Management in Cyberspace: From Firewall to Zero Trust

WOJCIECH PIZŁO

Abstract Households, enterprises, as well as the entire sphere of public services, are undergoing intense digitization. We are learning to use information and communication tools at work to a greater extent than before and enterprises are increasingly using new technologies to improve management in many spheres. The aim of this research is to identify changes in the approach to management in cyberspace that are mediated by information technologies. This paper presents the key issues pertaining to the definition of cyberspace, defines the characteristics of cyberspace management and the framework regulating its functioning – international and national legislation. Additionally, it discusses the principles of risk management in cyberspace, including the core principles of cybersecurity, best practices of regulators, as well as the approach to security known as Zero Trust.

Keywords: • cyberspace management • zero trust • digital security • cyberspace regulations

CORRESPONDENCE ADDRESS: Wojciech Pizło, BEng, Ph.D., Dr. Habil., University Professor, Warsaw University of Life Sciences (SGGW), Institute of Management, Nowoursynowska (Street) 166, 02-787 Warszawa, Poland, e-mail: wojciech_pizlo@sggw.edu.pl, ORCID:0000-0002-5212-0990.

https://doi.org/10.4335/2022.1.13 ISBN 978-961-7124-10-1 (PDF)
Available online at http://www.lex-localis.press.

1 Introduction

Remote work has become an essential part of many areas of the economy, in particular public services such as medical care and education. The scope of computerization of societies and the global economy has expanded considerably. Consequently, the increased dependence of citizens and businesses on the provision of digital services and the related availability of technical infrastructure can be observed. Management in the sphere of cyberspace is related to property rights, IT resources, the availability of technical infrastructure as well as the capabilities of people operating in the digital space.

Due to the implementation of information and communication technologies in various spheres of life, enterprises are subject to intense changes. Research shows that in organizations with a hierarchical structure, the flow of information is limited (Jarvempaa & Tanriverdi 2003: 403-412). The universal access to IT tools results in flattening of the organizational structures and change in power dynamics (networking of power) in organizations which often gains an informal dimension. Organizations, even small and medium-sized enterprises, create networks of relationships that extend beyond national borders. For this purpose, they use modern technologies to build groups of customers, suppliers and business partners. Business networks, modern IT tools, databases, and above all, creative people constitute the basis for creating new organizational solutions and new management methods characterized by high degree of flexibility and efficiency (Snellman, 2014: 1251-1261). The emergence and dynamic development of social and market cyberspace produce changes in social relations and transform the management methods (Pizło, Parzonko, 2022: 61-79), the organizational structure of enterprises, and stimulate the creation of organizations, (not only enterprises), which are designed from the very beginning as virtual. The literature indicates that the main factors mediating new management solutions are the construction of open virtual organizations and the lack of administratively limited access to selected innovative technologies (Gassmann, 2006: 223-228). The currently used knowledge management support tools (Le-Nguyen, Dyerson, Harindranath, 2018: 1117-1133) include: document management systems (Sun, Lei, Cao, Zhong, Wei, Li, Yang, 2020), Web 2.0 (Orenga-Roglá, Chalmeta, 2019: 195-213), supporting the development of innovation (Schmidt, von der Oelsnitz, 2020: 9-21) and team work, as well as corporate portals and decision support systems.

The aim of this research is to identify changes in the approach to management in cyberspace mediated by information technologies. The paper addresses the following research questions: 1) How are the issues of cyberspace and cybersecurity perceived in the literature?; 2) What are the characteristics of cyberspace management, taking into account the zero trust approach?

The research method was desk based analysis of literature. The data sources included the selected publications from Elsevier and Researchgate databases.

2 Definition of cyberspace

The term "cyber" used in the literature usually refers to two elements, namely, the virtual reality and the interconnected electronic communication networks. In the case of virtual reality, the emphasis is put on the intangible nature of the maintained relationships; in the second approach, the concept of "cyberspace" is synonymous with the Internet. This concept is broader because it covers any network connecting information systems, including local area networks (LAN), i.e. a local computer network that connects selected areas, e.g. laboratories, offices, or entire enterprises and wide area network (WAN), which is a computer network extending beyond urban agglomerations, the country even the continent. Cyberspace is defined as "(...) a collection of interconnected computerized networks, including services, computer systems, embedded processors and controllers, as well as information in storage or transit" (Refsdal, Solhaug, & Stølen, 2015), and also as "global domain within the information environment, consisting of an interdependent network of information systems infrastructure, including the Internet, telecommunications networks, computer systems and embedded processors and controllers" (NIST, 2020). The concept of cyberspace in military terminology refers to (DOD 2021) infrastructure and systems supporting it. In this approach, cyberspace is defined as "the global domain within the information environment consisting of interdependent networks of information technology infrastructure and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers" (DOD 2021: 55). The cyberspace security is defined as "actions taken within protected cyberspace to prevent unauthorized access to, exploitation of, or damage to computers, electronic communications systems, and other information technology, including platform information technology, as well as the information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation". The concepts of cyberspace are based on several important elements, that is: 1) human perception penetrating the world of information, both posted and created on the network; 2) range of impact; 3) virtual reality.

