„Ante Portas – Security Studies”
2020, No 1(14)
DOI: 10.33674/3201911

Tomasz GAJEWSKI[1]
Poland

TOWARDS RESILIENCE. EUROPEAN CYBERSECURITY STRATEGIC FRAMEWORK

Abstract:
Cyberspace has become critical domain of contemporary societies and states. Growing presence and dense network of various activities have resulted in transformation of strictly technical dimension into nervous system of the world. Naturally, with humans' immersion in cyberspace, the catalogue of threats is growing exponentially - from risks to individuals' security through hazards to corporate, government entities to threats to complex social systems. Resilience of the latter depends on cyberspace. The aim of the paper is to analyse EU's approach to growing dangers, with European Cybersecurity Strategy as main research field. Document will be employed to conduct the study.

Keywords:
European Union; cybersecurity; cyberattacks; resilience; security policy

Introduction

The socio-technological interactions defined by the so called fourth industrial revolution[2] are empowering the transformation of states and international organizations behaviour. As a result, cybersecurity has grown to strategic rank in policies of states and international organizations. The public sphere is fulfilled by reports of cyberattacks on individuals, corporate entities, state and social institutions. There are also ongoing discussions about alleged operations of state's militaries cyber units or state-sponsored hacker groups. This myriad of actors reflects the complexities of cyberspace itself. Therefore, planning and execution of security policies of states and international organizations must be based on comprehensive strategic awareness.

[1] Tomasz Gajewski, PhD, Institute of International Relations and Public Policy Jan Kochanowski University, Kielce, Poland. Email: tomasz.gajewski@ujk.edu.pl
[2] K. Schwab, *The Fourth Industrial Revolution*, London 2016, pp. 1-3.

Cybersecurity threats do not respect state boundaries. Interdependent world requires holistic, transnational approaches. Only the strongest international actors like the United States, China or Russia can effectively manage cyberspace hazards with vast and sophisticated capabilities and resources. European Union members, acting as separate units, have no sufficient potential to face cyberspace threats. There is a sense of urgency to create versatile, commonly accepted strategy to cope with growing danger from hostile actors in cyberspace. Internal crisis in EU is important factor, generating deep divisions in Community. SARS-CoV-2 pandemic has strengthened those negative processes and highlighted new threat vectors. In times of massive anti-EU disinformation activities in cyberspace, offensive operations operations against critical infrastructure elements, data theft and privacy breaches, the question of cybersecurity is crucial.

Crisis-torn EU has managed to launch an initiative aiming at rebuilding and preparation for the post-pandemic world. European authorities underscored the value of o cyberspace, stressing that "recovery investment will be channelled towards strategic digital capacities and capabilities, including artificial intelligence, cybersecurity, secured communication, data and cloud infrastructure, 5G and 6G networks, supercomputers, quantum and blockchain"[3]. The document titled *Europe's moment: Repair and Prepare for the Next Generation*, states that "A new Cybersecurity Strategy will look at how to boost EU-level cooperation, knowledge and capacity (…). This will accompany the review of the Directive on security of network and information systems and a proposal for additional measures on Critical Infrastructure Protection. Together with the ongoing work on cybersecurity as part of the EU Security Union, this will increase capabilities within Member States and boost the EU's overall cybersecurity"[4].

The most important regulations of EU's cybersecurity regulations are merged in a package containing Cybersecurity Strategy outlined in the document cited above; *The Cybersecurity Act: For an enhanced cyber resilience*, empowering ENISA (European Union Agency for Network and Information Security); *The EU cybersecurity certification framework*; *The Directive on security of network and information systems (NIS Directive)*; *Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises*; *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*; *Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*; *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*; *Draft Council Conclusions on a*

[3] *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions*, <https://ec.europa.eu/info/sites/info/files/communication-europe-moment-repair-prepare-next-generation.pdf> (27.06.2020).
[4] *Ibidem*.

Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox")[5]. These regulations, communiqués and joint proposals constitute the framework of EU's cybersecurity activities. There is a need to analyse them and measure their consistency with contemporary and prognosed future security environment in cyberspace.

The scientific output on dealing with subject matter is vast and still growing. Numerous authors analyse EU's (and member states) security policies in cyberspace[6] or cybersecurity itself[7]. There is also a large base of scientific articles in internationally recognized journals[8]. Researcher will also find rich body of material in think-tanks' analytical documents[9] and professional media outlets[10]. Another category of important sources can be found on national government's civil and military cybersecurity units or private companies[11]. The sources set used to this analysis will be comprised mainly of official EU documents. The author will also reach to general sources, reports and analyses in order to sufficiently draw up the context.

[5] *Cybersecurity*, <https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#use-fullinks>, (27.06.2020).

[6] See i.e. P. Baumard, *Cybersecurity in France*, Cham 2017; G. Christou, *Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy (New Security Challenges)*, London 2016; W. J. Schünemann, Wolf J., M. Baumann (Eds.), *Privacy, Data Protection and Cybersecurity in Europe*, Cham 2017; A. Savin, *EU internet law*, Cheltenham 2017; T. H. Synodinou, P. Jougleux, C. Markou, T. Prastitou (Eds.) *EU internet law: regulation and enforcement*, Cham 2017.

