ONLINE JOURNAL MODELLING THE NEW EUROPE
NO. 37 / 2021

DOI: 10.24193/OJMNE.2021.37.06

COMPARATIVE ANALYSIS OF CYBERSECURITY STRATEGIES. EUROPEAN UNION STRATEGY AND POLICIES. POLISH AND SELECTED COUNTRIES STRATEGIES

Andrzej JACUCH, PhD
Military University of Technology, Poland
andrzej.jacuch@wat.edu.pl

Abstract: *The Western democracies: the United Kingdom, the United States, the European Union countries are targeted by hybrid threats predominantly on two fronts – cyberspace and information. This article focuses on cybersecurity. The rapid development of ICT technologies and cyberspace have had a tremendous impact on societies and more general on the international security environment. The EU and its members efficient functioning depends on a coherent and effective system to counter cyber threats at strategic, legal and institutional levels. The objective of this paper is to identify, analyse and assess the adequacy of the Polish National Cyber Security Strategy (Polish NCSS), including the implementation of EU's regulations. The article presents description and analysis of the the EU responses to cyber threats; and the Polish strategy. For comparison, strategic documents of the United Kingdom, the United States, France, Lithuania and Estonia are analysed. It presents the findings of a comparative analysis of the Polish strategy with the five national strategies and present recommendations to enhance cybersecurity.*

Keywords: Cyberspace, Cyber security, National Cyber Security Strategy, EU Cyber Security strategy and policies.

Introduction

Emerging innovations in cyber technologies - artificial intelligence, encryption, authentication, quantum computing, 5G mobile technology, IT-OT Convergence and others - impact cybersecurity and contribute to changes in the area of national and global security. During the COVID-19 pandemic organisations, public and private at local, national and international levels, have switched to work from home and it may continue in a post-COVID world. A boom in remote working also impacts the future cybersecurity (Bisson, 2020). It is becoming more and more problematic to define the nature and methods of preventing cyber threats. Further increase

in cyber threats using more advanced information and communication technologies may concern ever newer aspects.

A country is exposed to higher cyber threats impacts and damages because: its laws and policies related to cyber security being not sufficient or not implemented effectively; technology and infrastructure inadequacies and lack of knowledge and preparedness against attacks; and lack of training and awareness of users and lack of coordination and cooperation between institutions and organizations (Senol and Karacuha 2020, p. 17).

In 2007, a wide-ranging cyber attack on Estonia paralysed numerous government and corporates sites. The escalation in these kinds of attacks highlighted the need for governments to formulate national cyber strategies (Attatfa et al. 2020, p. 60). Cyber Strategies and regulations on the safety and security of cyberspace enable a safer use of cyberspace. National Cyber Security Strategies (NCSS) improve the security and resilience of national infrastructures and services. A NCSS is "a national plan of action based upon a national vision to achieve a set of objectives that contribute to the security of the cyberspace domain" (Besseling et al. 2013, p. 4).

Cyber security strategic documents of Central European countries, including a comparison with the strategic documents of Estonia and the United Kingdom were discussed in "Cyber security strategic documents analysis". Its attention is on the history of cyber security in EU and structure of national cyber security strategic documents (Buřita and Halouzka 2019, pp. 6). National Cyber Security Strategies and policies worldwide are analysed in "Creating and Implementing an Effective and Deterrent National Cyber Security Strategy" (Senol and Karacuha 2020, pp. 1-19). It stresses that countries around the world continue to develop and strengthen their national strategies and policies incorporating their cyber defence and offence forces, into their national security. Other authors adopt the framework of securitization theory on both civil and military approaches to cybersecurity and discuss policies of Eastern European countries and the Baltic states (Tomic et al. 2018, pp. 1039-1055).

In the following paragraphs, I seek to analyse the EU's Cybersecurity Strategy and policies, their implementation in Poland and to compare the Polish NCSS with the strategies of five countries leading in cyber security according to the 2018 ITU Global Cybersecurity Index. The question is how Polish NCSS responds to cyber threats. This requires answering such questions as: How to define cyberspace? What are EU responses to cyber threats? How has Poland implemented the EU Cyber Security Strategy and policies? What are the strengths of the top

national strategies? What needs to be improved concerning cyber security in Poland? The aim of the study is to substantiate the thesis that the Polish NCSS, legislative and institutional tools require continued further work, including fully implementing upcoming EU proposals as well as best practices adopted by the most cyber security advanced countries.