3 Management in cyberspace

An important aspect of cyberspace realm is cyberspace management, which strives to organize the processes taking place there. Management in cyberspace is determined by the framework of international law and national regulations, as well as the capabilities to manage the organization's resources in cyberspace. The purpose of this activity is, on the one hand, to maximize the benefits of using new technologies and, at the same time, to minimize the risk of their negative effects. The activities of enterprises in business cyberspace have been carried out for several dozen years. The wide spread of new technologies has made security in the digital space one of the key sources of threats. Cybersecurity covers a wide spectrum of challenges e.g. ensuring the free use of critical infrastructure, influencing civic participation, such as elections in democratic countries, as well as preventing the loss of key data by strategically important enterprises and organizations. The threat comes not only from hostile countries, but also from competing

enterprises as well as criminal and terrorist organizations. One of the first studies on cybersecurity referred to: the design of cyberspace intrusion detection systems requiring the fusion of data from myriad heterogeneous distributed network sensors (Bass 2000: 99-105), as well as insurance covering the potential loss of important information as a result of cyber-attacks (Biener , Eling, Wirfs 2015: 131-158). In the inclusive approach, "cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from occurrences that misalign de jure from de facto property rights". (Craigen, Diakun-Thibault, Purse, 2014). The intention of the authors of this definition was to emphasize the interdisciplinary nature of the concept of cybersecurity and thus change the approach of scientists, financing agencies and the organizations themselves to the challenges related to cybersecurity. This approach shifts the focus from the technical point of view to the interdisciplinary perspective, supporting inclusiveness, as well as through the relationship with other functional areas of cyberspace and pointing to the issues of access to resources and property rights. The issue of organizations' willingness to invest in cybersecurity is thoroughly analyzed in research by Wessels, van den Brink, Verburgh, et al. (2021) which provides a typology of incentives for cybersecurity investments. Research on cybersecurity is often based on the Global Cybersecurity Index, which measures the commitment of countries to cybersecurity at a global level to raise awareness of the importance and different dimensions of the issue. It indicates that most governments have developed national cybersecurity defense strategies to combat the cybersecurity risks (Fadia, Nayfeh, Noble, 2020: 2), because an increasing group of citizens, enterprises and public institutions managing critical infrastructure is exposed to cyber attacks.

The literature points to the role of cybersecurity and the associated risks related to the economic situation of enterprises (Yang, Lau, Gan 2020: 167-183), and also emphasizes the relationship between the competitive strength of individual enterprises and the trust of various entities, including investors, in the information security management. People create communities by working, having fun and spending time together. Every time they do so, they benefit from trust. In online communication people are unable to verify who they are interacting with. Online communication adds new dimensions to trust (Marsh, Atele-Williams, Basu, Dwyer, Lewis, Miller-Bakewell, Pitt, 2020). The role of the state is to build trust and security in cyberspace. The pandemic has indicated a different approach to understanding macroeconomic principles of operation in the field of cyber security (Global Cybersecurity Index 2021). Trust is important in a society and digital economy, because the main trust-encouraging features on the Internet is transparent and reliable data, but most of all, what is emphasized in the literature, is the "need to democratize big data, and not let it be the preserve of corporate, scientific, or political elites" (Marsh, et al 2020). The essence is the responsible and ethical use of big data instead of using it for business purposes (corporate power) or political purposes, especially when it comes to lowering the rank of democracy (power of political parties) or in scientific circles (power of knowledge).

The core principle of enterprises' activities in cyberspace is the creation of an individual model of reacting to potential malicious incidents. Concern for maintaining a high level of security and minimizing cyber risk is important in the long-term perspective. It is confirmed (Ferens, 2021) that information on cyber threats is important enough to be consolidated and standardized. Cyberspace is built by individual network elements, but even when one network is secure; it is not known how it will behave in an interaction with other network elements of other entities. Relationships between several elements can lead to unpredictable instability (Helbing, 2013: 51-59).