[7] C. J. Brooks, C. Grow, P. Craig, D. Short, *Cybersecurity Essentials*, New York 2018; B. Buchanan, *The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations*, Oxford 2017; R. Ellis, V. Mohan (Eds.), *Rewired cybersecurity governance*, Hoboken, NJ 2019; R. Ellis, V. Mohan (Eds.), *Rewired cybersecurity governance*, Hoboekn, NJ 2019; A. N. Guiora, *Cybersecurity: geopolitics, law and policy*, London 2017; F. Kaplan, Dark Territory: The Secret History of Cyber War, New York 2017; J. Kosseff, *Cybersecurity Law*, Hoboken, NJ 2020; D. Van Puyvelde, A. F. Brantly, *Cybersecurity: Politics, Governance and Conflict in Cyberspace*, Oxford 2019; P.W. Singer, A. Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford 2014.

[8] See i.e. "European Journal of Information Security", "Intelligence and National Security", "International Journal of Information Security", "International Security", "Journal of Cybersecurity", "Journal of Cyber Policy", "Network Security", "Political Science", "Survival".

[9] See output of i.e.: Belfer Center, Brookings Institution, Center for Strategic and International Studies; European Institute of Security Studies, German Institute for International and Security Affairs, International Security Information Service Europe, Rand Corporation.

[10] CNET, Computerworld, CSO Online, Infosecurity Magazine, PC World, Security Weekly Signal Magazine, ThreatPost, Wired.

[11] See i.e. Agence nationale de la sécurité des systèmes d'information (France), Försvarets radioanstalt (Sweden), Instituto Nacional de Ciberseguridad (Spain), Narodowe Centrum Bezpieczeństwa w Cyberprzestrzeni (Poland), Národní úřad pro kybernetickou a informační bezpečnost (Czech Republic) The National Cyber Security Centre (Ireland), Nationale Cyber-Abwehrzentrum (Germany), Nucleo per la Sicurezza Cibernetica (Italy).

Before moving to exploration of subject matter, there is a need to introduce methodological toolbox, which will be concluded with hypotheses and research questions needed to verify them along with conceptual framework of the analysis.

Methodology and conceptual framework

Author employs quantitative research strategy, based on scientific pragmatism. The latter emphasizes liberal approach to the selection of research methods, determined by their maximum utility in the exploration of given subject and achieving established objectives[12].

Document analysis constitutes the main method, used in the study. According to Glenn A. Bowen. "document analysis is a systematic procedure for reviewing or evaluating documents—both printed and electronic (…) material. Like other analytical methods in qualitative research, document analysis requires that data be examined and interpreted in order to elicit meaning, gain understanding, and develop empirical knowledge (…). Documents contain text (words) and images that have been recorded without a researcher's intervention. (…) refer to documents as 'social facts', which are produced, shared, and used in socially organised ways"[13]. This method is considered sufficient by the author. The effects of the analysis of the European strategic documents on cybersecurity will be put in contemporary security environment context.

The research problem outlined in the introduction and employed methodological approach, led the author to put following hypotheses:

1) European cybersecurity strategic framework appropriately addresses present and future challenges, risks, threats and chances in cybersecurity domain.
2) To build cyber resilience, the EU will need strategic coherence among member states.

To verify these hypotheses, several questions must be answered:

1) What are the areas of interest of the EU's cybersecurity policies?
2) How the EU constructs its capabilities to perform effectively in cybersecurity domain?
3) What are the parameters of the EU's cyber resilience?
4) What are the main obstacles to achieve cyber resilience in the EU?

To be proper, the analysis needs a definition of the most important analytical categories. The author assumes, that these categories are cyberspace, cybersecurity and cyber resilience.

Cyberspace has no single, commonly accepted definition. However, there is a consensus among scholars, that classic definition coined by William Gibson in 1984 novel "Neuromancer" has high explanatory potential. Gibson wrote,

[12] D. Creswell, *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*, London 2013, pp. 10-12.

[13] G. A. Bowen, *Document Analysis as a Qualitative Research Method*, "Qualitative Research Journal" 2009, vol. 9, no. 2, p. 27.

that cyberspace is "a consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts... A graphical representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the non-space of the mind, clusters and constellations of data"[14]. Gibson's definition emphasizes technological dimension. However, it is impossible to avoid the human realm of cyberspace. Modern societies, as it was said, are immersed in cyberspace. This phenomenon generated digital dependence[15], which grows consequently, causing social vulnerabilities. Author assumes, that cyberspace - as "space without conventionally defined space" – is sphere, where technological and human domains are intertwined.

The EU identifies the "needs of cyberspace" comparing their structure to Maslow's Pyramid, pointing to aspects, the EU cybersecurity strategies have to cover (see the figure 1). Theses aspects can be treated as a junction, where European perception of cyberspace meets with security questions.

Fig 1. The needs of cyberspace.

Source: *ENISA overview of cybersecurity and related terminology*, <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology>, (29.06.2020), p. 4.

[14] W. Gibson, *Neuromancer*, New York 1989, p. 128.
[15] Detailed analysis of this problem can be found in: V. Bartlett, H. Bowden-Jones, *Are We All Addicts Now? Digital Dependence*, Liverpool 2017.

Cybersecurity is likewise hard to define. As result there are many definitions, proposed by scientific, military and state circles. The author seeks to present the EU's perspective on this issue, rather than presenting one of the most popular definitions. European Union Agency for Cybersecurity (ENISA) recognizes four domains of cybersecurity: *communication security* ("protection against a threat to the technical infrastructure of a cyber system which may lead to an alteration of its characteristics in order to carry out activities which were not intended by its owners, designers or users"); *operations security* ("protection against the intended corruption of procedures or workflows which will have results that were unintended by its owners, designers or users"); *information security* („protection against the threat of theft, deletion or alteration of stored or transmitted data within a cyber system"); *physical security* („protection against physical threats that can influence or affect the well-being of a cyber system. Examples could be physical access to servers, insertion of malicious hardware into a network, or coercion of users or their families"); *public/national security* ("protection against a threat whose origin is from within cyberspace, but may threaten either physical or cyber assets in a way which will have a political, military or strategic gain for the attacker. Examples could be 'Stuxnet' or wide-scale DOS attacks on utilities, communications financial system or other critical public or industrial infrastructures")[16]. These domains are interconnected and reflect the complexity of cyberspace itself and chaotic (in deterministic way) actions of individuals and institutions operating in networked "space without space". The EU therefore represents holistic approach to this issue.

