Polish Political Science Yearbook, vol. 50(1), 2021, pp. 71–89
DOI: https://doi.org/10.15804/ppsy202112 PL ISSN 0208-7375
www.czasopisma.marszalek.com.pl/10-15804/ppsy

Marek Górka
Koszalin University of Technology (Poland)
ORCID: 0000-0002-6964-1581
e-mail: marek.gorka@tu.koszalin.pl

Cybersecurity Politics – Conceptualization of the Idea

Abstract: The cybersecurity issue discussed in the paper is seen from the perspective of political science with the indication that the subject under discussion concerns the multifaceted nature of the state's actions, which consists of political, economic, social, and cultural factors. At the same time, the work also intends to prove that cybersecurity is not only a domain of technology because it is the mentioned aspects that shape the conditions of stable development of the state and its citizens in a space dominated by cyber technology in a much more decisive way. Given the growing role of cybertechnology in almost all areas of human life, its importance also forces and inspires political science to question the shape and model of modern policy, which is significantly evolving under the influence of new technologies. On the one hand, emerging cyber threats reveal the weakness of the state and the dependence of state institutions on cybertechnologies, but on the other hand, existing cyber incidents may also motivate many governments to take action to increase the level of cybersecurity.

Keywords: *cybersecurity policy, cybersecurity, political theory, international relations*

Traditionally, technology evolves faster than humans' ability to predict its influence on political, social, or economic systems. Therefore, authorities of numerous countries and international organizations try to implement laws, regulations, and governance systems aiming at the normalization of this influence. However, the results of these efforts are often less advanced than technological progress. It is especially evident in the countries where the extension of communication is growing much faster than the capability of governments, industries, and civil societies to develop their technical and political possibilities to take advantage of technological advancements and, at the same time, to reduce threats related to cyberinfrastructure.

Since the geography of the Internet is permanently changing, there is a growing need to tighten international cooperation for creating a transnational approach to managing cybersecurity. Moreover, the increasing potential of the cyber world is a key factor not only for protecting the sensitive areas of politics, economy, and society against the emerging digital threats but also for protecting other, less technologically developed countries against cyber-attacks, often consequent to the expansive and hostile policy (Schia, 2018, pp. 821-837). Therefore, the strategies for developing cyber potential are not only aimed at extending a state's power and prominence as an active actor in managing cybersecurity on the international scale, but they are equally important for its internal policy.

In many parts of the world, the activities of states and societies are based on an unstoppable flow of digital services, and this enormous dependence raises concerns about their security. The cyber incidents of the last decade, such as Stuxnet (Baezner & Robin, 2017), WannaCRy, and NotPetya (Baezner, 2018) or the interference in the US election, give an impression that cyberattacks are gathering momentum and cause destruction to many areas of a state's activities (Baezner & Robin, 2017). As a result, cyber incidents understood as an intrusion into the routine operations of digital technologies have become a matter of great importance for national and international security strategies. It is a common phenomenon that the state bodies try to find appropriate means to counteract the new threats.

It seems that the emphasis given to the role of a "state" is quite appropriate and necessary because power and authority are inevitably linked to cybersecurity. However, it should be noted that a state plays an important role in this field, but non-state actors are getting stronger positions both at the national and international levels. The relationships between them are not only the specificity of cybersecurity but are also present in the state policy, and as such, they require more and more involvement from the authorities.

We may believe that the interaction between technologies, politics, and science shall always be considered in research on cybersecurity and cybersecurity politics. Finally, it may be said that research on politics shall evolve due to the technological possibilities, internships, and political choices (Cavelty & Wenger, 2019, pp. 5-32).

The paper is based on a review of existing analyses and opinions of researchers in cybersecurity policy. The paper's starting point is the claim that research reflections have the value of shaping and broadening public debate and thus contribute to the formulation and creation of informed policy based on scientific analysis, regardless of – sometimes – conflicting research positions. The analysis of the problem of the functioning of cybersecurity policy undertaken in the paper is so far sufficiently described in the scientific literature. However, in practice, the dynamic and increasingly frequent processes occurring in the public space with the help of cyber technology leave an insufficient analysis of the phenomena occurring. Therefore, the article attempts to systematize the existing theories of contemporary cybersecurity policy to better understand the nature of current challenges facing the state.

Cyber politics presents many challenges, including how to organize collective action against cyber-attacks and malicious activities. It is a serious problem for most countries grappling with the promise and peril of networked information technology. From a theoretical perspective, the question of how much politics there is or should be in security – and how much security in politics – allows us to link research in cybersecurity to debates in security studies.

The purpose of this paper is to establish a conceptual foundation that is coherent and integrated, allowing the generation of debate and discussion of cybersecurity policy. The issues of cyberspace are diverse and numerous. Consequently, the very concept of cybersecurity policy is multidimensional, encompassing various conflicting concepts and perspectives relating to the virtual information environment. As a result, the creation of an underlying methodology and unified theory has proven challenging.

The Complex Nature of the Relationship Between Cybertechnology and Politics

The development of digital technologies entails new governance mechanisms that are influenced by politics, and the relationships between more and more complex social and technological systems are bound to rise. Therefore, cybersecurity will become an increasingly important subject for countries throughout the world, creating the processes of digital transformation, which influence societies, economies, and political entities (Timmers, 2019a, pp. 1-20).

In the context of so-called the "fourth industrial revolution", due to the omnipresent digitalization and automation of processes that are an inseparable part of various social and political institutions or support their activities, the complexity of the social and technological systems will systematically grow. The phenomena appearing within cybersecurity will inevitably cross the borders of many fields, expanding their influence on other political activities, both at the national and international levels. These changes will trigger new needs for technological and organizational research that must be better integrated with the perspective of political sciences.