The first section analyses the definitions of cyberspace concluding there has been no unified definition in international and national legal acts agreed upon yet. In the second section the EU approach to cyber security is discussed. The last section compares Polish NCSS with the strategies of the United Kingdom, the United States of America, France, Lithuania and Estonia. It concludes with findings from the above analyses proposing further directions of work on the Polish NCSS.

The research process uses qualitative research methods as well as work experience, synthesis, abstracting, comparison, generalization and implication. The article analyses reference texts and legal acts, the cyber security strategies, directives and regulations. Other sources are monographs, articles referring to the investigated questions, and internet sources.

How to define cyberspace?

The lack of a common definition of cyberspace is an obstacle to the formal and legal regulation of cyber security at both national and international level. The deficit of international regulations is also a problem in relations between states.

“The term ‘cyber’ has been used to describe almost anything that has to do with data networks and computers, especially in the security field. Unfortunately, however, there is no consensus on what ‘cyberspace’ is, let alone what are the implications of conflicts in cyberspace” (Lorents and Ottis 2010, p. 267).

Lan and Inkster (2020, p. 79.) conclude that “cyberspace had its own uniqueness – both a virtual, man-made side, characterized by outstanding technical empowerment and a highly complex operation mechanism, and an integration with the traditional real world, with the boundary between the two becoming ever more blurred and even able to be ignored. In general, conflict and cooperation co-exist in the international governance of cyberspace, exploration and practice are being constantly developed, some basic principles and rules have reached consensus and been put into practice”.

The European Union defines cyber space as “the time-dependent set of tangible and intangible assets, which store and/or transfer electronic information. Cybersecurity comprises all activities necessary to protect cyberspace, its users, and impacted persons from cyber threats” (ENISA 2017, p. 6).

The UK Cyber Security Strategy defines cyberspace as “the interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, Internet-connected devices and embedded processors and controllers. It may also refer to the virtual world or domain as an experienced phenomenon, or abstract concept” (HM Government 2016, p. 75). The definition also includes the essential functions of cyberspace, which are to store, modify and transmit information.

The US Department of Defence defines cyberspace as “a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (US Congressional Research Service 2021).

These definitions put impact on the technical aspect of cyberspace. However, cyberspace is not only the sum of physical components or operations performed by users on networks, but also a new area for human activities that eludes physical measurements. This social aspect is included in the definition adopted by the NATO Cooperative Cyber Defence Centre of Excellence from Lorents and Ottis (2010, p. 267): “cyberspace is a time-dependent set of interconnected information systems and the human users that interact with these systems”.

The concept of cyberspace was introduced into the Polish legal system by the Act of 30 August 2011 (Kancelaria Sejmu RP 2011). The Act, in Article 1, section 2, point. 1b defines cyberspace as an area of "processing and exchange of information created by information and communication systems, ..., together with links between them and relations with users". This definition overlooks the issues of data collection in ICT systems, including their vulnerability to various threats. This data will often be more difficult to recover or restore than to rebuild the cyber infrastructure (Wasilewski 2013, pp. 225-234).

Cyberspace like the physical world, also has military and strategic dimensions and requires countries to work together to defeat cyber opponents. (Attatfa et al. 2020, p. 60). It is important to note that Cyberspace was recognised by NATO as another domain of law enforcement operations (NATO 2016, pars 70-71). In July 2018, NATO decided to establish a Cyberspace Operations

Centre in Belgium to provide situational awareness and coordination of NATO operational activity within cyberspace. NATO members are developing offensive cyber capabilities to provide intelligence, active defences, and retaliatory cyberattacks (Libicki 2019, pp. 12-13). In 2019, France announced its doctrine for offensive cyber operations (Laudrain 2019).

Cyberspace is governed by national and international laws, standards, political agreements, and technical protocols. Cybernorms are not uniform in nature. This diversity requires different legal solutions. The standards for protecting the integrity of databases are a completely different set of issues from those for protecting a company's network or protecting critical infrastructure against a cyber attack. Achieving consistency between national and international standards governing various aspects of cyberspace would improve progress in this area.