The concept of social resilience is quickly gaining attention, especially in climate crisis context[17]. Resilience has also psychological, organizational and engineering connotations. Cyber resilience, in turn, is defined by Alexander Kott and Igor Linkov as the „ability of the system to prepare, absorb, recover, and adapt to adverse effects, especially those associated with cyberattacks". Depending on the context, they "(…) use the term cyber resilience to refer mainly to the resilience property of a system or network"[18]. It is important to add a non-technical layer of cyber resilience – adaptability and skills of professionals working with cyber technologies and societies' intellectual capacity to withhold pressures generated by "living immersed" in cyberspace (cybercrime, privacy issues or disinformation to name a few).

---

[16] *Definition of Cybersecurity. Gaps and overlaps in standardisation*, <https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport> (29.06.2020), pp. 11-12.

[17] See: M. Keck, P. Sakdapolrak, *What is Social Resilience? Lessons Learned and Ways Forward*, „Erdkunde. Archive for Scientific Geography" 2013, vol. 61, no. 1, pp. 6-8.

[18] A. Kott, I. Linkov, *Fundamental Concepts of Cyber Resilience: Introduction and Overview* [in:] *Cyber Resilience of Systems and Networks*, eds. A. Kott, I. Linkov, Cham 2018, pp. 2-3.

Cybersecurity strategy – prepare for the worst

"Securing network and information systems in the European Union is essential to keeping the online economy running and to ensure prosperity. The European Union works on a number of fronts to promote cyber resilience" – states the introductory message on the EU's cybersecurity package website[19]. The EU represents complex approach to cybersecurity question, recognizing the complexity of the cyberspace itself.

First of all, the EU is betting on multilateral cooperation. Cyberspace, as it was noted, does not have sharp, securable boundaries. The threats emerging from it endanger the interconnected European systems, therefore a cooperation between state and non-state actors or stakeholders is required. The document cited in the introductory part of the paper, *Europe's moment: Repair and prepare for the next generation*, emphasizes this cross-sectoral, coordinated activities. The crucial areas of the EU operations are critical infrastructure security, network and information systems security, SMEs and industrial engagement[20]. Cybersecurity policies are placed within the framework of Security Union, which is the evidence of their high rank in the whole EU's political portfolio. Overall increase of the EU and member states capabilities in cybersecurity domains is the main objective. The emphasize put on EU-level cooperation is significant.

In *Cybersecurity Act*, the EU recognizes, that digitalization and growing connectivity make European societies increasingly vulnerable. This can be described as the lowest level (basic security protection) of the EU's cybersecurity policies focus. According to the document, there is an urgent need to develop mitigation procedures of those risks. What is more, the regulation points to information systems and networks used by various types of organizations – from small and medium enterprises to operators of critical infrastructure - as spheres of particular attention of cybersecurity activities[21]. The question of citizens' and organizations' awareness of cybersecurity is also crucial: "Cybersecurity is not only an issue related to technology, but one where human behaviour is equally important. Therefore, 'cyber-hygiene', namely, simple, routine measures that, where implemented and carried out regularly by citizens, organisations and businesses, minimise their exposure to

[19] *Cybersecurity*, <https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#use-fullinks> (08.06.2020).

[20] *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committee*, ibidem.

[21] *Regulation (EU) 2019/881 of The European Parliament and of The Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN> (11.06.2020).

risks from cyber threats, should be strongly promoted"[22]. The possible disruptions of this social "soft underbelly" of cyber systems, constitute severe threat to overall resilience of European networks. Therefore, the EU aims to enhance the resilience on this level. It should be noted, that this type of actions must be delegated to member states, which should ensure appropriate systemic measures to provide educational and technical capabilities to social stakeholders.

The EU is aware that with fast-paced growth of digital markets, comprehensive security measures must be put in place in order to develop efficient "firewall" for this sphere, which is crucial for economy. The European Digital Single Market depends on products and services created along with different certification standards. Therefore, there is a significant risk of "fragmentation and barriers" in undisrupted functioning of European economy. It is required to create certification procedures on the EU level to conduct evaluation of aforementioned products and services. The EU recognizes the necessity of employing risk mitigation procedures in order to tighten control on "evaluation of the security properties of a specific ICT-based products or service e.g. smart cards"[23]. In the words of EU's understanding of this issue, such measures should include: "the categories of products and services covered; the cybersecurity requirements, for example by reference to standards or technical specifications; the type of evaluation (e.g. self-assessment or third party evaluation), and d) the intended level of assurance (e.g. basic, substantial and/or high)[24].

The question briefly described above lies on the intersection of several layers of the EU's cybersecurity policy focus. Basic levels, where it sees threats to "soft" societies' cyber systems, critical infrastructure protection, digital market functions and cyber defence (cyber war). Its particularly important manifestation is 5G network rollout in the EU member states. 5G is crucial for European economic development and global competitiveness, thus it should be considered as a cybersecurity question. The most pressing problem is how to manage Chinese economic offensive. Intensive action of Middle Kingdom's corporate entities generates vast array of threats to cybersecurity. In geopolitical terms, the 5G implementation by Chinese entities may be a method to generate global advantages.

