Jakub Wołyniec
Uniwersytet Marii-Curie Skłodowskiej w Lublinie
e-mail: jakub.wolyniec@umcs.pl
ORCID ID: 0000-0001-9411-8568

Cybersecurity in the European Union

Introduction

The complexity of cyberspace as a security environment requires complex and multidimensional actions. Activities taken by states seem to have some effect but are still insufficient given the nature of the threats in cyberspace and the dynamics of their evolution[1]. Since a non-territorial character is a key feature of the Internet, cyberspace security applies to countries with the traditional status of the current or former power, i.e. the United States, Russia, France, the United Kingdom, Germany[2], and emerging powers, e.g. China[3].

Unlike some other threats, cyber-threats affect both great powers with great potential and small states[4]. Because of complex interdependencies between states, they also pose a threat to non-state actors created by states such as intergovernmental organisations or military alliances, in which the vulnerability of one member state poses a significant threat to other members. This is due to the exchange of information about each other and the high level of computer networks. Hence,

[1] D. Galinec, D. Možnik, B. Guberina, *Cybersecurity and cyber defence: national level strategic approach*, "Automatika" 2017, vol. 58, no. 3, pp. 273–286.

[2] See V.K. Aggarwal, A.W. Reddie, *Comparative industrial policy and cybersecurity: the US case*, "Journal of Cyber Policy", 2018 vol. 3, no. 3, pp. 445–466; N. Solovieva et al., *Program Modeling in the Investigation of Crimes Against Cybersecurity in Russia*, [in:] *Creativity in Intelligent Technologies and Data Science*, ed. by A.G. Kravets et al., Cham 2019, pp. 305–314; J. Wołyniec, *The UK Government's Response to Cyber Threats*, "Teka of Political Science and International Relations" 2019, vol. 13, no. 2, pp. 143–154; C. Guitton, *Cyber insecurity as a national threat: overreaction from Germany, France and the UK?*, "European Security" 2013, vol. 22, no. 1, pp. 21–35.

[3] See N. Kshetri, *Cyber-victimization and cybersecurity in China*, "Communications of the ACM" 2013, vol. 56, no. 4, p. 35; J.R. Lindsay, T.M. Cheung, D.S. Reveron, *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, Oxford 2015; G. Austin, *Cybersecurity in China*, Cham 2018; T.M. Cheung, *The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities*, "Journal of Cyber Policy" 2018, vol. 3, no. 3, pp. 306–326.

[4] M. Crandall, C. Allan, *Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms*, "Contemporary Security Policy" 2015, vol. 36, no. 2, pp. 346–368.

there is a clear trend in the international environment towards multilateralisation of cybersecurity activities[5]. This applies to highly developed regions as well as the Global South regions such as Africa, Asia, and Latin America[6].

The aim of the present paper is to analyse actions for the security of cyberspace undertaken by one of the most complex and comprehensive international organisation operating on the European continent, i.e. the European Union (EU). The article also aims at establishing scope and character of the evolution of cybersecurity measures adopted by the EU in recent years. In determining the subject of the analysis, the paper adopts the perspective of the levels of analysis of international relations[7], concentrating on its non-nation-centric angle. Further research in this field developed the idea of a regional, or continental, level of analysis[8]. The class of phenomena and processes analysed at this level includes regional security issues, so it is reasonable to examine how the major regional organisation deals with cybersecurity[9]. Cyber threats and cybersecurity functions in both external and internal environments, crossing fuzzy boundaries. Some processes take place across national borders in a transnational space "at the intersection" of the state interior and the international environment[10].

The first part of the article serves as an introduction to the cyber-threat issue and embeds threats to cybersecurity in the European context by presenting the European cyber threat landscape. The second part presents actions taken by the EU to combat those threats. The activities are presented with reference to published programme documents, the activities of institutions and initiatives undertaken by them. Cybersecurity has been gaining more and more attention within the European

[5] See T. Maurer, *Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security*, https://www.un.org/en/ecosoc/cybersecurity/maurer-cyber-norm-dp-2011-11.pdf, access date: 10.02.2020.