EU Cyber Security Strategy and Polices

Cyber attacks can cause disruption not only to companies or states but also to organisations such as the EU. Number of recorded incidents in the EU is continuously growing, resulting in increased cooperation between Member States. The EU has been expanding its international role in foreign and security policy to include cybersecurity, where it plays a vital role. The EU's role as a global cyber-player is better understood through the prism of the global cyber regime complex and the strategies that the EU pursues within this complex, rather than by merely examining the effectiveness of its actions within individual regimes (e.g. cybercrime, stability, human rights) (Pawlak 2019, pp. 167-186). The EU aims to unify regulations for functioning in cyberspace and to increase cooperation between member countries, as well as with NATO and other international organisations.

The 2013 EU cybersecurity strategy clarified roles, responsibilities and activities, like: achieving cyber resilience, reducing cybercrime, developing an EU Cyber Defence Policy and capabilities in the framework of the Common Security and Defence Policy, developing the industrial and technological resources for the Digital Single Market, establishing an international cyberspace policy for the EU (European Commission 2013). The EU has updated its priorities for network and information security policy with the aim to develop a capacity to cope with security challenges within the EU Agency for Network and Information Security (Official Journal of the

European Union 2013). The Digital Single Market Strategy from 2015 serves the creation of better access to digital goods and services (European Commission 2015).

Since then, the EU has adopted legislative proposals, secured investment, and fostered cooperation within the EU and with partners, particularly NATO. It adopted a set of measures for cooperation in case of a large-scale cyber incident (European Commission 2016). The adoption of the Directive on security of network and information systems (NIS) is the first EU-wide legislation on cybersecurity across the EU (The European Parliament and the Council of the European Union 2016). It calls for Member States to adopt a national strategy for the security of networks and information systems, defines the structure of the national cybersecurity system[1] and the tasks and responsibilities of the entities comprising that system and the Critical Incident Panel.

In September 2017, the EU published a cybersecurity package including initiatives in three areas: resilience to cyber-attacks and cybersecurity capacity, an effective criminal law and global stability through international cooperation (European Commission 2017a). In 2018, a Network of Cybersecurity Competence Centres and a new European Cybersecurity Industrial, Technology and Research Competence Centre were proposed, having built on the expertise that has already existed in more than 660 cybersecurity centres from all Member States. It is also ensuring cybersecurity of 5G networks and developing measures which can be used to strengthen the EU's response to activities that harm its interests (European Commission 2018). The 2019 Cybersecurity Act has provided a consolidated cybersecurity certification framework (Official Journal of the European Union 2019). It has reformed the ENISA and created a certification framework, which provides support to Member States, EU institutions and businesses, including the implementation of the NIS Directive.

The sanctions system, so called Cyber Diplomacy Toolbox, agreed in May 2019 allows the EU to impose targeted restrictive measures to prevent and respond to cyber attacks (The Council of the European Union 2019). Based on this legislation, in July 2020, the EU for the first time ever imposed sanctions on six people and three entities responsible for various cyber attacks, including an attempted cyber attack on the Organisation for the Prohibition of Chemical Weapons (OPCW) in 2017. Restrictions were imposed on the GRU's Main Centre for Special Technologies, four

[1] 1) key service providers; 2) digital service providers; 3) three Computer Security Incident Response Teams, sectoral cyber security teams; and public finance sector entities.

GRU officials, two Chinese citizens and one Chinese and one North Korean company. The sanctions include a travel ban on EU territory and an assets freeze (CyberDefence24.pl 2020).

Despite the EU's efforts to ensure greater coherence, the legislative framework in the Member States relating to cyber security remains incomplete. The ECSO Digital Europe (2019) present current status of the implementation of the NIS Directive in all member countries. In March 2019, several countries did not have a fully implemented Directive in place. The European Court of Auditors has considered challenges to effective implementation of the EU cybersecurity policy and produced a non-exhaustive list of gaps and uneven transposition in the legislative framework of EU members (European Court Of Auditors 2019, Table 1, p. 34).

The process of shaping the cybersecurity of the EU continues. On 16 December 2020, the EU presented three proposals, the EU's Cybersecurity Strategy for the Digital Decade, the Directive on measures for a high common level of cybersecurity across the Union, called NIS2 Directive (European Commission 2020a), and the Directive on Critical Entities Resilience (CER) (European Commission 2020b).