What is more, technology as a factor stimulating various applications in all aspects of our life relates cyberspace to the various fields of politics. These new technologies will be developed mainly by the global subjects that work efficiently in the highly competitive environment. As a result, the state institutions will become more dependent on technological companies and experts in cybernetics, so the relationships between the public and private bodies should tighten. However, there is great uncertainty as to the pace and scope of technological development that creates new needs for research (Timmers, 2019b, p. 636). The questions concerning analyses, assessments, and forecasts are related to the possible impact of new technologies on public life and certainly will be a source of many scientific reflections. From the political science standpoint, this is a real challenge now to understand more complex social and political issues and their impact on the models of cooperation and conflicts at the national and international level.

Technological development and its progress will be influenced and managed by politics, and at the same time, the political world will depend on technology. One of the key challenges is to indicate which of these spheres shall be dominant and determine the other elements of their environment. In this context, we should search for the best methods to manage the transformation of government agencies in the digital era, when they become more and more dependent on cyber services provided by private companies and entrepreneurs. It appears that governments are not able to protect their ownership of cyberspace without taking into account both the market and social power.

To describe a debate concerning cybersecurity, we need to indicate the key questions, such as the factors determining the state's capacity for providing cybersecurity. These presumptions have been accepted by now and may explain the challenges concerning cybersecurity and allow us to understand this process in the context of creating the state's regional and global potential. Therefore, international policymakers shall adopt these priorities for a further enhancement of the cyber issues.

In this context, it is necessary to call for developing not only the state's engineering skills and technical solutions but also for improving conditions to participate in the transnational cybersecurity governance (Brantly, 2019, pp. 275-289; Eriksson & Giacomello, 2007, pp. 6-10). Therefore, creating cyber potential, understood as an ability to govern cyber technologies, is addressed to the appropriate bodies, such as governments and industries, and those who represent civil society and ensure the development of permanent relationships between them (ENISA, 2015, p. 13).

Political analyses indicate that the democratically elected governments, due to their limited executive power, are more sensitive to social demands than the authoritarian ones (Maoz, & Russett, 1993, pp. 624-638).

In democratic systems, any harmful consequences caused by cyber activities may put significant social pressure on the government, even if cyber threats may not result in considerable material damage. It means that the authorities who want to avoid negative phenomena tend to be more compliant with the expectations and needs of their citizens. Moreover, in the market economy and in a highly competitive market, where technological innovations play a key role, democratic countries are more sensitive to the so-called "cyber-industrial complex" (Carr, 2016, pp. 43-62). In other words, economic and political interests encourage governments to increase their investments into cyberspace, partly due to the growing cyber threats and out of the fear related to pretty costly consequences of harmful cyber activities. First of all, they are under pressure to keep pace with the global expansion of the cyber-economy and cyber-society (Lawson, 2013, pp. 86–103). This kind of political approach is more frequently visible in democratic systems as their authorities take a great part in public life, and their political decisions are more influenced by groups of interests.

The transnational character of communication infrastructure becomes more and more relevant for a cybersecurity strategy outside the country. It is worth noting that cyber potential greatly contributes to enhancing cyber diplomacy on the international stage. On the one hand, it poses a real challenge, but on the other, it also helps many countries in playing an active role in global politics (Fuster & Jasmontaite, 2020, pp. 97-115).

Despite the numerous initiatives undertaken by various international actors and foreign policy centers, an essential element to understand the processes occurring in cyber politics are the factors affecting its development, which are also a key to understand the cyber abilities influencing cybersecurity of many countries (Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019).

Considering the scientific and technological findings and their impact on cyber efficiency, it is necessary to treat them as an integral element of cybersecurity politics. Furthermore, this knowledge may help achieve sustainable development, especially in regions where supporting education about cybersecurity is limited.

The Chosen Aspects of the Conceptualization of Cybersecurity

Despite the growing awareness of potential consequences related to cyber threats, there is still a limited understanding of the importance of enhancement in applying new technologies. A good illustration of this phenomenon is various interpretations referred to cybersecurity definitions and their interpretations which depend on the society involved in the issue. The extensive scientific literature offers the same differentiated approach to the analysis of the concept of cybersecurity. However, in the academic environment, there is a wide difference between the scientists who conceptualize cybersecurity from the perspective of human security (Deibert, 2013) and cyber threats in the context of national security (Rid, 2013; Singer & Friedman, 2014).

The first approach focuses on cybersecurity as a bunch of strategies, the execution of laws, and technical solutions to protect a society that uses them and public digital services in daily life. From this point of view, cybersecurity politics applies to the protection of digital rights, that is, the right to privacy and the freedom of speech on the Internet. The second approach is based on understanding the possible cyber threats and violations of national sovereignty, which may result in perceiving cybersecurity as a military issue.

Although there is an existing division of security zones into internal and external ones, it is difficult to make a clear distinction between the two in the case of cyberspace. The security and stability of networks depend on a national strategy and the transnational approach to cybersecurity governance. Cybersecurity is perceived as a matter of national security and efforts to obtain a transnational perspective on it. However, this perspective on the Internet infrastructure collides with the guarantee of digital sovereignty. The necessity of implementing such a complementary approach complies with most of the contemporary challenges that initiate other transnational debates concerning, i.e., climate changes, migration crisis, human rights, etc. (Zürn, 2018).

Despite these differences, there is a consensus as to the presumption that cybersecurity relies on obtaining resilience to cyber threats, which is possible by the implementation of a wide range of political schemes, including the national strategies for cybersecurity, the activities of computer security incident response teams (CSIRT) as well as strengthening of cyber-crime laws, promoting the public and private partnership, education and social awareness. Thus, little is known about the factors which determine the existing cybersecurity capacity of states.