This threat matrix is composed of global and local 5G network disruptions (denial of availability; spying of network traffic or data; modification or rerouting of traffic; destruction or modification of digital or information systems[25]. This also a question of abovementioned standardization procedures

[22] *Ibidem*.
[23] *The EU cybersecurity certification framework*, <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework> (11.06.2020).
[24] *Ibidem.*
[25] *EU coordinated risk assessment of the cybersecurity of 5G networks*, Brussels 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132> (12.06.2020), p. 12.

in order to secure European networks secure against hardware with built-in backdoors. The EU sees threats generated by fully implemented 5G network as more serious than existing 4G, because of their exponentially larger potential, which stems from broader impact on interconnected economies. The integrity and availability of those networks will be a major concern on all levels of the EU and member states activities. The question of 5G is both a security matter (critical systems and services) and an issue of EU's economic position in rapidly changing world.

The EU authorities are also aware of possible cyber disruptions of election cycles on European and member states levels. European Commission recommendation from 2018 states, that "Online communication has reduced the barriers to and the costs of interacting with citizens of the Union in the electoral context. At the same time, it has increased the possibilities to target citizens, often in a non-transparent way, through political advertisements and communications, and to process personal data of citizens unlawfully in the electoral context"[26]. The case of alleged interference of external actors in U.S. presidential campaign and Brexit referendum in UK is the main frame of reference in the EU's logic and understanding of this pressing issue. Computational propaganda, disinformation, misinformation and other information weapons deployed in the interconnected networks with dispersed control, constitute major threat to European (Western) democracy itself[27]. This particular threat grows with relocation of human activities to networked environment (digital dependency)[28].

Cyber war and cyber diplomacy are another spheres of the EU interest in cybersecurity domain. European authorities are well aware, that trajectory of strategic security environment evolution is directed toward intensification of hostile operations in cyberspace[29].

A catalogue of the most sensitive elements of the European networks is constructed as follows:

- Core Network functions (e.g. User Equipment Authentication, roaming, Session Management Functions, access policy management; storage of

[26] *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf> (12.06.2020), p. 3.

[27] L. Bennet, *The disinformation order: Disruptive communication and the decline of democratic institutions*, "European Journal of Communication" 2018, vol. 33, no. 2, pp. 134-135.

[28] T. Gajewski, *Antyzachodnie działania propagandowe w środowisku sieciowym* [in:] *Przekonać, pozyskać, skłonić: re-wizje: teoretyczne i praktyczne aspekty propagandy*, ed. M. Sokołowski, Toruń 2020, pp. 358-362

[29] Cyber attacks: EU ready to respond with a range of measures, including sanctions <https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/> (13.06.2020).

end-user network data; link with third-party mobile networks; exposure of core network functions to external applications);
- Network Function Virtualization management and network orchestration;
- Management systems and supporting services (security management systems, network performance systems etc.);
- Radio Access network (base stations);
- Transport and transmission functions (routers, firewalls, IPS);
- Internetwork exchanges (e.g. network services provided by third parties)[30].

The document cited above, *EU coordinated risk assessment of the cybersecurity of 5G networks*, also introduces a catalogue of possible threat actors, posing danger for 5G networks. This catalogue can be extrapolated for overall security of "European" cyberspace.

- Non-adversary/Accidental;
- Individual hacker;
- Hacktivist group;
- Organised crime group;
- Insider;
- State actor or state-backed actor;
- Cyberterrorists or corporate entities[31].

The EU has constructed broad strategic awareness in cyberspace. The brief analysis of crucial areas of interest of European cybersecurity presented above gives only a limited, but meaningful picture of European perception.

European cybersecurity watchdogs

With defined structure of threat matrix, the EU has put or plan to put sufficient capabilities in place. The most important role in the European cybersecurity system is assigned to European Union Agency for Cybersecurity (ENISA). The Agency has evolved from strictly limited powers and resources to larger role in securing cyberspace. The Cybersecurity Act gave ENISA a permanent mandate. Further regulations empowered it to become operational and crisis management force in European cyberspace. ENISA acts as an umbrella organisation, preparing and conducting pan-European cybersecurity exercises. It helps to develop and evaluate member states' cybersecurity strategies, systems and coordinate network of national CSIRTs (Computer Security Incident Response Teams). ENISA also conducts technological horizon scanning, searching for emerging cyber threats.

[30] *EU coordinated risk assessment of the cybersecurity of 5G networks*, *op. cit.*, pp. 17-18.
[31] *Ibidem*, p. 13.

The ENISA's portfolio is broad. It operates within 4 communities: Cyber Resilience Community, Cyber Defence Community, Cyber Diplomacy and Policies Community and Justice in Cyberspace and Cybercrime Community.

Cyber Resilience Community has 13 functions, i.e. incident handling response, response for hybrid threats, awareness rising, developing industrial and technological resources[32]. Among 11 functions of Cyber Defence Community are interoperability in cyberdefence, situational awareness, information sharing, cooperation and research & development[33]. Cyber Diplomacy and Policies Community aims at capacity building, development and implementation policies and regulations[34]. Justice in Cyberspace and Cybercrime Community consists of 12 functions, i.e. prosecution, development of cyber forensics, attribution, investigation and others[35].