On 10 June 2021, the European Parliament (EP) adopted a resolution on the EU's Cybersecurity Strategy for the Digital Decade (European Parliament 2021) to make connected products and associated services secure by design, resilient to cyber incidents, and able to be quickly patched if vulnerabilities are discovered (Pingen (2021). The Strategy aims to ensure a global and open Internet with strong safeguards. Building on the progress made under previous strategy, it makes proposals for the use of three main instruments - regulatory, investment and policy initiatives in three areas: "resilience, technological sovereignty and leadership"; "building operational capacity to prevent, deter and respond"; and "advancing a global and open cyberspace through increased cooperation" (European Commission 2020c). The strategy demonstrates the EU's strong commitment to continuously develop its defensive cyber capabilities and to intensify cooperation between its members and with third countries, regional and international organisations as well as the multi-stakeholders.

The NIS2 Directive specifies 'essential entities' and 'important entities', introduces the EU Cyber Crisis Liaison Organisation Network (CyCLONe), the CSIRTs network and the Cooperation Group, to support the management of large-scale incidents at the European Union level. The EU-CyCLONe has the additional function of coordinating the disclosure of vulnerabilities of specific entities at the EU level. The NIS 2 Directive aims to increase the level

of cybersecurity in the EU as it would effectively oblige more entities and sectors to take necessary measures. The CER Directive will expand both the scope and depth of the 2008 European Critical Infrastructure directive.

The European Parliament and the Council continues to examine the NIS2 and CER Directives. Once the proposals are adopted, member states will transpose them into law. The Commission will periodically review NIS2.

Cooperation within the EU in the area of cybersecurity includes the harmonisation of the legal framework. It is planned, by 2030, to create attractive regulatory conditions to increase the potential contained in data. “The aim is to create a single European data space - a genuine single market for data, open to data from across the world - where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint” (European Commission 2020d).

The EU and NATO work closely on countering hybrid threats and enhancing resilience with a special focus on countering cyber attacks and disinformation. In 2018, NATO’s North Atlantic Council and the EU’s Political and Security Committee held the discussion on hybrid threats with a subsequent scenario-based exercises. Both NATO and the EU have been improving their capacities to detect, understand and counter malicious activities at an early stage; enhancing the resilience of critical infrastructure, societies and institutions. There are in place mechanisms allowing for NATO and the EU working together, particularly on staff level. Nevertheless, there is a scope for enhancement of the cooperation of both organisations and further building synergy in countering cyber threats (Jacuch 2020, p. 19).

The EU and NATO cooperate and/or provide fora and develop capabilities not only in cyber security. Both the EU and NATO established disaster response mechanisms. NATO provides added value in international disaster response in relation to the United Nations (UN) and EU actions. NATO with its transatlantic dimension and its military capabilities can assist when a stricken nation, its neighbours and/or other international organization(s) capacity or measures cannot cope with the potential negative consequences of a natural or man-made disaster.

Comparison of Cyber Security Strategies

A national cyber security strategy is a basic government document that reflects the interests and security principles in cyberspace and establishes a framework for future legislation, policies, standards, and other recommendations related to security and cyber-security. Any EU member county strategy must cover all aspects of cyber space to ensure a comprehensive approach to addressing the cyber challenges of tomorrow. ENISA's perspective on cyberspace needs starts with EU core values, such as democracy and human rights at the top, and, working the way down, to the basic citizens' needs. There are interdependencies between the layers (ENISA 2017, p. 4). The most widely accepted approach in the preparation of national cyber security strategies is lifecycle approach as proposed by ENISA with the aim of controlling and continuously improving the strategy and related policies as well as implementation through measures, actions, and processes (ENISA 2016, p. 13, Figure 2-1).

In 2017, Poland adopted its NCSS for 2017-2022. It defines cyber security as: "[...] the resilience of information and communication systems, at a given level of confidence, to any activity that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data, or the related services offered by or accessible via these information networks and systems" (Ministry of Digital Affairs 2017, p. 26).

In 2018, Poland adopted the National Cyber Security System Act (Kancelaria Sejmu RP 2018). Important elements of the Act have been the appointment of the Government Plenipotentiary and the Board for coordination of activities and implementation of state policy in the area of cyber security; division of responsibilities between individual CSIRs at national level and establishing supervision in the field of cyber security by appointing competent authorities and introducing financial penalties.

In 2019, in accordance with the ENISA' lifecycle approach, Poland adopted its improved NCSS for 2019-2024, which aims „to increase the level of resilience to cyber threats and to increase the level of protection of information in the public, military and private sectors and to promote knowledge and good practices enabling citizens to better protect their information" (Ministry of Digital Affairs 2019, p. 8). It also aims to develop new or translated existing norms and standards into specific recommendations in the field of cybersecurity.