Most scientists working on cybersecurity politics indicate the role of Internet Technologies in shaping international relations. Some of them have developed the concept of cyberweapons (Rid & McBurney, 2012, pp. 6-13) and military networks (Buchanan, 2016) and carried research on the impact of cyber capabilities on the dynamics of power in the international system (Kello, 2017; Valeriano, Jensen, and Maness, 2018) or studied cyber capabilities, which might be used for preventing military conflicts or other forms of intervention (Nye, 2017, pp. 44-71).

Many theories perceive the challenges in cybersecurity through a traditional approach towards security policy, which is usually linked with military initiatives. It may be seen in most definitions that there are two mutual elements in cybersecurity politics: the first refers to digital technologies used by various actors in the political, economic, and social areas; the second focuses on the ongoing and frequent conflicts, the formal and informal relationships between the state and its administration, the social and private sectors that are likely to redefine their roles, duties, legal boundaries and rules governing acceptable behaviors.

The first element is related to using various digital technologies and their relations with the broader concepts of social and economic changes (Alberts & Papp, 1997). The most important issues in cybersecurity politics, in respect of digital technologies, not only concern their features that may enable their activities or refrain them from actions but also raise the questions of who develops them, in what way and why, and who is entitled to use them, especially in an inappropriate way.

Then, there is a state's role and engagement with other actors inside and outside the country. From a theoretical point of view, there appears a question as to how much politics is in security and how much security there is in politics. At this point, a response to the above question is not as important as a reflection which encourages combining research on cybersecurity with discussions underway on the ground of the study of politics (Hagmann, Hegemann, and Neal, 2019, pp. 3-29). The important fact is that the state plays different roles in cybersecurity – from being a security guarantee, a legislator, a manager of public life to being an institution deciding about limits and restrictions for some social groups and countries (Cavelty & Egloff, 2019, pp. 37-57). Therefore, cybersecurity politics is defined in national and international relations within the limits of the state responsibility, economy, and social actors exercised through arbitration or a dispute. Moreover, this is frequently treated as both a stimulus or a consequence of competition and collaboration of many political powers involved in national and international relations.

Even if there are different definitions, "cyberpolitics" is understood as a capability to use cyberspace sources for obtaining specific (political) objectives inside and outside cyberspace

(Nye, 2010). Since cybersecurity has become increasingly important in the interaction between countries, experts and political decision-makers debate over the influence of digital technologies on the existing concept of political power (Nye, 2011).

Despite giving special importance to the digital domain, there is a broad frame of social life, and we should consider how international relations influence the use of these technologies. When we think about connections between technology and politics, we may note that world relations have a noticeable impact on the use or overuse of technologies. This fact raises questions about cooperation and conflicts, creating alliances and preserving strategic stability, proliferation, and controlling technologies, as well as about the efforts of countries aimed at an international consensus in the form of established norms and institutions (Buzan & Hansen, 2009).

The study of politics comprises cooperation and conflicts between states and their relation to the changes in the distribution of power in the international systems. Regarding the concept of cybersecurity politics, this international aspect is only one thing in the set of political interactions. Cybersecurity is not only a question of hostility and kindness, war and peace. In reality, cybersecurity issues do not concern urgent matters but more frequently refer to common conditions in public space. Like many complex political questions, cybersecurity is limited in various aspects of responsibility, demanding coordination and cooperation between different public entities and governing bodies. The same relations occur between the private sector actors and society when the assignments and government entitlements are delegated "downwards" (i.e., to the local bodies) and "upwards" (obtaining transnational character) or horizontally (concerning various public institutions) (Krahmann, 2003, pp. 5-26). In such conditions, governments do not operate in the existing frames but simply give instructions, supervise their implementation and try to find solutions for the most efficient collaboration, even without permanent monitoring. Therefore, it is a challenge for the relationship between the government and society (Salamon, 2002, pp. 600-610).

When there are threats of the cyber nature, there is a need to solve problems immediately by using practical knowledge. Consequently, we can observe the process of evolving the knowledge obtained as a result of work and efforts undertaken by the personnel of non-governmental organizations, and then this becomes an "academic specialty" (Waever, 2010, pp. 649-658).

As long as there is no mutual consent as to the definition of cybersecurity, and first of all, to the terminology describing cyder incidents, and no clear norms are regulating cyber operations between countries, it may be presumed that some forms of intervention into political processes of other subjects in cyberspace will be legitimized due to the lack of appropriate regulations. As a result, this phenomenon will grow, especially in the more powerful and technologically advanced political subjects.

There is a need for extensive research on the invisible participants in cybersecurity policies, and the results may shed light on the interactions in the political space and the phenomena influencing the institutionalization and stability of cyberspace. Accordingly, we will be able to find out whether the social and technical institutions established for cyberspace protection present the tools and practices of the public and private bodies. It would seem that scientific practice develops together with the dynamic changes in politics and technology.

Another significant challenge for the governance at the national political level is the question of tools that shall be applied to overcome the fragmentation of power. When there are more and more consolidated links between social and political institutions and the growing need for network management, the policymakers act under pressure or need to share responsibility with other actors who perform in social or business space. The integration of cyber politics involves creating a coherent whole and means difficult compromises between security and privacy and coordinating decisions. Moreover, there are numerous questions related to cooperation in management, economy, and society. The relevance of research themes within the scientific study of politics is that they describe the methods used by a modern state to create its assignments in a multidimensional environment. Cybersecurity policy is visible in authorities' decision-making processes, especially concerning the management of the technological base that influences economic, political, and military powers and the country's position on the international stage.