4 Risk management in cyberspace

Risk management in the case of organizations operating in cyberspace consists of: 1) identification of goals; 2) risk determination; 3) assessment of the probability of cyber incident occurrence; 4) avoiding and mitigating the negative effects of a cyber attack; 5) continual monitoring of threats. The implementation of the indicated elements of cyber risk management depends on the IT department's ability to cooperate with other parts of the organization. It is indicated in the literature that enterprises holding the position of the head of information security or a similar position bear lower costs related to cyber attacks. In the case of some countries, having a digital security certificate opens the public procurement market for the company. This takes place in Japan and the countries of the European Union.

5 Cybersecurity in different economic systems

The literature indicates that (Biener, Eling, Wirfs 2015: 131-158) cybersecurity is a public good and the market provides an insufficient level of cybersecurity, therefore government interventions such as subsidies for technological support preventing cyber attacks or compulsory cybersecurity insurance may be considered. Governments, at least a considerable number of them, focus their efforts on preventing and cyber attacks, mitigating their effects and protecting their citizens, businesses and critical infrastructure. The main regulators, which are states and institutions of international law, have the possibility to directly increase cybersecurity through appropriate legislation, as well as, by acting indirectly to stimulate the desired behavior of both organizations and individuals in the field of cybersecurity.

In economics, two different approaches to market regulation are differentiated. The first approach is the command-and-control regulation consisting in an arbitrary determination of the rules regulating the market. The second approach involves regulation through economic incentives or automatic regulation or self-regulation developed by a given community. In the case of "motivated regulations" defined through the prism of the applied rewards and penalties, their aim is to achieve the desired results, while maintaining a certain decision-making autonomy. Giving freedom to the actors in the market does not mean that the regulator's decision is the only single factor, (even if it is one of the stronger ones), but it is always one of the many stimuli that coexist in the

structure of stimuli. Another approach to "motivated regulation" is the perception of markets through the prism of people's inclination to build social bonds, spontaneous knowledge sharing (Smith, 2013, XXXVI, 50-57), which is the foundation for creating new markets. In this case, the knowledge and skills of the community constitute the basis for spontaneously arising rules that often create a sophisticated system of using shared resources by community members (Ostrom, 2013).

An important element of building a rational framework of regulations relating to cyberspace is the use of the provisions of the Budapest Convention (Convention on Cybercrime, 2001) ratified by over 60 countries and the EU Directive 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. The Budapest Convention recommends the adoption of substantive and procedural regulations. The substantive regulations define different types of cybercrime, including copyright infringement, computer-related fraud, data and systems interference and child pornography. In turn, the procedural regulations provide the law tools to investigate cybercrime and secure electronic evidence in relation to any crime. Due to technological progress, the rules of enacting cyberspace law should be modified in order to keep up with the innovativeness of the market. The element that binds the cybersecurity system is the observation of both the development of technology and social attitudes towards potential threats.

When building national institutional structures dealing with cybersecurity, it is necessary to consider the following questions (Fadia, Nayfeh, Noble, 2020): 1) Should the agency reside within a defense and intelligence entity or within a civilian body? 2) What level in the government does the agency report to? 3) What is the scope of the agency’s control and oversight (for example, does it focus only on critical infrastructure or also on citizens and small and midsize businesses)? The questions should be treated rhetorically, as they refer to the choices that reflect the "philosophy" of internal policy, the development of cyber infrastructure and aspirations in the field of cybersecurity of an individual country.

Cyber risk is a derivative of the regulatory approach to the issue of how to ensure security and related to the behavior of network users as a result of which identity theft (loss) and disclosure of confidential, most often personal, information occurs. The probability of a threat related to interference in the managed cyberspace of the enterprise is referred to as cyber risk (Eling, Schnell, 2021). Knowledge of the market and threats in cyberspace minimizes the likelihood of its negative effects, and also contributes to easier modeling and management of this type of threat.

The simplest division of cyber risk is the indication of threats caused by independent natural factors causing mechanical damage to IT infrastructure and man-made threats (intentional and unintentional). The susceptibility of enterprises to cybercrime threats may be determined by the specific features of the organization that minimize the threat of a cyber attack. These specific features include: technology that the company has at its

disposal, processes as well as knowledge and IT skills of employees. Threats of cyber attacks result from the widespread use of IT tools both in public administration and private enterprises. The changing area of cyber threats makes it necessary to observe a wide and interdisciplinary spectrum of issues.