The NIS Directive provides for minimum - not maximum - harmonisation (European Commission 2017b). Hence, the Polish legislator has chosen a more detailed regulation to address public administration and the telecommunications sector. The objectives of the legislator were to create a political and strategic framework for managing cyber security in Poland, the efficient operation of the most important entities in the Polish cyber security system and implementation of EU recommendations in the area of telecommunications network security. By containing a minimum level of harmonisation of 5G cyber security solutions at EU level it also implements the recommendations and standards published in the EU 5G Toolbox.

The International Telecommunication Union (ITU) observes and compares the overall commitment of its 193 Member States to cybersecurity through the ITU Global Cybersecurity Index (GCI). The GCI is a reference that measures the commitment of countries to cybersecurity at a global level. It analyses differences in the provision of cyber security focusing on law, technology, organisation, capacity development and cooperation. According to the GCI ranking the following countries are on the top of the cybersecurity list: Great Britain - the first place in the world, the United States of America - second place, France - 3rd, Lithuania 4th, Estonia - 5th. Poland is ranked at 29th (International Telecommunication Union 2018, p. 62).

The aims and objectives of the Polish NCSS and the strategies of the UK, the USA, France, Lithuania and the Republic of Estonia are as follows:

- Main aims of the Polish NCSS are increasing resilience to cyber threats and increasing the level of protection of information in the public, military and private sectors, and promoting knowledge and best practices that enable citizens to better protect their information. The objectives include the following: develop the National Cyber Security System; increase the level of resilience of public administration and private sector information systems and achieving the capacity to effectively prevent incidents; enhance national security capabilities in cyberspace; build public awareness and competence on cyber security; active role of the Republic of Poland on the international arena in the area of cyber security (Ministry of Digital Affairs 2019);
- The UK aims are to defend, deter and develop and international activities. The UK has the means to defend the UK against evolving cyber threats, to respond effectively to incidents, and to ensure UK networks, data and systems are protected and resilient. Citizens,

businesses and the public sector have the knowledge and ability to defend themselves. The UK will be a hard target for all forms of aggression in cyberspace. The UK detects, understands, investigates and disrupts hostile action, pursuing and prosecuting offenders. It has the means to take offensive action in cyberspace. It has an innovative, growing cyber security industry, underpinned by world-leading scientific research and development. It has a self-sustaining pipeline of talent providing the skills to meet its national needs across the public and private sectors. The UK cutting-edge analysis and expertise will enable the UK to meet and overcome future threats and challenges (HM Government 2016, p. 25).

- The USA objectives are to: manage cybersecurity risks to increase the security and resilience of the Nation's information and information systems; preserve US influence in the technological ecosystem and the development of cyberspace as an open engine of economic growth, innovation, and efficiency; identify, counter, disrupt, degrade, and deter behaviour in cyberspace that is destabilizing and contrary to national interests, while preserving United States overmatch in and through cyberspace; preserve the long-term openness, interoperability, security, and reliability of the Internet, which supports and is reinforced by United States interests (The White House 2018).
- France focuses on fundamental interests, defence and security of State information systems and critical infrastructures, major cybersecurity crisis; digital trust, privacy, personal data, cybermalevolence; awareness raising, initial training, continuing education; environment of digital technology businesses, industrial policy, export and internationalisation; and Europe, digital strategic autonomy, cyberspace stability (Republique Française 2015, p. 3).
- Lithuanian NCSS' main aims are to provide the opportunity to explore the potential of information and communications technology (ICT) by identifying cyber incidents timely and effectively, by preventing cyber incidents and their recurrence, and by managing the impact of cybersecurity breaches. The objectives are to strengthen cyber security of the country and the development of cyber defence capabilities; ensure prevention and investigation of criminal offences in cyber space; promote cyber security culture and development of innovation; strengthen a close cooperation between private and public sectors; enhance international cooperation and ensure the fulfilment of international

obligations in the field of cyber security (Government of the Republic of Lithuania 2018); and

- Estonian NCSS' main areas to work on are: 1) A sustainable digital society - Developing technological resilience, Ensuring cyber incident and crisis prevention, preparedness and resolution, Fostering comprehensive governance and development of a cohesive cybersecurity community; 2) Cybersecurity industry, research and development - Supporting and promoting Estonian cybersecurity R&D and research-driven industry; 3) A leading international contributor - Advancing substantial cooperation on cyber issues with strategic international partners, Promoting sustainable cybersecurity capacity building across the globe; A cyber-literate society - Raising cybersecurity awareness among citizens, state and private sector, Developing talent to meet the needs of both state and private sector (Republic of Estonia 2019, pp. 14-15).