The Changes in Perceiving the Concept of Cybersecurity

One of the most frequently used concepts in public debate on the Internet is the general and broad term "cybersecurity" and comprises various issues that may refer to technology, society, and politics.

Due to the lack of a clear definition identifying this term, many phenomena occurring in new technologies are named with the prefix "cyber". Therefore, such terms as "cyberattack" or "cyberterrorism" are often used interchangeably, which causes numerous misconceptions as to the idea of cybersecurity. Moreover, this is a very complex term that may be used in various areas, and it is impossible to assign it to one field.

The attempts to characterize the concept of cybersecurity often mirror ongoing debate in public space on the government's direct role in this issue, the ways a private sector shall be encouraged or forced to cooperate, and the tools that may guarantee a proper level of information networks security. The individual approach of each author and conditions in the cyber environment plays an important role in defining cybersecurity (Lindstrom & Luiijf, 2012, pp. 45-47). Another important factor is permanent technological progress that contributes to the extension of this phenomenon. Thus, digital development creates new situations and relations which influence the interpretation of processes that occur within cybersecurity. This term is widely discussed in public space, and many of its elements are exposed, which results in the reflection on the further evolution of this concept.

A definition of cybersecurity is indispensable to define the functions of state authorities, especially in a practical context. However, much depends on an actor who creates a conceptual framework of this issue and highlights the specific threats included in such a definition. There are two main approaches visible in the attempts to define the phenomenon.

The first one relates to technology, software, and individual skills applied for the reduction of risk arising from online transfer and data storage, such as encryption technology, anti-virus software, and staff training (Weber, 2018, pp. 306-308; Ayala, 2016, pp. 43-48; Donaldson et al., 2016, pp. 3-4).

It should be noted that the concept of cybersecurity may not be clear enough as long as it is treated as a reaction of the government to the technical problems in security issues (Nissenbaum, 2015, pp. 61-73; CDT, 2013). The undertaken actions go far beyond the physical safety measures and outline objectives for many areas of social and political life (Walker & Melinda, 2011, pp. 143-160; Nissenbaum, 2005, pp. 61-73). One reason for extending the scope of this concept beyond technical aspects is sending illegal and harmful content that affects computer networks and systems and may have a negative impact on political and social issues.

In the second approach, the changes in military technology appear to be a traditional element used to define cybersecurity (Rid, 2012, pp. 5-32; Stone, 2013, pp. 101-108; Libicki, 2009, p. 52; Dillon, 2002, pp. 71-79). There was a growing number of international conflicts and disputes at the beginning of the 21st century that involved, almost in each case, the digital technology that used "malware" to weaken the opponent's critical infrastructure. Consequently, emphasizing the negative results of the used technology is a typical feature of most definitions of cybersecurity and security mechanisms implemented by governments to protect their countries against cyberattacks.

Since it was realized that cyberattacks go far away beyond cyberspace and affect citizens' daily lives, the question of providing protection and stability has become a political matter. Cyber threats have also become a significant problem because they may affect the country's infrastructure and the enormous costs of preventive measures. It means that the obligation to ensure protection against such threats cannot pass unnoticed or be neglected by the government, as the costs of inaction would influence the vast majority of society.

However, the authorities must find solutions to arising questions such as: how high shall be the means intended to cover the cost of cybersecurity? What preventive actions shall be taken in the face of possible threats? How to preserve proportions and the appropriate scope of the reaction to a cyberattack? These are only some of many questions that the governments must answer in their official strategic documents. Therefore, it is not possible at present to discuss cyber threats issues without considering political aspects, and finding solutions to the above dilemmas is a real challenge to each government.

It seems that when focusing solely on the military aspects, the image of cybersecurity may be restricted by other processes occurring in public space, which determine a model of governance and internal relations. Overall, this indicates that the political aspect is as important for perceiving the term as technical and military ones.

Definitions of cybersecurity created by individual actors often mirrors their interpretation of threats. It shall be indicated that a vast number of threats, which appear in cyberspace, have different objectives and nature, which blur the boundaries between already defined areas and have been thought to be the separate fields of politics. An example of this is the division of the phenomena occurring in the internal and external dimensions of a state, which loses its descriptive character in the context of the transnational character of cyberspace. Cyberspace, in the process of its growing recognition, has gradually become a subject of state regulations, i.e., by criminal law provisions or by multidimensional and multilateral surveillance of the private sector.

Cybersecurity is a concept provoking many questions about the state's role in regulating public space based on new technologies (Weber, 2017, pp. 397-423). Moreover, due to the digitalization of daily life, cybersecurity is perceived as a complex political concept that requires solutions at different levels and uses tools available to the state and the private sector, and other non-governmental organizations (Liedel, 2011, p. 57). At the same time, the problem of setting the limits of liability of the institutions participating in shaping cybersecurity policy has become a real challenge.

The digital reality, in which the hierarchical structures of management are not used any longer or must be complemented, exerts pressure to create a broader approach to the regulations that ensure the desired results in reducing and detecting cyber threats (Dupont, 2013, pp. 6-11). In addition, the decentralized nature of cyberspace has changed the existing division of liability between the government, private sector, and society. Moreover, because the management of the internet standards is a multidimensional process, many subjects of various interests and objectives are taking part in it.

Because of this, cybersecurity has become a significant challenge to the state and causes problems with defining roles for the actors involved in combating cybercrime and ensuring the safety of the cyber environment. Furthermore, the complex nature of cybersecurity may raise dilemmas as to what subjects shall be or are responsible for a given area of cyberspace and what actions shall be undertaken against the specific cyber incidents. Therefore, this question is becoming an imminent and inseparable part of contemporary politics, and cybersecurity requires the participants of political space to treat digital risk as a challenge for their further cooperation.