ENISA cooperates with 21 actors from EU and member states structures within the functionalities described above: European Judicial Cybercrime Network (EJCN); European Parliament Committee on Industry, Research and Energy (ITRE), European Judicial Network (EJN); European Commission Directorate-General for Research and Innovation (DG RTD); Europol – European Cybercrime Centre (EC3); European Commission Directorate-General for Migration and Home Affairs (DG Home); CEPOL – European Union Agency for Law Enforcement Training; NIS Cooperation Group; Council, Horizontal Working Party on Cyber Issues (HWP); CERT – EU; CSIRTS Network; European External Action Servie (EEAS); European External Action Service (EEAS) – EU Hybrid Fusion Cell; European Defence Agency (EDA); European Commission Directorate-General for Communications Networks; European Anti-Fraud Office (OLAF); European Commission Directorate-General for International Cooperation and Development (DG DEVCO); European Union Military Committee (EUMC); European Commission Joint Research Centre (JRC); European Commission Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW)[36]. The communities operating within ENISA-led system cover wide

[32] *Cybersecurity Instituional Map – Cyber Resilience Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Cyber%20Resilience%20Community> (14.06.2020).

[33] *Cybersecurity Instituional Map – Cyber Defencee Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Cyber%20Defence%20Community> (14.06.2020).

[34] *Cybersecurity Instituional Map – Cyber Diplomacy and Policies Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Cyber%20Diplomacy%20and%20Policies%20Community> (14.06.2020).

[35] *Cybersecurity Instituional Map – Justice in Cyberspace and Cybercrime Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Justice%20in%20Cyberspace%20and%20Cybercrime%20Community> (14.06.2020).

[36] *Cybersecurity Institutional Map – Actors*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=actors> (14.06.2020).

range of spheres, crossing different domains, from citizen-level and SMEs or industrial sectors to international cyber conflicts.

There are spheres of particular importance for EU cyber policies. One of them is certification schemes mentioned earlier in the analysis. European Cybersecurity Certification Group (ECCG), established by the Cybersecurity Act, is in charge of coordinating certification activities with European institutions and relevant member states bodies. ECCG cooperates with ENISA, exchanges information "to facilitate the alignment of European cybersecurity certification schemes with internationally recognised standards, including by reviewing existing European cybersecurity certification schemes and, where appropriate, making recommendations to ENISA to engage with relevant international standardisation organisations to address insufficiencies or gaps in available internationally recognised standards"[37]. This capability should be recognised as *in statu nascendi*, therefore it is impossible to evaluate its efficiency. ECCG met 3 times in 2019 and 2020. During the January 2020 7-hour long meeting, an update from ENISA and member states were discussed, while DG GROW presented legislative developments[38]. The importance of this Group cannot be overstated, especially in times of 5G network rollout and upcoming "Cambrian explosion" of Internet of Thing over the horizon. With aggressive steps taken by China and other state and non-state actors, European Digital Single Market requires urgent implementation of security measures with common certification mechanism at their centre. It can be stated, that these activities are some type of replenishment to procedures of screening foreign investments connected with critical technologies[39].

The EU tries to build adequate capabilities to enhance overall security of Community's networks. *Directive on security of network and information systems* (NIS Directive) elaborates on broad ranges of threats and establishes common cybersecurity mechanisms on the EU level[40]. In the Article 8, the NIS Directive calls for establishing a single point of contact in member states, to ensure cross-border cooperation of the multi-node cybersecurity network, operating permanently and increasing readiness in times of crisis[41]. It provides

[37] European Cybersecurity Certification Group, <https://ec.europa.eu/digital-single-market /en/european-cybersecurity-certification-group> (14.06.2020).
[38] *European Cybersecurity Certification Group 3rd Meeting, Brussels, 27 January 2020*, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65194> (14.06.2020).
[39] Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union, "Official Journal of the European Union" 2019, L 79 I/7, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN> (14.06.2020).
[40] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, "Official Journal of the European Union", 19.07.2016, <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN> (14.06.2020).
[41] *Ibidem*.

clear procedures of pan-European security requirements and incident notification[42]. The NIS directive constitutes a basis for European Commission recommendation regarding to large scale cyber contingencies. Actors involved in crisis response operations must cooperate in incident handling, monitoring and surveillance. Actors involved must activate and coordinate all required actions and technical mitigation measures to reduce or stop attacks. What is particularly significant, the joint European activities may be coordinated under Integrated Political Crisis Response scheme. There is also required to have common public communication playbook in times of crisis[43].

This brief analysis of the EU's deployed or planned potentials and capabilities to prepare, manage, mitigate and overcome cybersecurity threats and risks does not aspire to status of comprehensive study. It attempts to signal the complexity of the problem, as it is perceived by the EU, and intricacies of institutions and capabilities prepared to cope with cybersecurity dangers.

The EU has appropriate understanding of the cybersecurity landscape. There are no flaws in this perception, that can be identified. It refers both to threat awareness, own constraints and measures required to deploy. To build more detailed picture of the EU' cybersecurity strategy, a reflection on the exact parameters of desired state of cybersecurity and the possible obstacles, that can deny the EU's attempts to achieve it.

European cyber resilience through political cohesion?

Cybersecurity is about people. This succinct phrase explains the inextricable connection between biological and technological domains. People operate devices and networks. They are the most important actors on the receiving end of every process located in cyberspace. It is people, who develop technology and create rules of operating it. They must also face consequences of every negative or hostile behaviour in cyberspace.

When the (still) most important form of social organisation, states, are concerned, cyberspace and cybersecurity questions are extremely complicated. They are political, social and economic. When it comes to even higher form of organisation, i.e. community of sates, which is exemplified by the European Union, the question of coherent policy is exceptionally difficult.