The analysis of the above strategies indicate they have many common conceptual elements, including: actions aimed at developing and researching cyber security, protecting critical infrastructure, promoting best practices, technological development, increasing the capacity for effective incident prevention, promoting Internet freedom, adapting and extending international law in this area and highlighting the need for further legislative work in this field. It has become common knowledge of the importance of public awareness of cyber security. Hence, the governments of many countries are promoting continuous, up-to-date education in this area. There is also a tendency to train young cyber-security professionals through various programmes and training. Most countries emphasise the need for the state to cooperate with the private sector and the academic community. Other measure, like decided by Lithuania, could be to create a data transfer network which would be independent from public communication networks and suitable for using during a crisis or war.

In most of the criteria, the Polish strategy does not differ significantly from other countries and is even a pioneer in some aspects of cyber security, for example the Polish NCSS is the only one to have information on the source of funding for the activities described in the strategy.

There is a lack of information on the countries of origin of cyber attacks in most compared strategies but the US one. The US is fighting against economic cybercrime and cyberterrorism. Some countries, like the US and the UK are seeking to improve transport (air, inland, maritime) and space cyber security.

Poland - like Estonia - sees the opportunity to strengthen its cyber security as a potential benefit from membership of the allied defence and cyber structures of the EU, NATO, UN, OSCE. Poland is also promoting cooperation within the framework of the Visegrád Group and the countries of the Three Seas Initiative, also known as the Baltic, Adriatic, Black Sea (BABS) Initiative[2]. The strategies of the United Kingdom, Estonia and the United States emphasise the importance of ensuring cryptographic security. The last two strategies also highlighted the need to update the law on cybercrime.

Conclusions

In the core of the discussed national strategies is building resilience, with civil preparedness as its central pillar, into the systems and structures/organisations to prepare for, withstand, recover from and counter cyber threats. Cooperation with private stakeholders at national and international levels is necessary. It is crucial for countries to realise that their economies, global competition, and cyberspace security rely on a functioning and secure cyberspace.

To date, common definition of cyberspace and cybersecurity have not been adopted internationally; however, both of these concepts appear in important strategic documents and laws of countries and organisations. Inconsistency of concepts related to cyberspace is also a problem for Poland. It is therefore necessary to take the right legislative action to bring together the concepts and definitions contained in important legal acts.

Poland's relatively distant position in the GCI ranking proves that cyber security needs to be improved at national level in many respects. The national regulations of Poland concerning cyber security are contained in twelve legal acts. As a member of the European Union, Poland has adopted EU directives and regulations into its legal order. However, the implementation or transcription of these acts into Polish legislation proves problematic. The legal regulations concerning the cyber security of Poland require further work while maintaining care in the implementation of international acts concerning cyberspace in Polish legislation.

Cyber security is a national security issue and should be integrated into national security. The current Act of 21 November 1967 on the obligation to defend the Republic of Poland, despite

[2] Austria, Bulgaria, Croatia, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia

numerous amendments, is not tailored to contemporary needs (Kamiński 2018, p. 128). One solution would be to adopt, as in Estonia, a basic law regulating the tasks of state bodies in times of peace, crisis and war. Other recommended change would be appropriate legal provisions concerning the security of the Internet of Things, imposing an obligation on IoT manufacturers to implement appropriate security measures, e.g. the requirement for a unique password for each device (Czajkowski 2019).

In order to ensure security in cyberspace not only for the Republic of Poland, but at global level, it is necessary to develop coherent legal norms to regulate the problem of jurisdiction in cyberspace; in addition, the application of the new rules requires the creation of a body to monitor compliance with the aforementioned standards. Uniformity of law on cyberspace is very important because traditional state borders do not refer to cyberspace and therefore their legal provisions cannot regulate cyberspace exclusively, which only proves how important international cooperation in this area is. Increased cooperation between states in this area may, in future, help to integrate legal standards, improve preparedness and resilience to cyber threats and allow for the efficient prosecution of cyber criminals.