In the context of political analysis, an attempt to define cybersecurity raises questions about the influence of this phenomenon on the convergence of views between different states. Another challenge is establishing a commonly approved model of separation of duties concerning cyber policy regulations. For example, despite the EU's current attempts to create a uniform approach to cybersecurity, achieving a unified stance within different governing actors and bodies is a highly complex process. Moreover, the international dimension of the problem and the fact that there may be a contradiction between the interests of states contribute to the growing complexity of the stability in cyberspace development (Schmidt, 2014, pp. 169-187).

The official documents that identify the priority areas of the concept are an important support for creating a cybersecurity definition in the literature on the subject. Strategic studies emphasize the most important areas of cybersecurity noted from the perspective of the policymakers, which indicate the methods of obtaining objectives such as: achieving cyber immunity, reducing cybercrimes, enhancing cybersecurity policy and cyber capability, developing industrial and technological sources, or establishing a coherent international policy towards cyberspace. This division in cybersecurity strategies is largely consistent with the definitions found in the literature on the subject that indicate analogous areas (Nowak & Nowak, 2011, p. 103).

The perception of cybersecurity as an essential area of politics started with spreading cybertechnologies in everyday use, and then, in the next stage, has increased in importance due to the growing dependence of the national economic sectors on new technologies.

The cybersecurity process evolved from tasks focused on tackling cybercrime to more complex solutions, which comprise most of the ongoing operations and the actors participating in them. In other words, the Internet has permeated most areas of social and economic activities, and consequently, more and more countries and their citizens have become dependent on IT infrastructure (Sienkiewicz, 2004).

The correlation of sectors, both the public and private ones (i.e., banking, energy, and IT providers) and their growing dependence on IT networks, have made them more vulnerable to attacks. As a result, policymakers (Cornish, 2011) paid more attention to the importance of this phenomenon, which contributed to the gradual immersion of cybersecurity into national policy. Thus, this stage may be considered a turning point in the governments' approaches towards cybersecurity.

The growing dependence on information technologies and more advanced tools used for committing internet crimes have increased the activities of many bodies responsible for cybersecurity. Consequently, the involvement of the private sector has become an important factor in creating a cybersecurity definition (Aleksandrowicz, 2014, p. 75). Moreover, there has appeared an opinion that no government can provide a sufficient level of cybersecurity by using only its capacity and without the participation of the private sector institutions (Irion, 2013, pp. 83-116).

As a result, the governments gradually started cooperating with private bodies to combat cybercrimes (Marsden et al., 2008). Over time, this form has been thought to be more efficient than the actions based on the execution of laws. This fact has also contributed to the change in interpreting the power as well as the role of a state, which from the hierarchical perspective has developed horizontal features. In other words, the central, top-down governance and supervision over cyberspace processes have turned out to be ineffective. Thus, good practice in conducting activities demands shifting responsibility to the private sector and the bottom-up and voluntary initiatives as a part of broader cooperation. In this context, companies and non-governmental organizations have become an important element of cybersecurity policy.

At present, many societies exchange personal data by the use of digital technologies. However, data protection is the isolation of data and the rules and methods of their transmission and usage. Thus, cybersecurity is also perceived as a concept related to the actions taken up by public and private actors to ensure the security of communication and online resources (Sienkiewicz & Świeboda, 2009, p. 80).

Although data protection is important for the stable development of a state, cybersecurity is a much broader phenomenon comprising numerous questions that are not directly consequent to information technology and computer services (Nissenbaum, 2015, pp. 61-73). In the literature on the subject, we may find that the present living conditions of many people rely on applications and services based on data analysis (Cohen, 2013, pp. 1904-1933). There is a great volume of data collected, processed, and analyzed by numerous organizations to provide personalized services or to design more efficient systems in various sectors such as healthcare, public transport, and insurance. In addition, data transmission may be an advantage for some companies in the digital market. In this way, organizations may also influence a range of alternatives available to an individual. In this context, data protection takes on special relevance as it goes hand in hand with the liberal values related to an individual's right to self-determination and the choice of media information. Therefore, cybersecurity constitutes an individual's right to decide not only for themselves but also about the data they want to transmit, to whom, and why. Thus, the protection of personal data as an individual objective may compete with the collective interests of society in the areas such as public order or security.

The right to privacy as one of the basic human rights shall protect an individual against state interference. However, in the circumstances when cybertechnology enables big data storage, the private service providers, who handle the data, are especially important for cybersecurity policy as they may release unique information about their users to authorities. It turns out that protecting personal data against unauthorized access becomes a political issue and is often a matter of political debate.

Another reason indicating that cybersecurity is an important element of politics is the presence of this phenomenon in ongoing discussions about the proper choice of activities used to fight the threats. The most visible examples of this process are debates related to personal liberty and privacy in global combat against threats. In addition, the question of acceptable preventive measures and tackling harmful cyber phenomena is of significant importance for defining modern politics (Singer & Friedman, 2014, p. 12).

There are apparent differences in the implementation and execution of cybersecurity policies by different countries. They mirror political systems, geopolitical conditions, or the level of economic and social development.

Most of the available definitions of cybersecurity include mutual elements that may be useful for creating content describing this concept as a process comprising technology and activities aimed at preventing or reducing a negative influence of the incidents in cyberspace that may constitute a threat to a chosen country.

The definition adopted in this work relates cybersecurity to interactions occurring within/and with the help of cyberspace among countries, public institutions, private sector bodies, social groups, and other subjects that are of key importance to understand how cybersecurity politics evolve.

Cybersecurity from the Perspective of Political Sciences

When analyzing cybersecurity policy, including "technology" is an obvious choice as the question of cybersecurity is related to the development and use of cyberspace, which is a technological environment completely created by people. Researchers emphasize that the vision of cyberspace itself has the features of social construction (Graham, 1998, pp. 165-185). Consequently, the concept of cyberspace and its use changes frequently due to the circumstances, development, and application of technology in the existing social and political environment.

One of the basic features of political sciences and international relations studying digital technologies functioning in the political environment is "technological determinism" (Herrera, 2003, pp. 559-593). Most approaches from these sciences perceive technologies as insignificant objects or power resources that trigger social processes (Leese & Hoijtink, 2019). Noteworthy is that the intentions of these people who create technologies often get to artifacts, while policymakers influence the use of specific technologies. In other words, technologies are frequently used for issues and objectives other than they have been originally intended to.

Moreover, the incidents related to technological matters shall not be understood as causal powers that have a unidirectional impact on politics or science but are rather catalysts connected with the social and political environment (Buzan & Hansen, 2009). Thus, some incidents that happen out of the cybersphere may affect cybersecurity policy, i.e., after the 9/11 terrorist attack or when Edward Snowden revealed the highly classified information on US government activities. A cyber incident is a disastrous experience that may be a challenge for regular digital technologies. Unwanted changes in machinery cause technical changes. However, technical effects themselves are not sufficient to explain the meaning of cybersecurity in politics. Only when incidents, also these of cyber nature, are influenced by technical effects that have proper social or political values, they may be important for the security policy. It explains why only some cyber incidents may have political connotations and others may not (Matthewman, 2011). This sort of incidents reveals previously hidden social and technical features, which open new possibilities for the researchers of cybersecurity and observers to study such aspects of the phenomena that have not been noted before (Best & Walters, 2013, pp. 345-349). Incidents are also related to another fundamental question in studying cybersecurity, namely to data availability. The knowledge about cybersecurity is based mainly on the data derived from the reports on threats published by public institutions, non-governmental bodies as well as mass media. Unfortunately, they provide only partial and subjective images of threats as this type of relations and reports often are political and created under the pressure of their wealthy patrons or a part of the private sector businesses (Lindsay, 2017, pp. 493-514).

Although there is an ongoing debate about the impact of cyber capabilities on international security, relatively few studies have been searching for an answer to the question of why some countries are better prepared for cyber threats than others.

Another method of complementing a definition of cybersecurity politics may be a thesis based on a belief that the growth of cyber capabilities depends on a country's resources allotted to their development, regardless of political motives. The initiatives undertaken by states are aimed at promoting cyber capabilities and, on the one hand – they are driven by military paradigms, and on the other – by their accessibility to scientific and technological knowledge as well as innovations. Building cyberspace potential may be consequent to motivation for the containment of potential threats.

Regarding building cyber capacity, a state should own appropriate resources to attain the desired objectives within cybersecurity. This argument implies that states must have sufficient capacities and determination to act in a given field. These factors refer to the capacity of developing cyber technology, defined as access to the resources that are of key importance for explaining the difference in cyber potential between states concerning the historical inequalities in economic development, industrialization, and the creation of knowledge. Moreover, some arguments are supporting the significance of certain resources for developing cyber capacity. For example, financial resources shall be indispensable for exercising cybersecurity policies. Another factor is qualified personnel in the public institutions, human resources in science and technology, the participation rate in training and educational programmes, the level of advanced e-administration and e-banking, percentage of the ICT sector in GDP, the expenditure related to research and development, patent applications, Internet access, export and import of advanced technologies.

Summary

In the last decade, many studies have investigated cybersecurity politics as an interdisciplinary phenomenon important for analyzing political space in various aspects. As a political question, cybersecurity evolution needs to look at the possible new lines of inquiry that may determine future analyses in political sciences. Studies on cybersecurity politics evolve due to the changes in the public environment, which offer new empirical data for further investigations. New lines of inquiry also reveal these aspects of cybersecurity that previously have passed unnoticed by both the researchers and observers.

In this context, the relations between technology, science, and a state's practices are especially important and most frequently boil down to the way the public actors who participate in these areas articulate their aims, perform their tasks, how they perceive their roles and what activities they undertake in reference to cybersecurity at the national and international level. Thus, the history of cybersecurity politics is shaped by the interaction of three broad spheres: technology, politics, and science. The technological dynamics interact with the social and political ones. The social and economic processes are affected by capabilities and technological restrictions, and political preferences.

Due to the simultaneous changes in technology, politics, and science, the research carried out in political sciences and security is growing in popularity and encourages other researchers to look at this phenomenon (Deibert, 2017, pp. 531-546). To understand processes occurring in political space and accompanied by cyber technology, some researchers involved in political science see a need for applying various sets of theoretical tools for better understanding of the complex phenomena occurring both at the level of a state and the new digital technologies (Eriksson & Giacomello, 2006, pp. 221-244).

Some researchers indicate that non-governmental organizations may help shape a state's approach towards cybersecurity politics by determining standards and parameters of the acceptable behaviors on the international stage (Finnemore & Sikkink, 1998, pp. 887-917).

Another important line of the future research on cybersecurity politics and mechanisms of its development will be the field of building cyber potential between these countries that are more involved and interested in the international cooperation, in contrast to other political subjects being on the margin of global processes due to their political, economic or technological exclusion.

