics and Society*, 19 no 3 (2018): 355–375. Accessed date: December 16, 2022, doi: 10.1080/23745118.2018.1430722.

Christou, George. *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy*. Basingstoke: Palgrave Macmillan, 2016.

"Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States". European Defence Agency, May 12, 2017. Accessed date: April 25, 2022, https://eda.europa.eu/news-and-events/news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states

Dunn Cavelty, Myriam. "Europe's cyber-power." *European Politics and Society*, 19 no 3 (2018): 304–320. Accessed date: December 16, 2022, doi: 10.1080/23745118.2018.1430718.

European Commission. *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe,* COM(2010) 245 final. Brussels, May 19, 2010. Accessed date: April 25, 2022, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

European Commission. *Communication from the Commission to the European Parliament, the Council, The EU Internal Security Strategy in Action: Five steps towards a more secure Europe,* COM(2010) 673 final. Brussels, November 22, 2010. Accessed date: April 25, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52010DC0673&from=EN.

European Commission and High Representative. *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, JOIN(2013) 1 final. Brussels, December 7, 2013. Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN.

European Commission and High Representative. *Joint Communication to the European Parliament, the Council Resilience, Deterrence and Defence: Building strong cybersecurity for the EU*, JOIN(2017) 450 final. Brussels, September 13, 2017. Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

European Commission and High Representative. *Joint Communication to The European Parliament and The Council The EU's Cybersecurity Strategy for the Digital Decade,* JOIN(2020) 18 final. Brussels, December16, 2020. Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0018&from=EN.

European Union Agency for Network and Information Security. *Definitions of Cybersecurity: Gaps and Overlaps in Standardisation*, v1.0. Brussels, 2015. Accessed date: April 25, 2022, https://www.enisa.europa.eu/publications/definition-of-cybersecurity/view/++widget++form.widgets.fullReport/@@download/Cybersecurity_Definition_Gaps_v1_0.pdf.

Fahey, Elaine. "EU's Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security'. *European Journal of Risk*

Regulation, 5 no 1 (2014): 46–60. Accessed date: December 16 2022, http://www.jstor.org/stable/24323486.

Juncker, Jean Claude. *State of the Union Address 2017*. Transcript of Speech delivered at the European Parliament, Brussels, September 13, 2017. Accessed date: April 25, 2022, https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_17_3165

"Key Objectives". The European Cybercrime Centre, March 01, 2022, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Köksoy, Fulya. "Avrupa Birliği'nin Siber Güvenlik Politikası: Kurumsalcılık mı Tutarlılık mı?". *Güvenlik Stratejileri Dergisi*, 16 (2020): 635–674. Accessed date: December 1, 2022, doi: 10.17752/guvenlikstrtj.807014.

Official Journal of the European Union. *Regulation (EU) 2019/881 of The European Parliament And of The Council on ENISA (the European Union Agency for Cybersecurity) of 17 April 2019 and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*. Brussels, June 7, 2019. Accessed date: April 25, 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.

Pâris, Constant. *Guardian of the Galaxy? Assessing the European Union's International Actorness in Cyberspace*. College of Europe, 2021. Accessed date: December 16, 2022, Accessed date: https://www.coleurope.eu/sites/default/files/research-paper/edp_1_2021_paris_0.pdf

"PESCO Projects: Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity (CRRT)". Permanent Structured Cooperation. Accessed date: April 25, 2022, https://www.pesco.europa.eu/project/cyber-rapid-response-teams-and-mutual-assistance-in-cyber-security/

"PESCO Projects: Cyber Threats and Incident Response Information Sharing Platform (CTIRISP)". Permanent Structured Cooperation. Accessed date: April 25, 2022, https://www.pesco.europa.eu/project/cyber-threats-and-incident-response-information-sharing-platform/

"PESCO Projects: Cyber and Information Domain Coordination Center (CIDCC)". Permanent Structured Cooperation. Accessed date: April 25, 2022, https://www.pesco.europa.eu/project/cyber-and-information-domain-coordination-center-cidcc/

Pursiainen, Christer. "The Challenges for European Critical Infrastructure

Protection". *European Integration*, 31 no 6 (2009): 721–739. Accessed date: December 16, 2022, doi: 10.1080/07036330903199846.

Sieber, Ulrich. *Legal Aspects of Computer-related Crime in the Information Society (COMCRIME Study) prepared for the European Commission.* Würzburg, January 1, 1998.

Sliwinski, Krzysztof F. "Moving beyond the European Union's Weakness as a Cyber-Security Agent." Contemporary Security Policy, 35 no 3 (2014): 468–486. Accessed date: December 16, 2022, doi: 10.1080/13523260.2014.959261.

Tocci, Nathalie. "Resilience and the role of the European Union in the world," *Contemporary Security Policy*, 41 no 2 (2020): 176-194. Accessed date: December 16, 2022, doi: 10.1080/13523260.2019.1640342.

Wagner, Wolfgang and Rosanne Anholt. "Resilience as the EU Global Strategy's new leitmotif: pragmatic, problematic or promising?". *Contemporary Security Policy*, 37 no 3 (2016): 414–430. Accessed date: December 16, 2022, doi: 10.1080/13523260.2016.1228034

Youngs, Richard. *The EU's strategic autonomy trap*, Carnegie Europe, 2021. Accessed date: December 16, 2022, https://carnegieeurope.eu/publications/83955.