The Baltics, the Visegrád Group and Balkans countries, are particularly exposed to cyber threats. It is because of Russia's political objectives, geographical proximity, economic influence, Russian speaking minorities and/or economic migrants, and possibly cultural codes affected by Soviet dominance in these regions during the Cold War. Furthermore, other Western democracies such as Germany, France, the UK and the US are very often the target of cyber-attacks, both by Russia and China. Hence, additionally to member's cooperation at the EU and/or NATO, a regional, bilateral and/or multilateral cooperation between countries facing similar threats would allow for synergizing their efforts to counter those threats. To be prepared, protected and ready to respond to cyber threats requires cooperation and involvement of all relevant actors including partners and international bodies, key private industry players and from academia.

References

1. ATTATFA, A, RENAUD, K & DE PAOLI, S. (2020) Cyber diplomacy: a systematic literature review. In: Procedia Computer Science, vol. 176, pp. 60-69.
2. BESSELING K., DE GRAAF P. & LUIIJF E. (2013), Nineteen National Cyber Security Strategies, *International Journal of Critical Infrastructures*, vol. 9, No. 1/2.
3. BISSON D. (2020) 3 Emerging Innovations in Technology that Will Impact Cyber Security, The State of Security - News. Trends. Insights. *TRIPWIRE.COM*, 22 Jul.
4. BUŘITA, L. & HALOUZKA, K. (2019), Cyber Security Strategic Documents Analysis. In: Proceedings ICMT 2019 - 7th International Conference on Military Technologies. Brno, pp. 1-6.
5. CYBERDEFENCE24.PL (2020), Unia Europejska nakłada sankcje za cyberataki. Pierwszy raz w historii, 30 Jul.
6. CZAJKOWSKI P. (2019), Rząd Japonii rozpoczyna kampanię hakowania urządzeń IoT obywateli. *ITHARDWARE.PL*, 28 Jan.
7. ECSO DIGITAL EUROPE. (2019) NIS Implementation Tracker, Last update: 25 Mar.
8. ENISA (2016), *NCSS Good Practice Guide, Designing and Implementing National Cyber Security Strategies.* Heraklion: ENISA Publications.
9. ENISA (2017), *Overview of Cybersecurity and Related Terminology, Version 1*. Heraklion: ENISA Publications.
10. EUROPEAN COMMISSION. (2013) Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 07.02.2013, JOIN (2013) 1 final.
11. EUROPEAN COMMISSION. (2015) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Single Market Strategy for Europe. Brussels, 06.05.2015, COM (2015) 192 final.
12. EUROPEAN COMMISSION. (2016) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Strengthening Europe's Cyber Resilience System and Fostering

a Competitive and Innovative Cybersecurity Industry. Brussels, 05.07.2016, COM (2016) 410 final.

13. EUROPEAN COMMISSION. (2017a) Joint Communication to the European Parliament and the Council: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Brussels, 13.09.2017, JOIN (2017) 450 final.
14. EUROPEAN COMMISSION. (2017b) Communication from the Commission to the European Parliament and the Council: Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. Brussels, 04.10.2017, COM (2017) 476 final/2.
15. EUROPEAN COMMISSION. (2018) Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. Brussels, 12.9.2018, COM (2018) 630 final.
16. EUROPEAN COMMISSION. (2020a) Communication from the Commission to the European Parliament and the Council: Proposal for a Directive of the European Parliament and of the Council on Measures for a High Common Level of Cybersecurity Across the Union, repealing Directive (EU) 2016/1148 Brussels 16.12.2020, COM (2020) 823 final.
17. EUROPEAN COMMISSION. (2020b) Communication from the Commission to the European Parliament and the Council: Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities Brussels 16.12.2020, COM (2020) 829 final.
18. EUROPEAN COMMISSION. (2020c) Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade Brussels 16.12.2020 JOIN (2020) 18 final.
19. EUROPEAN COMMISSION. (2020d) Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European strategy for data Brussels, 19.02.2020, COM (2020) 66 final.
20. EUROPEAN COURT OF AUDITORS (2019) Briefing Paper (2019). Challenges to effective EU cybersecurity policy. Luxembourg, pp. 72.