Cyber resilience on systemic, pan-European level is desired by the EU. The documents analysed in this paper constitute an evidence of such approach. The parameters of this "state of resilience" stem from the EU's overall *modus operandi*. The Community is not a unified structure with clear separation of competences within the vast ecosystem of institutions. The important level of

[42] *Ibidem.*

[43] *Commission Recommendation (Eu) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises*, "Official Journal of the European Union" 19.09.2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN> (14.06.2020).

resilience will be achieved when the whole structure operates efficiently, especially in times of severe crises. Large scale emergencies, which start with hostile actions in European networks will demand flexibility. The EU has not faced situation of this kind. Major network disruptions did not occur for the time being. Of course, serious cyberattacks, like ransomware cases in Europe[44] or pandemic-related disinformation activities in cyberspace[45], DDoS attacks[46] and others hit European infrastructure. These attacks were managed within the scope of member state capabilities and resources. There is, however, a sense of danger of major cyberattack on cyber elements of critical infrastructure and ignition of multisectoral crisis. Some events in the close geographical vicinity of the EU can be described as a harbinger of the coming crises. The 'Industroyer' malware, which hit Ukrainian energetic grid was the first cyberattack which targeted physical infrastructure since operation against the Iranian nuclear installations with Stuxnet bug[47]. This particular case offers a glimpse of what to expect in conflicted world, where hostile operations against the struggling EU can be channelled through cyberspace with potentially devastating effects in networked European societies. The EU has limited autonomous potentials which are not dependent on member states. Therefore, the EU's cyber resilience means first and foremost its efficiency in coordinating member states, which maintain superiority in decision-making and conducting real operations in cyberspace. Although the EU is a security community[48], its competences and capabilities are limited by member states policies. In EU's cybersecurity strategies, resilience is coherence. Basically, EU treats increased level of coordination and cooperation as a success, especially in security sphere. Evidently, such complex issue as cybersecurity needs clear legal framework. Creation of abovementioned system o regulations is a step towards achievement of resilience of this type. It should be noted, that vast quantity of private entities functions within European cybersecurity system, therefore the existence of comprehensive legal spine is crucial[49]. It applies not only to common political reaction to large scale crises, but also strictly technical

[44] S. Coble, *Ransomware Attack on Europe's Largest Private Hospital Operator*, <https://www.infosecurity-magazine.com/news/ransomware-attack-on-fresenius/> (15.06.2020).

[45] B. Sander, N. Tsagourias, *The covid-19 Infodemic and Online Platforms as Intermediary Fiduciaries under International Law*, "Journal of International Humanitarian Legal Studies" 2020, vol. 17, no. 1, pp. 4-5.

[46] R. Millman, *Biggest-ever packets-per-second DDoS attack hits large European bank* <https://www.scmagazineuk.com/biggest-ever-packets-per-second-ddos-attack-hits-large-european-bank/article/1687794> (16.06.2020).

[47] A. Greenberg, *'Crash Override': The Malware That Took Down a Power Grid*, <https://www.wired.com/story/crash-override-malware/> (16.06.2020).

[48] J. Mitzen, *Anxious community: EU as (in)security community*, *European Security*, „European Security" 2018, vol. 27, no. 3, p. 394.

[49] M. G. Procedda, *Public - Private Partnerships: A „Soft" Approach to Cybersecuriy? Views from the European Union*, New York 2014, p. 196.

coordination in case of multilevel attack on elements of critical infrastructure, which may be owned by private operators. Achieving this type of coherence certainly equals top-down resilience and a step towards pan-European readiness.

Systemic resilience on EU level must be complimented by bottom-up constructed resilience. It is a question of the utmost importance in the case of cyber hygiene (around 80% of cyberattacks are effects of inadequate habits[50]), awareness of threats to day-day activities of the EU citizens and, especially, in case of external disinformation activities. The EU delegates large parts of responsibility for these spheres to member states, but also runs its own programs, aimed at building knowledge and spreading patterns of good practices (also for SMEs and civil society institutions)[51].

Cyber vulnerabilities are not limited to technical domain – integrity of firewalls, software and hardware in their most advanced functions (SCADA). They broad constellation of threats, but author argues, that disinformation induced through cyberspace is potentially most damaging phenomenon from EU perspective. According to ENISA, "societies will have to develop defences against such attacks, particularly the ones that aim to potentially affect democratic processes such as elections, legislative procedures, law enforcement and justice. In the context of cyber security, disinformation campaigns should be closely monitored and thoroughly analysed in order to counter similar attacks in the future"[52]. This mindset is elaborated in concrete activities of EU institutions and embodied in East StratCom Task Force, which is responsible for detection, analysis and debunking of false news in European electronic media ecosystem. The significance of resilience in this sector of cybersecurity was shown by several momentous events – migration crisis, Brexit referendum, Russian information operations and aggressive activities of China during pandemic[53]. Resilience against disinformation operations becomes one of the most important features of overall security posture. Disinformation has potential to disrupt whole social systems, expose and aggravate negative emotions[54]. Russian and Chinese disinformation campaigns are converged in general objective of weakening the EU as a whole and its ability to act as a

[50] *Review of Cyber Hygiene Practices*, <https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport> (17.06.2020).

[51] *European Cybersecurity Month 2019 is launched*, <https://www.enisa.europa.eu/news/european-cybersecurity-month-2019-is-launched> (16.06.2020), p. 6.

[52] *Disinformation Operations in Cyber-space*, <https://www.enisa.europa.eu/publications/info-notes/disinformation-operations-in-cyber-space> (17.06.2020).

[53] M. Scott, L. Kayali, L. Cerulus, *European Commission accuses China of peddling disinformation*, <https://www.politico.eu/article/european-commission-disinformation-china-coronavirus/> (17.06.2020).