Researchers also indicate that some political environments tend to perceive cyber potential as a factor enforcing a state position on the international stage. It is an analogy to the efforts made to possess nuclear weapons, which may be, as some countries believe, a symbol of their international status (Buzan & Herring, 1998). Anyway, the countries that consider themselves to be important players in international politics may aim to increase their cyber capabilities because this factor corresponds to their position and power on the global scale. Therefore, it may be expected that the countries that take leading positions in economic, military, and technological development shall have larger cyber capacities.

The next challenge for political scientists is to explain how different political systems, both democratic and authoritarian, keep balanced market powers, how they affect the state access to the private sector of technologies and its export as well as the usage and mechanisms of monitoring foreign investments in the strategic technology centers.

When research on cybersecurity and security policy shall remain up-to-date and be relevant for managing a country, many other subjects and processes shall be comprised in its analyses. However, they shall not be determined and restricted to specific scientific disciplines but shall be based on the free choice of the interesting and urgent issues. Thus, the key challenge for the research on cybersecurity politics is integrating the theory of various disciplines and research traditions. In addition, researchers shall pay more attention to the integration of concepts and mechanisms concerning studies on political science and security and the field of secret service and analysis of the transformation of intelligence and their impact on the private sector existing in cybersecurity and intelligence service.

Another question is the analysis of interactions between technical, social, and political areas at the national and international levels. This approach is a key factor for understanding how cyber politics and cyber practice at both levels may facilitate or obstruct the interests and practices of these actors, who are not easily seen in formal and official conditions of the country's activeness.

Moreover, in the future, the research on cybersecurity politics shall estimate the number of people possessing important data on cyber operations performed by various actors worldwide. Another interesting issue is the level of professionalization of the tools (designed for monitoring and analyzing this kind of processes) being in the hands of both public institutions and individuals.

There are some important political and social questions connected with privacy protection and the supervision of enforcement authorities who use cyber technology to monitor society. Thus, the governments and societies will have to discuss how much of the new data shall be made available to the public and what consequences for data and privacy protection might be expected. From a scientific standpoint, investigations at the interface between computer science, mathematics, economics, sociology, and political studies demand a more interdisciplinary approach.

References:

Alberts, D.S., & Papp, D. (Eds.). (1997). *The information age: An anthology of its impacts and consequences*. National Defense University.

Aleksandrowicz, T. (2014). Świat *w sieci. Państwa – społeczeństwa – ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*. Difin.

Ayala, L. (2016). *Cybersecurity lexicon*. Apress.

Baezner, M. (2018). *Hotspot analysis: Cyber disruption and cybercrime: Democratic people's Republic of Korea*. Center for Security Studies.

Baezner, M., & Robin, P. (2017). *Cyber-conflict between the United States of America and Russia*. Center for Security Studies.

Baezner, M., & Robin, P. (2017). *Hotspot analysis: Stuxnet. Zurich.* Center for Security Studies.

Best, J., & Walters, W. (2013). Translating the sociology of translation. *International Political Sociology, 7*, 345-349.

Bourbeau, P., Balzacq, T., and Cavelty, M.D. (2015). Celebrating eclectic dynamism: Security in international relations. In P. Bourbeau (Ed.), *Security: Dialogue across disciplines* (pp. 111-136). Cambridge University Press.

Brantly, A.F. (2019). Conceptualizing cyber policy through complexity theory. *Journal of Cyber Policy, 4*(2), 275-289.

Buchanan, B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford University Press.

Buzan, B., & Hansen, L. (2009). *The evolution of international security studies*. Cambridge University Press.

Carr, M. (2016). Public–Private Partnerships in National Cyber-Security Strategies. *International Affairs, 92*(1), 43-62.

Cavelty, M.D., & Egloff, F.J. (2019). The politics of cybersecurity: Balancing different roles of the st*ate. St Antony's International Review, 15*, 37-57.

Cavelty, M.D., & Wenger, A. (2019). Cybersecurity meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5-32.

Center for Democracy and Technology. (2013). *Unpacking "cybersecurity": threats, responses, and human rights considerations.* https://cdt.org/insight/unpacking-cybersecurity-threats-responses-and-human-rights-considerations.

Cohen, J.E. (2013). What privacy is for. *Harvard Law Review, 126*, 1904-1933.

Cornish, P. (2011). *The vulnerabilities of developed states to economic cyber warfare.* http://www.chathamhouse.org/sites/default/files/0611wp_cornish.pdf.

Deibert, R.J. (2013). *Black Code: Inside the Battle for Cyberspace.* McClelland & Steward.

Dillon, M. (2002). Network society, network-centric warfare and the state of emergency. *Theory, Culture & Society, 19*(4), 71-79.

Donaldson, S.E., Siegel, S., Williams, C.K., and Aslam, A. (2016). *Enterprise cybersecurity. How to build a successful cyberdefense program against advanced threats.* Apress.

Dunn-Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age* Routledge.

Dupont, B. (2013). Cybersecurity futures: how can we regulate emergent risks? *Technol Innovation Manage Review, 3*(7), 6-11.

ENISA. (2015). *Definition of Cybersecurity. Gaps and overlaps in standardisation.* https://www.enisa.europa.eu/publications/definition-of-cybersecurity

Eriksson, J., & Giacomello, G. (2007). Introduction: Closing the gap between international relations theory and studies of digital-age security. In J. Eriksson, & G. Giacomello, (Eds.), *International Relations and Security in the Digital Age* (pp. 6-10). Routledge.

Fuster, G.G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. In M. Christen, B. Gordijn, and M. Loi (Eds.), *The International Library of Ethics, Law and Technology* (pp. 97-115). Springer.

Graham, S. (1998). The end of geography or the explosion of place? Conceptualizing space, place and information technology. *Progress in Human Geography, 22*, 165-185.

Hagmann, J., Hegemann, H., and Neal, A.W. (2019). The politicisation of security: Controversy, mobilisation. Arena Shifting. *European Review of International Studies, 5*, 3-29.

Herrera, G. (2003). Technology and international systems. *Millennium: Journal of International Studies, 32*, 559-593.

Irion, K. (2013). The governance of network and information security in the European Union: The European public–private partnership for resilience (EP3R). In S. Gaycken, J. Krueger, and B. Nickolay, (Eds.), *The secure information society* (pp. 83-116). Springer.

Kello, L. (2017). *The Virtual Weapon and International Order.* Yale University Press.

Krahmann, E. (2003). Conceptualizing security governance*, Cooperation and Conflict, 38*, 5-26.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics, 10*(1), 86-103.

Leese, M., & Hoijtink, M. (Eds.). (2019). *Technology and agency in international relations.* Routledge.

Libicki, M.C. (2009). *Cyberdeterrence and cyberwar.* RAND.

Liedel, K. (2011). *Bezpieczeństwo informacyjne państwa*. In K. Liedel (Ed.), *Transsektorowe obszary bezpieczeństwa narodowego* (p. 57). Difin.

Lindsay, J.R. (2017). Restrained by design: The political economy of cybersecurity. *Digital Policy, Regulation and Governance, 19*, 493-514.

Lindstrom, G., & Luiijf, E. (2012). *Political Aims & Policy Methods*. In A. Klimburg, (Ed.), *National cyber-security framework manual* (pp. 45-47). CCDCOE.

Maoz, Z., & Russett, B. (1993). Normative and Structural Causes of Democratic Peace, 1946-1986. *The American Political Science Review, 87*(3), 624-638.

Marsden, C., Simmons, S., and Cave, J. (2008). *Options for an effective-ness of internet self- and coregulation. Phase 1 report: Mapping existing co- and self-regulatory institutions on the Internet* http://ec.europa.eu/dgs/informationsociety/evaluation/data/pdf/studies/s200605/phase1.pdf.

Matthewman, S. (2011). *Technology and social theory*. Palgrave Macmillan.

Mueller, M. (2017). *Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace*. Polity.

Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7*(2), 61-73.

Nissenbaum, H. (2015). Where computer security meets national security. *Ethics and Information Technology, 7*(2), 61-73.

Nowak, E., & Nowak, M. (2011). *Zarys teorii bezpieczeństwa narodowego*. Difin.

Nye, J.S. (2011). *The future of Power*. PublicAffairs.

Nye, J.S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security, 41*(3), 44-71.

Nye, J.S. (2010). *Cyber Power*. Belfer Center for Science and International Affairs, Harvard Kennedy School.

Regulation (EU) No. 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/PL/TXT/?uri=CELEX%3A32019R0881

Rid, T. (2012). Cyber war will not take place. *The Journal of Strategic Studies, 35*(1), 5-32.

Rid, T., & McBurney, P. (2012). Cyber-Weapons. *The RUSI Journal, 15*(7/1), 6-13.

Rid, T. (2013). *Cyber War Will Not Take Place*. Oxford University Press.

Salamon, L.M. (2002). The tools approach and the new governance: Conclusion and implications. In L.M. Salamon (Ed.), *The tools of government: A guide to the New governance* (pp. 600-610). Oxford University Press.

Schia, N.N. (2018). The Cyber Frontier and Digital Pitfalls in the Global South. *Third World Quarterly, 39*(5), 821-837.

Schmidt, A. (2014). Open security. Contributions of networked approaches to the challenge of democratic internet security governance. In R. Radu, J-M. Chenou, and R. Weber (Eds.), *The evolution of global internet governance* (pp. 169-187). Springer.

Sienkiewicz, P. (2004). *Wizje i modele wojny informacyjnej*. AGH.

Sienkiewicz, P., & Świeboda, H. (2009). Sieci teleinformatyczne jako instrument państwa – zjawisko walki informacyjnej. In M. Madej, M. Terlikowski, (Eds.), *Bezpieczeństwo teleinformatyczne państwa* (p. 80). Polski Instytut Spraw Międzynarodowych.

Sienkiewicz, P., *Wizje i modele wojny informacyjnej*. http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf

Singer, P. W., & Friedman A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press.

Singer, P.W., & Friedman, A. (2014). *Cybersecurity and cyberwar. What everyone needs to know*. Oxford University Press.

Stone, J. (2013). Cyber war will take place. *The Journal of Strategic Studies, 36*(1), 101-108.

Timmers, P. (2019). Challenged by Digital Sovereignty. *Journal of Internet Law, 23*(6), 1-20.

Timmers, P. (2019). Ethics of AI and Cybersecurity When Sovereignty is at Stake. *Minds and Machines, 29*, 636.

Valeriano, B., Jensen, B., and Maness, R.C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Waever, O. (2020). Towards a political sociology of security studies. *Security Dialogue, 41*, 649-658.

Walker, J., & Melinda, C. (2011). Genealogies of resilience. From systems ecology to the political economy of crisis adaption. *Security Dialogue, 42*(2), 143-160.

Weber, R.H. (2018). Privacy and security in the IoT—Legal issues. In A. Moallem, (Ed.), *Human-Computer Interaction and Cybersecurity Handbook* (pp. 306-308). CRC Press.

Weber, S. (2017). Data, Development, and Growth. *Business and Politics, 19*(3), 397-423.

Zürn, M. (2018). *A Theory of Global Governance: Authority, Legitimacy, and Contestation*. Oxford University Press.