21. EUROPEAN PARLIAMENT. (2021) European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)).
22. EUROPEAN PARLIAMENT. (2021) European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP)).
23. GOVERNMENT OF THE REPUBLIC OF LITHUANIA. (2018) National Cyber Security Strategy. Resolution No. 818, 13 Aug.
24. HM GOVERNMENT. (2016) National Cyber Security Strategy 2016-2021.
25. INTERNATIONAL TELECOMMUNICATION UNION. (2018) Global Cybersecurity Index, Geneva.
26. JACUCH A. (2020) Countering Hybrid Threats: Resilience in the EU and NATO's Strategies. *The Copernicus Journal of Political Studies*, No 2020/1, pp. 05-26.
27. KAMIŃSKI M. (2018) System cyberbezpieczeństwa Republiki Estonii. Czy warto wzorować się na estońskich rozwiązaniach prawno-organizacyjnych? In: KITLER W. et al, (eds.) *System bezpieczeństwa w cyberprzestrzeni*. Towarzystwo Wiedzy Obronnej, Warszawa, pp. 115-131.
28. KANCELARIA SEJMU RP. (2011) Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw. Dz.U. 2011 nr 222, pp. 1-2.
29. KANCELARIA SEJMU RP. (2018) Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. Dz. U. 2018 poz. 1560, pp. 1-74.
30. LAN, T. and INKSTER, N. (2020) International governance of/in cyberspace. In: TIKK E. and KERTTUNEN M. (eds.) *Routledge Handbook of International Cybersecurity* (pp. 79-93). Routledge.
31. LAUDRAIN A. P. B. (2019), France's New Offensive Cyber Doctrine, *Lawfare*, 26 Feb.
32. LIBICKI M. (2019), For a Baltic Cyberspace Alliance? In: MINÁRIK T. et. al, (eds.) *11th International Conference on Cyber Conflict: Silent Battle*, NATO CCD COE Publications, Tallinn.
33. MINISTRY OF DIGITAL AFFAIRS. (2017) National Framework of Cybersecurity Policy of the Republic of Poland for 2017-2022.

34. MINISTRY OF DIGITAL AFFAIRS. (2019) Cybersecurity Strategy of The Republic of Poland for 2019 – 2024.
35. NATO. (2016) Warsaw Summit Communiqué Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016.
36. OFFICIAL JOURNAL OF THE EUROPEAN UNION. (2013) Regulation (EU) 526/2013 of the European Parliament and of the Council of 21 May 2013 concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004.
37. OFFICIAL JOURNAL OF THE EUROPEAN UNION. (2019) 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).
38. OTTIS, R. & LORENTS, P. (2010). Cyberspace: Definition and Implications. In: *Proceedings of the 5th International Conference on Information Warfare and Security*. Dayton, 8-9 April. Reading: Academic Publishing Limited, pp 267-270.
39. PAWLAK P. (2019) The EU's role in shaping the cyber regime complex, *European Foreign Affairs Review*, Vol. 24, Issue 2, pp. 167 – 186.
40. PINGEN A. (2021) Parliament Calls for Tighter EU Cybersecurity Standards for Connected Products and Associated Services, EUCRIM 09.07.2021, <https://eucrim.eu/news/parliament-calls-for-tighter-eu-cybersecurity-standards-for-connected-products-and-associated-services/> [Accessed 9 December 2021]
41. REPUBLIQUE FRANÇAISE. (2015), French National Digital Security Strategy. 16 Oct.
42. REPUBLIC OF ESTONIA. (2019) Cybersecurity Strategy Republic of Estonia 2019-2022.
43. SENOL M. & KARACUHA E. (2020) Creating and Implementing an Effective and Deterrent National Cyber Security Strategy. *Journal of Engineering*, vol. 2020, pp. 1-19.
44. THE COUNCIL OF THE EUROPEAN UNION. (2019) Council Regulation (EU) 2019/796: Concerning Restrictive Measures Against Cyber-Attacks Threatening the Union or its Member States. Brussels, 17.05.2019.

45. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION. (2016) 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. Brussels, 19.7.2016, L 194/1.
46. THE WHITE HOUSE. (2018) National Cyber Strategy of the United States of America.
47. TOMIC D., SALJIC E., CUPIC D. (2018) Cyber-Security Policies of East European Countries. In: CARAYANNIS E. et. al, (eds) Handbook of Cyber-Development, Cyber-Democracy, and Cyber-Defense. Springer, Cham. https://www.academia.edu/36752428/Cybersecurity_Policies_of_East_European_Countries [accessed 10/12/2021].
48. US CONGRESSIONAL RESEARCH SERVICE. (2021) Defence Primer: Cyberspace Operations, Updated 1 Dec 2021. https://sgp.fas.org/crs/natsec/IF10537.pdf [accessed 10/12/2021].
49. WASILEWSKI J. (2013) Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*, No 9 (5) 201