[6] See N. Kshetri, *Cybercrime and Cybersecurity in Africa*, "Journal of Global Information Technology Management" 2019, vol. 22, no. 2, pp. 77–81; C.H. Heinl, *Regional Cybersecurity: Moving Toward a Resilient ASEAN Cybersecurity Regime*, "Asia Policy", 2014, vol. 18, no. 1, pp. 131–159; L.L. Alcantara, *Cybercrime and Cybersecurity in the Global South*, "Journal of Global Information Technology Management" 2013, vol. 16, no. 4, pp. 72–74; K. Smoleń, *The problem of cyber attacks on the critical infrastructure of the state in the energy sector: the case of Turkey*, "Teka of Political Science and International Relations" 2019, vol. 13, no. 2, pp. 27–47.

[7] J.D. Singer, *The Level-of-Analysis Problem in International Relations*, "World Politics" 1961, vol. 14, no. 1, pp. 77–92.

[8] E. Haliżak, *Poziomy analiz w nauce o stosunkach międzynarodowych*, [in:] *Poziomy analizy stosunków międzynarodowych*, ed. by E. Haliżak, M. Pietraś, Warszawa 2013, p. 7.

[9] See B. Buzan, O. Weaver, *Regions and Powers: The Structure of International Security*, Cambridge 2003.

[10] M. Pietraś, *Przestrzeń transnarodowa jako poziom analizy w nauce o stosunkach międzynarodowych*, [in:] *Poziomy analizy stosunków międzynarodowych*, ed. by E. Haliżak, M. Pietraś, Warszawa 2013, p. 129.

Studies discipline as an emerging research and policy field[11], however, the research on the matter has been described as "relatively formative" and lagging behind China and the USA[12]. Although there are voices claiming that Europe possesses different kinds of cyber-power[13]. The literature on the subject of the cybersecurity of the EU presents a vast array of perspectives on the topic, varying from the general federalist approach highlighting vertical interactions of various levels of public authority[14] or works referring to the collective securitisation model[15] to more specific such as a study on Lawrence Lessig's theory of code of cyberspace[16] and, policy-wise, there are papers referring to a values-based approach to cybersecurity[17], joint cybersecurity industrial policy[18], and general cybercrime issues[19].

European cyber threat landscape

Threats to international security differ from others both in scope and scale. They are particularly dangerous as in the era of globalisation and increasing interdependencies they have serious consequences for many geopolitical actors and other players in the international community. An important feature of modern threats to international security is the negative consequences resulting from scientific and technological progress. Asymmetric threats from cyberspace called cyber threats are a good example. They result from both attacks on ICT systems and cyberspace itself. The asymmetry of this type of threat consists in using unconventional methods of action and obtaining a disproportionate result of the attack with relatively low effort[20].

[11] H. Carrapico, A. Barrinha, *European Union cyber security as an emerging research and policy field*, "European Politics and Society" 2018, vol. 19, no. 3, pp. 299–303.

[12] K.F. Sliwinski, *Moving beyond the European Union's Weakness as a Cyber-Security Agent*, "Contemporary Security Policy" 2014, vol. 35, no. 3, pp. 468–486.

[13] M. Dunn Cavelty, *Europe's cyber-power*, "European Politics and Society" 2018, vol. 19, no. 3, pp. 304–320.

[14] F. Mendez, *The European Union and cybercrime: insights from comparative federalism*, "Journal of European Public Policy" 2005, vol. 12, no. 3, pp. 509–527.

[15] G. Christou, *The collective securitisation of cyberspace in the European Union*, "West European Politics" 2019, vol. 42, no. 2, pp. 278–301.

[16] B. Rátai, *Understanding Lessig: implications for European Union cyberspace policy*, "International Review of Law, Computers & Technology" 2005, vol. 19, no. 3, pp. 277–286 which draws from L. Lessig, *Code and Other Laws of Cyberspace*, New York 1999.

[17] M. Schaake, M. Vermeulen, *Towards a values-based European foreign policy to cybersecurity*, "Journal of Cyber Policy" 2016, vol. 1, no. 1, pp. 75–84.

[18] P. Timmers, *The European Union's cybersecurity industrial policy*, "Journal of Cyber Policy" 2018, vol. 3, no. 3, pp. 363–384.

[19] A Kańciak, *Problematyka cyberprzestępczości w Unii Europejskiej*, "Przegląd Bezpieczeństwa Wewnętrznego" 2013, vol. 8, no. 5, pp. 109–120.