[54] I. Ciosek, *Aggravating Uncertainty¸ Russian Information Warfare in the West*, "Torun International Studies" 2020, vol. 13, no. 1, pp. 66-67.

consolidated actor[55]. Thus, cyber resilience, although not so "effective" like anti-terrorism or military security, is a strategic necessity in increasingly instable world.

Complex European cybersecurity system is burdened with serious shortcomings. If the cyber resilience in relations between EU institutions (horizontal) and relations between them and member states (vertical) is crucial, renationalization of political stance of the latter is most important obstacle. Member states tend to accumulate responsibilities for cybersecurity policies on national level. European authorities are aware of states superiority in security domain and acknowledges their role in official regulations. It stems from profound dilemma of European integration project – reluctance to build cross-sectoral, EU-driven mechanisms and, as result, limiting the role of member states. The EU recognizes the need to transnational, cross-sectoral approach to issues like cybersecurity, but its efforts are effectively blocked by member states. Thus, fragmentation of EU's cybersecurity policy remains the most important challenge on the path to achieve comprehensive cyber resilience[56].

Second tier of cyber resilience, disinformation immunity and proper habits in networked environment of citizens and organisations is extremely hard to achieve. The EU invests a lot of resources in awareness building. In the case of disinformation, the techniques are so sophisticated, that, as Ondrej Filipec argues "even experts may sometimes fall into the trap when thinking they can detect it and demarcate"[57]. The issue is complex, and the main obstacle is often unwillingness to reform traditional education system, direct it towards critical thinking skills and develop digital literacy among seniors.

Regarding to cyber hygiene habits, resilience building efforts are often denied by lack lack of compliance with security policies and good practices[58]. Creation of proper, responsible attitudes is a long process of fundamental work. There is no doubt, that member states governments are aware of this challenge, but the economic determinants, political questions and traditional approaches to education may contradict the EU's broad vision of strategic cyber resilience.

The points analysed above are mere manifestation of the complex question of cyber resilience in the EU. They stem from both complexity of the issue and structural problems of the Community itself.

---

[55] A. Legucka, M. Przychodniak, *Disinformation from China and Russia during the COVID-19 Pandemic*, "PISM Bulletin" 2020, no 86(1516), p. 2.

[56] J. Odermatt, *The EU as a cybersecurity actor* in: *Research Handbook on the EU's Common Foreign and Security Policy*, eds. S. Blockmans, P. Koutrakos, Cheltenham 2018, p. 346.

[57] O. Filipec, *Towards a Disinformation Resilient Society? The Experience of the Czech Republic*, "Cosmopolitan Civil Societies: an Interdisciplinary Journal" 2019, vol. 11, no. 1, p. 16.

[58] S. Pfleeger, M. A. Sasse A. Furnham, *From Weakest Link to Security Hero: Transforming Staff Security Behavior*, "Homeland Security & Emergency Management" 2014; vol. 11, no. 4, p. 496.

Conclusions

Hypotheses put in the beginning of this limited study were positively verified. The EU cybersecurity framework represents deep understanding of cyberspace environment, especially the present and future threats. There is also a clear evidence, that implementing policies programmed by the framework will encounter major obstacles, which are results of structural flaws in the EU itself and dynamically changing political, economic and social landscape.

The EU sees cybersecurity as a multidimensional security domain, where large scale, transnational threats intersect with dangers to citizens, organisations and business entities. Thus, the area of European interest in cybersecurity mirrors the intricacy of the cyberspace itself. The EU constructs its own resources and capabilities to effectively coordinate member states cybersecurity policies and, primarily, crisis response operations.

European agenda on cybersecurity also assumes investing in bottom-up initiatives like education and awareness building. The main objective of this broad set of activities is two-fold cyber resilience. The EU aims at achieving resilient operating system and smooth horizontal (European institutions ecosystem) and vertical (institutions and member states) coordination. Second, but not less important, objective is the bottom-up resilience of citizens and social institutions of various types (from NGOs to entrepreneurships) against disinformation and "day-to-day" dangers of broadening presence in cyberspace. Those activities face hurdles from conflicting interests of member states and reluctance to change habits of behaviour in cyberspace.

Whether the EU will overcome these obstacles remains to been seen. Nevertheless, cybersecurity and cyber resilience are questions of critical importance. The EU's strength and position in rapidly changing international environment will depend on the outcome of these efforts.

BIBLIOGRAPHY

- ✓ Bartlett V., Bowden-Jones H., *Are We All Addicts Now? Digital Dependence*, Liverpool 2017
- ✓ Bennet L., *The disinformation order: Disruptive communication and the decline of democratic institutions*, "European Journal of Communication" 2018, vol. 33, no. 2
- ✓ Bowen G. A., *Document Analysis as a Qualitative Research Method*, "Qualitative Research Journal" 2009, vol. 9, no. 2
- ✓ Ciosek I., *Aggravating Uncertainty¸ Russian Information Warfare in the West*, "Torun International Studies" 2020, vol. 13, no. 1
- ✓ Coble S., Ransomware Attack on Europe's Largest Private Hospital Operator, <https://www.infosecurity-magazine.com/news/ransomware-attack-on-fresenius/>