The research results indicate that (Naseer, Maynard, Desouza, 2021) the ability to quickly detect and effectively respond to cyber attacks is an important element of the efficient operation of any organization (Ahmad, Desouza, Maynard, Naseer, Baskerville, 2020: 939-953). The diagnosis of the threat, and in particular the response to incidents, i.e. incident detection, diagnosis of the areas of interference and its elimination, as well as restoration of the original state and elimination of the possibility of similar interference in the future, is the essence of rational counteracting cyber threats. The principal element of counteracting cyber attacks is the constant operation of an interdisciplinary team, whose task is to observe the information system, assess events and report on cybersecurity in an enterprise described as agile – capable of rapid reacting to unexpected challenges. An important factor of success (preventing interference) is the time that elapses from the detection of a cyber attack to the system recovery. The speed of this reaction is called agility and is important because the probability of a negative impact on the organization increases with time distance from the detection of the incident. The essence of counteracting cyber threats is collecting, storing and analyzing all data related to the incident.

6 Best practicies of cybermarket regulators

The McKinsey & Company report (2020) compared cyber security strategies in 11 countries that are best organized in this respect. The research has identified five components of a successful cybersecurity strategy. Firstly, it is the existence of a dedicated national cybersecurity agency (NCA), the aim of which is macroeconomic and macrosocial cybersecurity, secondly, a national critical infrastructure protection program, thirdly, a national incident response and recovery plan, fourthly, clearly defined legal regulations concerning cybercrime, and lastly, ensuring an efficient cybersecurity ecosystem. The recommendations of the report, summarizing good practices of best-in-class countries, include: 1) the need to establish a national cybersecurity agency responsible for defining and driving the cybersecurity agenda of the entire country; 2) the need to develop a cohesive national cybersecurity strategy to protect the critical infrastructure of the country; 3) define a wide range of actions in response to cyber incidents, including in particular the definition of cybersecurity standards; 4) improving the cyber awareness of citizens; 5) developing the cybersecurity capabilities of professionals.

A priority recommendation for public authorities is to eliminate the risk of a cyber attack on the national critical infrastructure which may lead to disruptions in other sectors of public life. Critical infrastructure is an attractive target for both hostile state actors and hostile organizations seeking publicity. Effective cyber attacks have a negative impact on

the economy, society and business confidence, and undermine national defense capabilities. The best cybersecurity programs targeting critical infrastructure focus on selecting critical sectors and assets to be specially protected. The choice of critical areas depends on the way in which the rulers define the role of individual sectors of the economy, well-being of the society, and national security of the country. The experience of countries with the best system of counteracting cyber attacks indicates the need to respond to incidents even when their losses are relatively small and recovery activities are ongoing (Fadia, Nayfeh, Noble, 2020: 2). The essence of counteracting is not only to prevent negative events, but if they occur, learn about their mechanism and mitigate their negative effects.

The McKinsey report (Fadia, Nayfeh, Noble, 2020: 2) defines actions needed to counteract cyber attacks, i.e. procedures for reporting observed incidents (cyber attacks) by citizens and enterprises. The best results were achieved in those countries where it was clearly defined to whom cyber incidents could be reported by institutions, citizens and enterprises. It was recommended (Fadia, Nayfeh, Noble, 2020: 2) to build a centralized repository where all data on cyber threats and cyber attacks will be collected. In addition to passively recording all reported cybercrimes, central institutions must actively monitor the Internet for cyber threats. The traditional national security intelligence to monitor threats should be combined with other channels like a platform collecting confidential information from the private sector (Great Britain - Cyber Security Information Sharing Partnership). This platform allows for quick and confidential sharing of information about threats. An important element of active protection against cyber attacks is automated manner of counteracting cyber threats (National Cyber Security Centre in Great Britain). When malicious content is detected on a website, the system blocks this content nationwide and works with the hosting company to remove it. Each cyber incident should be classified based on its level of threat in relation to e.g. critical infrastructure, national security or other socially and economically important criteria, as well as the type of victim and the expected interdependence of cyber threats, because a cyber attack on a "small" entity may be a preparation to attack an important public institution. The introduction of standardization of incidents organizes risk management in public cyberspace, allowing for a rational and orderly minimization of the risk of a cyber attack. Determining the threat level together with the "severity assessment matrix" is part of a well-developed mobilization plan that enumerates public entities that should respond to cyber incidents of varied severity. A local incident, such as a break-in into a small enterprise, is the domain of the local police, supported by procedures and expert advice from a national cybersecurity agency. On the other hand, counteracting threats to critical infrastructure should be coordinated, among others, by the police, proper sector regulator, intelligence agencies, etc., where the coordinating entity is a national cybersecurity agency.

7 Zero trust security model

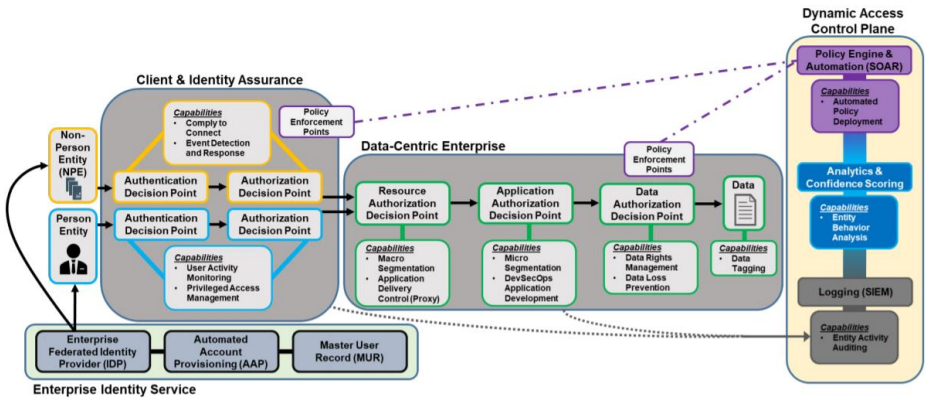
Contemporary organizations, when it comes to information systems, do not have easily identifiable borders. They rely on complex multifunctional systems supporting corporate offices, production departments, warehouses, sales and marketing departments including remotely working sales representatives, accounting and logistics. The complexity of such systems makes it difficult to protect them against cyber attacks (Department of Defense, 2021). One of the pioneers of the zero trust approach was. J. Kindervag (2010) who noticed that the dominant concept of categorizing network users into trusted and untrusted is not effective enough. The new approach, now known as zero tust, adopts the principle that no implicit trust is granted to any user or process. This approach assumes that the attacker is already present on the network. Therefore, an algorithm is used to grant access based on detailed requests. The following principles underlying the concept of zero trust (Kindervag, 2010) are indicated: 1) ensuring secure access to all resources regardless of location. This approach assumes that all network traffic is a potential threat until it is verified and secured; 2) adopting the strategy of the lowest privilege and strictly enforcing access controls. It is assumed that each user in the network must have limited – minimal, but sufficient for effective work - rights, with simultaneous strict (regulated) access to sensitive resources of the organization. Users who have access to the network are continuously monitored to determine if their activity does not deviate from the adopted security standards. The zero trust concept assumes that the network traffic is registered, verified and the response to unusual events is immediate.

The National Institute of Standards and Technology (NIST) pointed to the main factors that determine the choice of a zero-trust strategy by an organization (Rose, Borchert, Mitchell, Connelly, 2020). In the case of an enterprise, they may have a complex system serving the organization's network. The internal network may include: 1) a remote office with its own local infrastructure; 2) remote and/or mobile workers; 3) cloud services. Building security based on perimeters (firewalls) by such an organization is insufficient because after defeating the security, access to the organization's resources is unlimited (Rose, Borchert, Mitchell, Connelly, 2020).

The concept of zero trust in cybersecurity was developed at the Defense Information Systems Agency (DISA) and the US Department of Defense, where a strategy ensuring cybersecurity for enterprises referred to as "black core" was developed. Since 2004, the idea of "deperimeterization" has been promoted, which consisted in eliminating the implicit trust, which based, inter alia, on the location of the network, its static protection and static defense mechanisms in a large segment of the network (The Jericho Forum, 2007). The concept of "deperimeterization" has been changed, improved and called "zero trust". Today, the term "zero trust" is understood as a new cybersecurity paradigm that shifts defense from network-based perimeters to users, assets and resources. The zero trust strategy assumes that there is no basis for implicit trust. Trust cannot be completely based on the physical or network location, and on the ownership of assets, such as ownership of a business and its domain. Adopting a zero trust attitude in cybersecurity

requires designing a simpler and safer architecture of the company's IT system. While the classic approach to cybersecurity assumed "defense in depth", zero trust promotes a more secure, coordinated, seamless, transparent, and cost effective IT architecture. The core of zero trust is the principle of Continuous Diagnostics and Mitigation (CDM), related to external malicious interference harmful to the organization. The activities of the organization are aimed at limiting the access of persons and institutions to information resources and making them available only to authorized persons. Zero trust is a strategy that applies to the entire information architecture. The purpose of this approach is to prevent access to critical resources of the organization. The organization adopting this IT development strategy undertakes to secure, manage and monitor every device, user, application and network transaction occurring at the perimeter and/or within the network enclave (Department of Defense (DOD), 2021). In this approach, it is assumed that no entity, system, network or service operating outside or within the space used by the organization is secure. The organization and its structures must verify everything and everyone who tries to access their resources.

Figure 1: Zero trust security concept



Source: Department of Defense (DOD) Zero Trust Reference Architecture, ver. 1.0, (2021), Agency (DISA) and National Security Agency (NSA):12. https://dodcio.defense.gov (Access. 10 September 2021).

The adoption of the high-level zero trust operation concept implies the acceptance of such information architecture where non-person entity identity and user identity are tracked independently allowing for separate paths of validating confidence levels. Authentication and authorization activities are performed at defined points in the enterprise. In the enterprises where the zero trust concept is applied, the confidence level for individual devices and users is determined and the access level is adjusted to the current defined threats. Users and non-person entities have a confidence level assigned to them. In the case of an assessment that the level of threat to the organization is above the set threshold,

such an entity does not receive access to a given digital space. Both the access itself and the data are protected by the Data Loss Prevention System. Control of access to enterprise resources is related to the diagnosis of the risk level of both users and devices used by a given entity.

The zero trust architecture should include (Department of Defense, 2021): 1) Identity Provider - a system performing direct authentication 2) Automatic Account Provisioning – a system providing identity governance services such as user entitlement management, business role auditing and enforcement and account provisions and deprovisioning 3) Master User Record – a system reporting on the access of individual people and devices to the system and subsystems as well as to individual applications. In addition, MUR provides the identification of internal and external threats and the circumstances in which users are granted or denied access to the resources of the organization 4) Privileged Access Management - a system that secure, control, manage and monitor privileged access to critical assets. This includes administrative access of systems, applications and services.

Both private and public enterprises as well as numerous government agencies and non-profit organizations have embraced or are transitioning to a security strategy based on the principles of zero trust. There are several concepts regarding the zero trust approach in cybersecurity management in an organization. First, there is an assumption that there is no longer a trusted interface on our security devices; second, there is no longer a trusted network; and third, there are no longer trusted users (Kindervag, 2010: 2). In this approach, it is recommended to treat all network traffic as involving risk. At the same time, Kindervag notes that this concept does not imply that employees are untrustworthy; however, the concept of implicit trust should not be applied to network traffic and data. By not granting trust to the activities that take place in the network, we reduce the likelihood of abuse of procedures and inappropriate use of the network. The chance of detecting non-standard activities and, consequently, cybercrimes also increases.

8 Conclusions

In recent decades, management in the cyberspace sphere has been dominated by people professionally involved in building telecommunications and information systems. This environment has imposed a technology-focused perception of cyberspace, limiting it mainly to technological issues. Managerial approach to cyberspace and cybersecurity refers to the social dimension of the relationship between employees, as well as between a device and an employee. The dissemination of information technologies modifies the shape of an organization, as the flow of information has become widespread. The structures of many organizations are more flattened; power dynamics changes as it becomes more networked and often gains an informal dimension. The dynamic development of social and market cyberspace entails changes in social relations, and along with them, management methods are modified to adapt to new conditions. An important area of cyberspace is cyber management, which is a set of strategies undertaken

to effectively manage the information resources owned by organizations. The framework of management activity is determined, on the one hand, by the international law and national regulations, on the other hand, by individual capabilities of an organization to manage its digital resources.

The state plays an important role in shaping cybersecurity and market rules. In economics, and in particular in institutional economics, two basic concepts of regulating the market are recognized. The first regulatory technique is the command-and-control approach consisting in arbitrary determination of the market rules, where representatives of the political power take the floor and not the community affected by the regulation. The second approach to regulating the market is self-regulation developed by a given community. Giving the market actors the freedom to regulate it is often a simpler solution, and in most cases respected by the community. In the case of cyberspace, neither the knowledge nor capabilities of the community constitute sufficient competence to regulate the market. Therefore, it would be advisable to refer to the provisions of the Budapest Convention ratified by over 60 countries and the European Union Directive concerning measures for a high common level of security of network and information systems across the Union. In addition to legal regulations, an important area is the development of a cybersecurity strategy, involving the widest possible cooperation between specialized national cybersecurity agencies. Good practices of best-in-class countries show that it is necessary to establish a national cybersecurity agency, to develop strategies needed to reduce cyber threats, to define actions to be taken in response to cyber incidents, to improve citizens' cybersecurity awareness and to enhance the competences of cybersecurity professionals. An important recommendation that can be taken into account both in macro terms and for individual organizations is the implementation of zero trust strategy. It is based on the assumption that no user or network can be implicitly trusted and must always be verified. Zero trust concept represents a new cybersecurity paradigm that shifts defense from web-based perimeters to users (both non-person and person entities).

References:

Ahmad, A., Desouza, K. C., Maynard, S. B., Naseer, H. & Baskerville, R. L. (2020) How integration of cyber security management and incident response enables organizational learning, *Journal of the Association for Information Science and Technology*, 71, pp. 939-953, https://doi.org/10.1002/asi.24311.

Bass T. (2000) Intrusion detection systems and multisensor data fusion: Creating cyberspace situational awareness, *Communications of the ACM*, 43, pp. 99-105.

Biener C., Eling M., & Wirfs J.H. (2015) Insurability of cyber risk: An empirical analysis, *The Geneva Papers on Risk and Insurance-Issues and Practice*, 40, pp. 131-158.

Convention on Cybercrime (Budapest, November 23, 2001), available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention#{%22105166412%22:[0]} (August 18, 2021).

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014) Defining cybersecurity, *Technology Innovation Management Review*, 4, pp. 13-21, https://doi.org/10.22215/timreview835.

Creazza, A., Colicchia, C., Spiezia, S. & Dallari S. (2021) Who cares? Supply chain managers' perceptions regarding cyber supply chain risk management in the digital transformation era, *Supply Chain Management*, Vol. ahead-of-print (No. ahead-of-print), https://doi.org/10.1108/SCM-02-2020-0073.

Department of Defense (DOD) Zero Trust Reference Architecture, ver. 1.0 (2021) Agency (DISA) and National Security Agency (NSA), available at: https://dodcio.defense.gov (August 18, 2021).

DOD Dictionary of Military and Associated Terms. As of January 2021, available at: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (August 18, 2021).

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, available at: http://data.europa.eu/eli/dir/2016/1148/oj (August 18, 2021).

Eling, M. & Schnell, W. (2016) Ten Key Questions on Cyber Risk and Cyber Risk Insurance, In: Sommerrock, F. (ed.) *Ten Key Questions on Cyber Risk and Cyber Risk Insurance* (The Geneva Association – International Association for the Study of Insurance Economics' Zurich), pp. 8-37, available at: https://www.genevaassociation.org (August 18, 2021).

Fadia, A., Nayfeh, M. & Noble, J., (2020) *Public and Social Sector Practice, Follow the leaders: How governments can combat intensifying cybersecurity risks, It is undoubtedly challenging to craft and execute a national cybersecurity strategy. Our research reveals common elements of successful strategies* (McKinsey & Company), p. 5, available at: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/follow-the-leaders-how-governments-can-combat-intensifying-cybersecurity-risks (August 18, 2021).

Ferens, A. (2021) Cybersecurity and cyber risk in integrated and management reports of key service operators, *Theoretical Journal of Accounting*, 45(2), https://doi.org/10.5604/01.3001.0014.9558.

Gassmann, O. (2006) Opening up the innovation process: towards an agenda, *R &D Management*, 36(3), pp. 223-228.

Global Cybersecurity Index 2020 (2021) *Measuring commitment to cybersecurity* (Geneva: International Telecommunication Union), available at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (August 18, 2021).

Helbing, D. (2013) Globally networked risks and how to respond, *Nature*, 497, pp. 51-59, available at: http://www.marsh-stresstest.eu (August 18, 2021).

Sun, J., Lei, K., Cao, L., Zhong, B., Wei, Y., Li, J. & Yang, Z. (2020) Text visualization for construction document information management, *Automation in Construction*, 111, https://doi.org/10.1016/j.autcon.2019.103048.

Jarvempaa, S.L & Tanriverdi, H. (2003) Leading virtual Knowledge Networks, *Organizational Dynamics*, 31, pp. 403-412, http://dx.doi.org/10.1016/S0090-2616(02)00127-4.

Kavanagh, K., Bussa, T. & Collins, J. (2021) *Magic Quadrant for Security Information and Event Management*, (Gartner Technical Report), available at: https://www.gartner.com/doc/reprints?id=1-26OLSQ2N&ct=210630&st=sb (August 18, 2021).

Kindervag, J. (2010) *Build Security Into Your Network's DNA: The Zero Trust Network Architecture* (John Kindervag for Security & Risk Professionals), pp. 1-25, available at: https://www.virtualstarmedia.com/downloads/Forrester_zero_trust_DNA.pdf (August 18, 2021).

Le-Nguyen, K., Dyerson, R. & Harindranath, G. (2018) Exploring knowledge management software implementation from a knowing-in-practice perspective, *Inf Syst Front*, 20, pp. 1117-1133, https://doi.org/10.1007/s10796-016-9713-3.

Marsh, S., Atele-Williams, T., Basu A., Dwyer, N., Lewis, P.R., Miller-Bakewell, H. & Pitt, J. (2020) Thinking about Trust: People, Process, and Place, *Patterns*, https://doi.org/10.1016/j.patter.2020.100039.

Naseer, H., Maynard, S.B. & Desouza, K.C. (2021) Demystifying analytical information processing capability: The case of cybersecurity incident response, *Decision Support Systems*, 143, https://doi.org/10.1016/j.dss.2020.113476.

NIST (2020) Security and Privacy Controls for Information Systems and Organizations, *NIST Special Publication 800-53*, Revision 5, (National Institute of Standards and Technology), https://doi.org/10.6028/NIST.SP.800-53r5.

Orenga-Roglá, S. & Chalmeta, R. (2019) Methodology for the Implementation of Knowledge Management Systems 2.0, *Bus Inf Syst Eng*, 61, pp. 195-213, https://doi.org/10.1007/s12599-017-0513-1.

Ostrom, E. (2013) *Dysponowanie wspólnymi zasobami* (Warszawa: Wolters Kluwer).

Chamoso, P., Rodriguez, S., de la Prieta, F. & Bajo, J. (2018) Classification of retinal vessels using a collaborative agent-based architecture, *AI Communications*, 31, pp. 427-444.

Pizło W. & Parzonko A. (2022) Virtual organization and trust, In: Paliszkiewicz, J. & Chen (eds.) *Trust, Organization and Digital Economy* (London: Taylor and Francis), pp. 61-79.

Rashid, Z., Noor, U. & Altmann, J. (2021) Economic model for evaluating the value creation through information sharing within the cybersecurity information sharing ecosystem, *Future Generation Computer Systems*, 124, pp. 436-466.

Refsdal, A., Solhaug, B. & Stølen, K. (2015) *Cyber-Risk Management* (Cham: Springer International Publishing).

Rose, S., Borchert, O., Mitchell, S. & Connelly, S. (2020) Zero Trust Architecture, *NIST Special Publication 800-207* (National Institute of Standards and Technology), https://doi.org/10.6028/NIST.SP.800-207, available at: https://www.nist.gov (August 19, 2021).

Schmidt, S. & von der Oelsnitz, D. (2020) Innovative business development: identifying and supporting future radical innovators, *Leadersh Educ Personal Interdiscip*, 2, pp. 9-21, https://doi.org/10.1365/s42681-020-00008-z.

Smith, V.L. (2013) *Racjonalność w ekonomii* (Warszawa: Wolters Kluwer).

Snellman, L. C. (2014) Virtual teams: Opportunities and challenges for e-leaders, *Procedia – Social and Behavioral Sciences*, 110, pp. 1251-1261.

The Jericho Forum (2007) *Jericho Forum Commandments*, version 1.2., available at: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf (August 19, 2021).

Wessels, M., van den Brink, P., Verburgh, T., Cadet, B. & van Ruijven, T. (2021) Understanding incentives for cybersecurity investments: Development and application of a typology, *Digital Business*, 1(2), pp. 1-7, https://doi.org/10.1016/j.digbus.2021.100014.

Yang, L., Lau, L. & Gan H. (2020) Investors' perceptions of the cybersecurity risk management reporting framework, *International Journal of Accounting & Information Management*, 28(1), pp. 167-183.