[20] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*, Warszawa 2007, pp. 44–45.

A cyber threat can be defined as an "action that may result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system"[21]. Threats to cyberspace can generally be divided into two categories. The first category includes threats caused by intentional and unintentional human activity. Intentional attacks motivated by different harmful intentions constitute the most dangerous threat to the security of cyberspace. They are, for the most part, carried out in cyberspace and using cyberspace. Unintentional mistakes and negligence, such as the lack of appropriate knowledge, bypassing procedures and shortcomings in training people can also be used to carry out attacks. The consequences of cyber attacks include unauthorised access, seizure, or destruction to software and data as well as destruction or damage of hardware. The second category of cyber threats includes threats lacking the human factor, that is, not related to human activity. These might include, among others, manufacturing defects leading to software and hardware malfunction, power grid failures leading to power outage and communication failures, and natural disasters that might damage critical infrastructure, such as floods and earthquakes.

Published annually, the ENISA Threat Landscape Report (ETL) offers a comprehensive overview of threats based on "hundreds of reports from security industry, networks of excellence, standardisation bodies and other independent institutes"[22]. Its 2018 edition (ETL 2018) published in 2019, provides an independent perspective on observed threats, its agents, and current and emerging threat trends. Top five threat include: malware, web-based attacks, web application attacks, phishing and denial of service (DOS). Out of fifteen threats, ETL 2018 report shows that four threat, namely DOS, botnets, data breaches, and information leakage, have both risen in the ranking and are expected to be on the increasing trend. There is one new threat that is also expected to be more dangerous in the future: cryptojacking[23]. Two threats went down in the ranking: spam and ransomware, the latter being also on the declining trend. Also declining are inside threats and cyber espionage, but they have not changed their position in the ranking[24].

The European Union and cybersecurity

The first attempts to prevent the use of cyberspace to disseminate information prohibited by European Community law took place in the late 1980s and early

[21] P.C. Reich, E. Gelbstein, *Law, Policy and Technology: Cyberterrorism, Information Warfare and Internet Immobilisation*, Hershey 2012, p. 228.

[22] *ENISA Threat Landscape*, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape, access date: 10.02.2020.

[23] *Ibid.*, pp. 92–99.

[24] *Ibid.*, p. 9.

1990s. A number of documents on harmful content on the Internet were adopted at that time.[25] Almost a decade later, just before the Amsterdam Treaty entered into force in 1999, a task force for justice and home affairs created by the Maastricht Treaty was developed into a Directorate General. It was the initiator of activities in the field of organised crime and cybercrime[26]. A study on computer-related crime, the so-called COMCRIME study, resulted in its findings being presented to the Council of the European Union (the Council) by the European Commission in 1998[27].

Later, the Commission launched the eEurope initiative in December 1999 in order to ensure that Europe can benefit from emerging digital and information technologies. In June 2000, the European Council adopted a comprehensive eEurope Action Plan and called for its implementation before the end of 2002. The Action Plan underscored the importance of cybersecurity and battling cybercrime. One of the objectives around which the actions were clustered was to make the Internet faster, cheaper and secure[28]. In 2001, the Commission's communication referred to creating a safer information society by increasing the security of information infrastructures and combating cybercrime, both domestic and transnational[29]. This document was supplemented by another communication Network and Information Security, which analysed problems related to the security of computer networks[30].

The process of implementing common standards for criminalising cybercrime, e.g. through framework decisions, was ongoing[31]. It aimed at bringing together all elements from the three-level approach for network and information security: network and information security measures, the regulatory framework for

[25] C. Pounder, *First Steps Towards a European Union Policy on The Securing of Electronic Communications*, "Computers & Security" 1997, vol. 16, no. 7, pp. 590–594.

[26] F. Mendez, p. 519.

[27] U. Sieber, *Legal Aspects of Computer-Related Crime in the Information Society*, 1998, https://www.oas.org/juridico/english/COMCRIME Study.pdf, access date: 10.02.2020.

[28] *eEurope Action Plan*, https://ec.europa.eu/idabc/en/document/70/5849.html, access date: 10.02.2020.

[29] *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM/2000/0890 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890, access date: 10.02.2020.

[30] *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions - Network and Information Security: Proposal for A European Policy Approach*, COM/2001/0298 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52001DC0298, access date: 10.02.2020.

[31] See *Council Framework Decision 2001/413/JHA of 28 May 2001 combating fraud and counterfeiting of non-cash means of payment,* OJ L 149, 2.6.2001, pp. 1–4 and *Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, OJ L 69, 16.3.2005, p. 67–71.

electronic communications, and the fight against cybercrime. In the proposed EU Constitution, Article III-271 referred to the harmonisation of criminal laws in areas of cross-border serious crime. It lists ten crimes including computer crime as well as organised crime and terrorism[32]. In February 2005, the Council adopted a framework decision on attacks against information systems. It introduces a common definition of cyber attacks and EU Member States have agreed together to clarify what constitutes such acts. It also required national legal systems to regulate effective action against cyber attacks[33]. This important document remained in force for eight years until a new directive replaced it.

In 2007, a communication *Towards a general policy on the fight against cyber crime* was published highlighting the need to improve the fight against cybercrime at European and international level[34]. The document identifies the latest trends in cybercrime describing it as more and more sophisticated and internationalised. Three categories of cybercrimes were applied: traditional forms of crime using computer networks, the publication of illegal content over electronic media, crimes unique to electronic networks such as hacking. The communication warns that even though one can observe the growing involvement of organised crime groups in cybercrime, there was no increase in the European prosecutions that were based on cross-border law enforcement cooperation. The Financial Programme *Prevention of and Fight against Crime* is set to support certain important actions: fighting against cybercrime in general, fighting against traditional crime in electronic networks, combating illegal content and improving cooperation structures in the EU[35]. A cybercrime strategy was also being prepared at the time. In 2008, the French EU presidency presented its global plan to combat cybercrime and in 2010, the European Commission prepared the document entitled *Digital Agenda for Europe*. This was the IT sector security development plan and it was to be one of the seven pillars of the Europe 2020 strategy. This program adopted by the European Council replaced the existing Lisbon Strategy[36]. Legislative action towards the EU's cybercrime framework included the 2011 Directive on combating the sexual exploitation of children online and child pornography, and the 2013 Directive on attacks against information systems. It aimed to combat large-scale cyber attacks by

[32] F. Mendez, p. 519.

[33] *Council Framework Decision* 2005/222/JHA of 24 February 2005 on attacks against information systems, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222, access date: 10.02.2020.

[34] *Communication from the Commission to the European Parliament, the Council and the Committee of the Regions - Towards a general policy on the fight against cyber crime*, COM/2007/0267 final, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52007DC0267, access date: 10.02.2020.

[35] *Ibid*.

[36] *Digital Agenda for Europe*, https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe, access date: 10.02.2020.

requiring EU members to strengthen their national cybercrime laws and introduce stricter criminal sanctions[37].

A key document on the security of cyberspace in the EU is the *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* published in 2013. It reflects the EU's comprehensive vision on how best to prevent and respond to disruptions and attacks. The strategy promotes values such as freedom, democracy, safe growth of the digital economy. In addition, it targets actions to reduce cybercrime, increase resilience, and strengthen international cybersecurity and defence policies. The strategy has several priorities: achieving resilience in the field of cybersecurity, reducing cybercrime, linking the development of cyber defence policies and capacity building in the arena of cybersecurity, developing industrial and technological resources for cybersecurity, establishing a coherent international cyberspace policy, and promoting EU core values[38]. Since the strategy was published, the progress within the area of EU's cybersecurity has been achieved not only at political and legislative but also at capabilities level[39]. Not only is cybersecurity among one of the EU's most important priorities but the creation of research and innovation funding streams of 600 million euros for the period 2014–2020[40] reinforced capabilities for cybersecurity so that in the future every Member State has its own cybersecurity centre, and the partnership between public and private sectors will eventually enhance emerging Digital Single Market[41]. The publication was accompanied by the proposed directive on network and information security to strengthen the security information systems in the EU, but it took a couple of years to adopt the directive, considered as one of the most ambitious instruments of EU cyber policy[42].

The details of a draft directive on Network and Information Security (NIS) were agreed in June 2015. It required the EU Member States to develop a network and information security plans and designate competent authorities in this field. An EU cooperation group was to be set up to deal with these issues at a strategic level and to guide operational activities. Moreover, a network of national Computer Security Incident Response Teams (CSIRT) was to be established for operational cooperation

[37] M. Socco, *The EU's efforts in fighting cybercrime: putting together legislative action, cross-sectoral and international cooperation, as well as capacity building*, https://www.thegfce.com/news/news/2017/05/31/the-eus-efforts-in-fighting-cybercrime, access date: 10.02.2020.

[38] *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels 2013.

[39] H. Carrapico, A. Barrinha, p. 300.

[40] *EU Cybersecurity Initiatives – Working Towards a more Secure Online Environment*, https://ec.europa.eu/information_society/newsroom/image/document/2017-3/factsheet_cybersecurity_update_january_2017_41543.pdf, access date: 10.02.2020.

[41] *Digital Single Market*, https://ec.europa.eu/digital-single-market, access date: 10.02.2020.

[42] H. Carrapico, A. Barrinha, p. 300.

in order to increase confidence between the Member States[43]. The NIS Directive (sometimes referred to as NISD) was adopted by the European Parliament in July 2016 and entered into force next month. EU Member States had time to transpose the Directive into their national laws by mid-2018 using a "NIS Toolkit"[44]. Together with the General Data Protection Regulation (GDPR), it ensures a "culture of security" across sectors relying heavily on information communication technology. Entities operating in these sectors, identified as operators of essential services, and digital service providers are obliged have to meet certain security standards[45].

Insufficient action in the defence sphere of cybersecurity was duly noted in the European Union. In order to achieve the strengthening of EU Member States' capacities in this field, in 2018, the Council adopted an updated version of the EU cyber defence policy framework (CDPF). It clarifies the roles of those involved in the cyber defence (i.e. EEAS, EU Military Staff, European Defence Agency, Cyber Defence Project Team and others) and protection of the EU security and defence infrastructure[46]. Also in 2018, the Council and the European Parliament started working on the Cybersecurity Act. The regulation, adopted in April 2019, contains two major elements. First of all, it introduced a system of EU-wide certification schemes for digital products and services. The overall framework sets rules that attempt to solve the problem of the numerous existing certification schemes. Secondly, the new Cybersecurity Act transformed the agency responsible for cybersecurity – ENISA[47].

ENISA, formerly known as the European Union Agency for Network and Information Security (now the European Union Agency for Cybersecurity), has always been a crucial element of EU cybersecurity. The agency was established in 2004 for a time-limited mandate. It is responsible for ensuring an effective level of cybersecurity in IT systems and networks. ENISA is a consultancy centre for EU countries on security issues in cyberspace, the agency also harmonises activities related to risk management and contributes to the development of the information society.

[43] *Network and information security: breakthrough in talks with EP*, https://www.consilium.europa.eu/en/press/press-releases/2015/06/29/network-information-security, access date: 10.02.2020.

[44] *The Directive on security of network and information systems (NIS Directive)*, https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive, access date: 10.02.2020.

[45] *Ibid*.

[46] *EU Cyber Defence Policy Framework (2018 update),* http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf. access date: 10.02.2020.

[47] *EU to become more cyber-proof as Council backs deal on common certification and beefed-up agency*, https://www.consilium.europa.eu/en/press/press-releases/2018/12/19/eu-to-become-more-cyber-proof-as-council-backs-deal-on-common-certification-and-beefed-up-agency, access date: 10.02.2020.

Not only is ENISA increasing awareness of the vulnerability of communication networks and information systems, but it is pointing to the importance of such systems to the socio-economic development of the EU. By analysing current and new trends, ENISA's role is also to mitigate negative consequences of cyber threats that might damage financially some key sectors, for example, e-commerce. In 2010, ENISA was granted a second mandate, and in a 2017 proposal for an EU Cybersecurity Agency, it was suggested that ENISA be given "a more operational and central role in achieving cybersecurity resilience"[48]. New regulations repealed the 2013 Cybersecurity Act and established ENISA as the European Union Agency for Cybersecurity. As of June 2019, ENISA's mandate has been set for an indefinite period of time.

ENISA's activities include publishing annual ENISA Threat Landscape (ETL) of current and emerging trends of cyber threats. The agency also publishes reports and studies on cybersecurity issues such as cloud security, data and privacy protection, and electronic identification and trust services. Moreover, ENISA works closely with a wide range of public and private sector actors to build expertise and capacity for the benefit of society. In 2020, the EU Member States and ENISA planned to organise Cyber Europe 2020 (CE2020) – the 6th pan European cyber crisis exercise. It is part of the Cyber Europe series of exercises launched in 2010 and taking place every two years. Other activities of the EU Agency for Cybersecurity include, for instance, naming October as a European Cybersecurity Month and organising Cybersecurity Standardization Conference in February 2020.

Because of the health crisis linked with the coronavirus pandemic, ENISA is making increased efforts to ensure security in cyberspace. In view of the increased online activity of EU citizens, it is important to make Internet users aware of the risks and manipulations they may face when active in social media. Particular attention is paid to possible disinformation and fake news on coronavirus disease (COVID-19) caused by SARS-CoV-2. Information on the symptoms of the disease and the state of the spread of the pandemic concerns sensitive area: human life and health. Other countries may deliberately circulate false information to spread panic and destabilise EU Member States, as part of the so-called *sharp power* strategy pursued by countries such as China and Russia. ENISA publishes recommendations on a variety of topics including working remotely, and in such sectors as e-health and e-commerce for individual users and entrepreneurs. Free resources and articles have been made available and are updated frequently[49].

The Council of the European Union articulated a serious concern about malicious cyber activities undertaken by non-EU states and non-state actors which led to an adoption of a framework for a joint EU diplomatic response to malicious

[48] G. Christou, p. 285.

[49] *COVID19 – ENISA*, https://www.enisa.europa.eu/topics/wfh-covid19, access date: 08.06.2020.

cyber activities, the so-called cyber diplomacy toolbox. In May 2019, the Council established a framework allowing the EU to impose measures to deter and respond to cyber attacks which are a threat to the EU by imposing sanction on individuals or entities that are involved in or provide support for cyber attacks or attempted cyber attacks. Moreover, if it aligned with the objectives of the Common Foreign and Security Policy (CFSP), it is also possible to sanction those responsible for attacks against non-EU states or international organisations[50].

Other actors are also involved in activities against cybercrime. An example is Europol, which established the European Cybercrime Platform. The EU has its own European Cybercrime Centre (EC3), attached to Europol with headquarters in The Hague, which supports EU institutions and member states in capabilities building required to coordinate anti-cybercrime activities[51]. The EU also has a permanent Computer Emergency Response Team (CERT-EU), established in September 2012, which protects EU agencies and institutions committing to a strengthened and high-level EU Networking and Information Security Policy in Europe. However, there are also voices that its defensive character "limits the EU's leverage in cyberspace"[52]. CERT-EU contributes to the security of the Information and Communications Technology infrastructure of all EU institutions, bodies and agencies. It helps to prevent, detect, respond to, and recover from cyber attacks by "acting as the cyber-security information exchange and incident response coordination hub for the constituents"[53]. An interesting initiative is the Prevention of and Fight against Crime (ISEC) programme, under which ILLBuster operates – a buster of illegal contents spread by malicious computer networks. The project is funded by the European Commission and aims to develop an integrated system for automatic detection of illegal activities on the Internet[54]. The CASES (Cyberworld Awareness and Security Enhancement Structure) operational program also works to protect information data. The latest activities undertaken by the Council concern the security of 5G technology and plans to establish the European Cybersecurity Competence Centre and the Network of Coordination Centres. While it will increase the potential of mobile networks, it is also a source of possible cybersecurity risks. However, in the conclusions adopted by the Council in December 2019, 5G networks are perceived as part of the crucial infrastructure that is necessary for "the maintenance of vital societal and economic functions"[55].

[50] *Cyber-attacks: Council is now able to impose sanctions*, https://www.consilium.europa.eu/en/press/press-releases/2019/05/17/cyber-attacks-council-is-now-able-to-impose-sanctions, access date: 10.02.2020.

[51] K.F. Sliwinski, p. 477.

[52] *Ibid*.

[53] *CERT-EU*, http://cert.europa.eu/static/RFC2350/RFC2350.pdf, access date: 10.02.2020.

[54] *ILLBuster*, http://illbuster-project.eu, access date: 10.02.2020.

[55] *Council Conclusions on the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G*, https://www.consilium.europa.eu/media/41595/st14517-en19.pdf, access date: 10.02.2020.

Conclusion

Due to the asymmetric nature of cyber threats and the dynamics of their evolution, there is a tendency for a growing role of security cooperation activities in cyberspace through joint efforts of states and non-state actors in international relations. Cross-border, trans-sectoral, and global nature of threats arising from cyberspace force the transition from unilateral actions to collective and coordinated actions. States must be involved in guaranteeing institutions and citizens security outside their borders, which results from the dynamics and tendency of changes in the area of new technologies. The dynamics of the emergence of new challenges and their evolution can be seen, for example, in the recent spread of fake news related to COVID-19 caused by SARS-CoV-2 coronavirus. International organisations serve as a forum for discussion to disseminate and analyse knowledge about cybersecurity and the effects of cyber threats, they are at the same time creators of common principles of prevention, legal and institutional solutions, and are complementary to the activities of countries in this field. The legal instruments introduced by the European Union are binding only on the Member States but have also become a benchmark for certain standards in the field of cybersecurity adopted by countries aspiring to join the organisation.

The article shows a natural evolution of cybersecurity means from the time of the 1990s and early 2000s when the focus was set on computer and cyberspace as a tool of serious and organised crime, through the stage when computer crime was endangering cyberspace of the EU Member States, to the period when finally the EU objectives was to achieve an open, safe and secure cyberspace keeping in mind the importance of raising awareness and acquiring skills and knowledge how to avoid or face cyber threat. At the early stages of establishing the EU cybersecurity policy, the documents focused on definitions and identifications of threats and trends. Later stages included organising institutional and legal framework, and setting up specialised institutions, centres and teams.

Not only did the understanding of cyber-related issues changed but also the response of the EU to cyber threats. The transition here is from the soft law instruments (recommendations) such as guidelines, communications, declarations, roadmaps, actions plans, and even comprehensive strategies (2013 Strategy) towards more hard law instruments (obligations) such as directives and other legislative acts (2019 EU Cybersecurity Act). The character of directives has also changed – from directives on cyber-related issues to those characterised as cyber-oriented, for example, the 2016 NIS Directive; each document being more ambitious than the previous one.

The analysis shows that the actions taken by the EU do not directly relate to military operations, but this is an aspect that is still evolving. As the latest research indicates, based on the war in eastern Ukraine and Syria, temporal analysis suggests that cyber activities are independent of traditional warfare. For now,

an attack on cyberspace is not yet an effective tool of exerting pressure in war[56]. The abovementioned steps were followed by a comprehensive package of reforms – an "ambitious data strategy" adopted on 19th of February 2020, a day dubbed "Super Wednesday" and "Europe's Digital Independence Day" in the *Forbes* article entitled the same way[57]. Even if these claims are exaggerated, one cannot overlook the struggles and efforts of the EU in achieving its ambitious cybersecurity goals.

The analysis provides a basis for trying to assess the effectiveness of EU cyber security policy. However, is such an assessment even possible? A study commissioned in 2015 by the European Parliament aimed at developing a better understanding of cybersecurity threats, existing capabilities as well as policy effectiveness. Its executive summary reads: "Due to the inherently relative nature of cybersecurity and the challenges associated with attaining cyberresilience, it is difficult to state whether the new initiatives have been successful"[58]. Instead, its key findings revolved around perceptions about the effectiveness. First of all, while there is still fragmentation in understanding of the cyberdomain by the Member States and in operational capabilities, there is also a noticeable improvement especially with regard to initiatives and cooperation of ENISA and E3C. Secondly, there is a question whether the approach to cybersecurity should be voluntary and informal or mandatory and formal. Thirdly, there is an issue of scope of newly proposed regulations. Thus, operationalisation and a lack of data are main problems in establishing EU cybersecurity effectiveness. The problem is still important today just as it has been in 2015. This is evidenced by a briefing paper published in 2019 which analyses challenges to effective policy delivery. Continued commitment to an effective EU cyber policy is endangered for example by disinformation, departing from the core EU values. Moreover, as the report states, digital systems are so complex that it is impossible to prevent all attacks[59]. These are not the only challenges facing the effectiveness of EU cyber security policy. Other include the proper choice of appropriate regulatory measures, targeting the right audience and a recast of Product Liability Directive[60].

[56] N. Kostyuk, Y.M. Zhukov, *Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?*, "Journal of Conflict Resolution" 2019 vol. 63, no. 2, pp. 317–347.

[57] A. Renda, W. Bytes, *Europe's Digital Independence Day,* Forbes, https://www.forbes.com/sites/washingtonbytes/2020/02/19/europes-digital-independence-day/#40248c544af3, access date: 20.02.2020.

[58] N. van der Meulen, E.A. Jo, S. Soesanto, *Cybersecurity in the European Union and beyond: exploring the threats and policy responses*, https://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU%282015%29536470_EN.pdf, access date: 08.06.2020.

[59] *Challenges to effective EU cybersecurity policy*, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf, access date: 08.06.2020.

[60] G.G. Fuster, L. Jasmontaite, *Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights* [in:] *The Ethics of Cybersecurity*, ed. by M. Christen, B. Gordijn, M. Loi, Cham 2020, pp. 107–111.

While it is difficult to appraise the effectiveness of the EU cyber security, it is not entirely impossible. In her 2018 study, M.G. Porcedda evaluates the effectiveness of the EU cyber security regulations against security breaches[61]. The paper indicates lack of consistency between the measures adopted in the different regulatory instruments which creates a "cacophony of requirements" that is "reducing the ability to counter cyber security breaches"[62]. According to Porcedda, current EU regulations offer "solutions to the symptoms, rather than the causes"[63]. Although the above-mentioned study is focused on the issue of cyber security breach, it partially overlaps with the subject of analysis of the present study (especially as both papers cover ENISA and the NIS Directive). To conclude, the system is as effective as its weakest link. There are gaps in capability and priority differences among Member States. The more similar and convergent policies and strategies are, the more effective they are, and this approach should be part of these strategies.

Keywords:
cybersecurity,
cyber threats,
European Union.

Cybersecurity in the European Union

Because of the asymmetric nature of cyber threats and the dynamics of their evolution, there is a tendency for a growing role of security cooperation activities in cyberspace through joint efforts of states and non-state actors in international relations. New challenges and threats caused by the global pandemic are linked with an increased internet activity. The recent spread of fake news related to COVID-19 illness caused by SARS-CoV-2 coronavirus might be seen as part of sharp power disinformation strategy applied by state actors. International organisations serve as a forum for discussion to disseminate and analyse knowledge about cybersecurity and the effects of cyber threats, they are at the same time creators of common principles of prevention, legal and institutional solutions, and are complementary to the activities of states in this field. By adopting the regional level of analysis as its methodological perspective, the article shows a natural evolution of cybersecurity means from the time of the 1990s and early 2000s when the focus was set on computer and cyberspace as a tool of serious and organised crime, through the stage when

[61] M.G. Porcedda, *Patching the patchwork: appraising the EU regulatory framework on cyber security breaches*, "Computer Law & Security Review" 2018 vol. 34, no. 6, pp. 1077–1098.

[62] *Ibid*., pp. 1091–1092.

[63] *Ibid*., p. 1097.

computer crime was endangering cyberspace of the EU Member States, to the period when finally the EU objectives were to achieve an open, safe and secure cyberspace keeping in mind the importance of raising awareness and acquiring skills and knowledge how to avoid or face cyber threats. At the early stages of establishing the EU cybersecurity policy, the documents focused on definitions and identifications of threats and trends. Later stages included organising institutional and legal framework, and setting up specialised institutions, centres and teams. Not only did the understanding of cyber-related issues changed but also the response of the EU to cyber threats. The transition is from the soft law instruments (recommendations) such as guidelines, communications, declarations, roadmaps, actions plans, and strategies towards more hard law instruments (obligations) such as directives and other legislative acts. The character of directives has also changed – from directives on cyber-related issues to those characterised as cyber-oriented, each being more ambitious than the previous one. The complete appraisal of the effectiveness of the EU cyber security policy is impeded by a specific nature of cyberspace and its security, as well as problems with gathering appropriate data.