- ✓ *Commission Recommendation (Eu) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises*, "Official Journal of the European Union" 19.09.2017, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H1584&from=EN>
- ✓ *Commission Recommendation of 12.9.2018 on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament*, <https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-cybersecurity-elections-recommendation-5949_en.pdf>
- ✓ *Communication From The Commission To The European Parliament, The European Council, The Council, The European Economic And Social Committe And The Committee Of The Regions*, <https://ec.europa.eu/info/sites/info/files/communication-europe-moment-repair-prepare-next-generation.pdf>
- ✓ Creswell D., *Research Design: Qualitative, Quantitative, and Mixed Method Approaches*, London 2013
- ✓ Cyber attacks: EU ready to respond with a range of measures, including sanctions <https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/>
- ✓ *Cybersecurity Institutional Map – Actors*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=actors>
- ✓ *Cybersecurity Institutional Map – Cyber Defence Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Cyber%20Defence%20Community>
- ✓ *Cybersecurity Institutional Map – Cyber Diplomacy and Policies Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Cyber%20Diplomacy%20and%20Policies%20Community>
- ✓ *Cybersecurity Institutional Map – Cyber Resilience Community*, <https://www.enisa.europa.eu/cybersecurity-institutional-map/results?root=communities&community=Cyber%20Resilience%20Community>
- ✓ *Cybersecurity Institutional Map – Justice in Cyberspace and Cyber-crime Community*, <https://www.enisa.europa.eu/cybersecurity-institutionalmap/results?root=communities&community=Justice%20in%20Cyberspace%20and%20Cybercrime%20Community>
- ✓ *Cybersecurity*, <https://ec.europa.eu/digital-single-market/en/policies/cybersecurity#usefullinks>
- ✓ *Definition of Cybersecurity. Gaps and overlaps in standardisation*, <https://www.enisa.europa.eu/publications/definition-of-cybersecurity/at_download/fullReport>,

- ✓ *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, "Official Journal of the European Union", 19.07.2016, <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN>
- ✓ *Disinformation Operations in Cyber-space,* <https://www.enisa.europa.eu/publications/info-notes/disinformation-operations-in-cyber-space>
- ✓ *EU coordinated risk assessment of the cybersecurity of 5G networks*, Brussels 2019, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132>
- ✓ *European Cybersecurity Certification Group 3rd Meeting, Brussels, 27 January 2020*, <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=65194>
- ✓ European Cybersecurity Certification Group, <https://ec.europa.eu/digital-single-market/en/european-cybersecurity-certification-group>
- ✓ *European Cybersecurity Month 2019 is launched*, <https://www.enisa.europa.eu/news/european-cybersecurity-month-2019-is-launched>
- ✓ Filipec O., *Towards a Disinformation Resilient Society? The Experience of the Czech Republic*, "Cosmopolitan Civil Societies: an Interdisciplinary Journal" 2019, vol. 11, no. 1
- ✓ Gajewski T., *Antyzachodnie działania propagandowe w środowisku sieciowym* [w:] Przekonać, pozyskać, skłonić: re-wizje: teoretyczne i praktyczne aspekty propagandy, red. M. Sokołowski, Toruń 2020
- ✓ Gibson W., *Neuromancer,* New York 1989
- ✓ Greenberg A., *'Crash Override': The Malware That Took Down a Power Grid*, <https://www.wired.com/story/crash-override-malware
- ✓ Millman R., *Biggest-ever packets-per-second DDoS attack hits large European bank* <https://www.scmagazineuk.com/biggest-ever-packets-per-second-ddos-attack-hits-large-european-bank/article/1687794>
- ✓ *Regulation (EU) 2019/452 of the European Parliament and of the Council of 19 March 2019 establishing a framework for the screening of foreign direct investments into the Union*, "Official Journal of the European Union" 2019, L 79 I/7, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0452&from=EN>
- ✓ Keck M., Sakdapolrak P., *What is Social Resilience? Leassons Learned and Ways Forward*, „Erdkunde. Archive for Scientific Geography" 2013, vol. 61, no. 1
- ✓ Kott A., Linkov I., *Fundamental Concepts of Cyber Resilience: Introduction and Overview* [in:] *Cyber Resilience of Systems and Networks*, eds. A. Kott, I. Linkov, Cham 2018
- ✓ Legucka A., Przychodniak M., *Disinformation from China and Russia during the COVID-19 Pandemic*, "PISM Bulletin" 2020, no 86(1516)

- ✓ Mitzen J., *Anxious community: EU as (in)security community, European Security*, „European Security" 2018, vol. 27, no. 3
- ✓ Odermatt J., *The EU as a cybersecurity actor* in: *Research Handbook on the EU's Common Foreign and Security Policy*, eds. S. Blockmans, P. Koutrakos, Cheltenham 2018
- ✓ Pfleeger S., Sasse M. A., Furnham A., *From Weakest Link to Security Hero: Transforming Staff Security Behavior*, "Homeland Security & Emergency Management" 2014; vol. 11, no. 4
- ✓ Procedda M. G., *Public - Private Partnerships: A „Soft" Approach to Cybersecuriy? Views from the European Union*, New York 2014
- ✓ *Regulation (EU) 2019/881 of The European Parliament and of The Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)*, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN>
- ✓ *Review of Cyber Hygiene Practices*, <https://www.enisa.europa.eu/publications/cyber-hygiene/at_download/fullReport>
- ✓ Sander B., Tsagourias N., *The covid-19 Infodemic and Online Platforms as Intermediary Fiduciaries under International Law*, "Journal of International Humanitarian Legal Studies" 2020, vol. 17, no. 1
- ✓ Schwab K., *The Fourth Industrial Revolution*, London 2016
- ✓ Scott M, Kayali L., Cerulus L., *European Commission accuses China of peddling disinformation*, <https://www.politico.eu/article/european-commission-disinformation-china-coronavirus/>
- ✓ *The EU cybersecurity certification framework*, <https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework>