Nowa Polityka Wschodnia 2022, nr 4 (35) ISSN 2084-3291

DOI: 10.15804/npw20223503 s. 51–71

www.czasopisma.marszalek.com.pl/pl/10-15804/npw

Marek Górka

Koszalin University of Technology
ORCID ID: https://orcid.org/0000-0002-6964-1581

Cybersecurity culture in the public and private sector area in the Central European region

Cybersecurity culture in the public and private sector area in the Central European region

Abstract

Cyber security is a growing problem associated with everything a citizen or organisation does in cyberspace. The problem thus outlined fits into a multifaceted programme that can be addressed through cyber security management. The analysis in the article compares the level of cyber security awareness among the staff of public institutions and the private sector in four Central European countries, namely Poland, the Czech Republic, Slovakia and Hungary. Public institutions are by nature open, decentralised and rich in a wide range of data about the state, society, economy, economics and research and innovation. For this reason, they are often exposed to serious cyber threats. This study examines the relationship between cyber security culture and the urgent need for preventive action against possible cyber threats.

The main thesis of the study is that an adequate understanding of cyber security culture and improved awareness among employees about digital threats is key to achieving cyber security growth. The research illustrates breaches in so-called digital hygiene, which are caused by a lack of knowledge, skills and errors in employee behaviour. Following a survey of staff employed in both public and private organisations, an identification of key cyber security risk factors is made. Increasing staff competencies can help improve cyber resilience.

Keywords: cyber security, cyber security culture, organisational culture, public entities, innovation, cyber security management

Культура кибербезопасности в государственном и частном секторах Центрально-Европейского региона

Аннотация

Кибербезопасность – это растущая проблема, связанная со всем, что гражданин или организация делают в киберпространстве. В таком виде эта проблема вписывается в многогранную повестку дня, которую можно решить с помощью управления кибербезопасностью. Анализ, проведенный в статье, сравнивает уровень осведомленности о кибербезопасности среди сотрудников государственных учреждений и частного сектора в четырех странах Центральной Европы - Польше, Чешской Республике, Словакии и Венгрии. Государственные учреждения по своей природе открыты, децентрализованы и богаты широким спектром данных о государстве, обществе, экономике, научных исследованиях и инновациях. По этой причине они часто подвергаются серьезным киберугрозам. В данном исследовании рассматривается взаимосвязь между культурой кибербезопасности и острой необходимостью превентивных действий против возможных киберугроз.

Основной тезис исследования заключается в том, что адекватное понимание культуры кибербезопасности и повышение осведомленности сотрудников о цифровых угрозах является ключом к достижению роста кибербезопасности. Исследование иллюстрирует нарушения так называемой цифровой гигиены, которые вызваны недостатком знаний, навыков и ошибками в поведении сотрудников. После опроса сотрудников, работающих в государственных и частных организациях, были определены основные факторы риска кибербезопасности. Повышение компетентности персонала может способствовать повышению киберустойчивости.

Ключевые слова: кибербезопасность, культура кибербезопасности, организационная культура, государственные организации, инновации, управление кибербезопасностью

1. Introduction

The Internet has undoubtedly changed the world and the way modern people live their lives. Politics, the economy, finance, the armed forces, infrastructure, health care, culture, and intelligence services are heavily dependent on cyber technology. Billions of data, secrets and industrial projects are now stored in systems that are inseparable from the Internet (McCrohan, Engel, Harvey, 2010, pp. 23–41). This means that any collection of confidential information is vulnerable to attack. The threats also force the use of training on a larger scale to make employees of public institutions aware of the dangers of operating in cyberspace (Korpela, 2015, pp. 72–77).

In today's reality, it is impossible to define security without emphasizing the importance of the new phenomenon of cybersecurity culture. The development of information technology has a huge impact on political, economic, cultural and social aspects of life. This article touches on topics concerning both the current state and the future scenario of the development of a cybersecurity culture operating at the interface between the public and private sectors.

Digital technology is often considered a critical factor in the functioning of modern organizations. In order to prevent the loss of revenue and money, as well as to protect an organization's reputation, data sets must be protected from threats. Organizations use various standards and best practices when it comes to cybersecurity. However, it often turns out that despite the numerous recommendations on cyber threats and the many inspections that have been carried out, there are still situations in which mistakes in the cyber area result in huge financial and reputational losses (Arlitsch, Edelman, 2014, pp. 46–56).

Public entities are increasingly dependent on complex, interdependent and integrated information systems. Key industries constitute the core infrastructure of the state, including telecommunications, energy, healthcare, agriculture and transportation, among others. The economy is increasingly dependent on information infrastructure, which is proving to be an essential element for the continuity of industry (Hicks, Nivin, 2000, pp. 115–127). Organized criminal groups have the opportunity to increase the effectiveness of their operations through the increase in the number and scope of cyber-attacks carried out, which are increasingly threatening IT infrastructure systems. Since a significant portion of the vulnerabilities exploited by criminals are unavoidable, implementing a program of education and training for government employees may prove to be one of the key countermeasures to protect the country's critical information infrastructure systems. In an increasingly interdependent network of information systems, the private sector as well as the administrative structures of many countries can work together to improve digital resilience by defining threats and setting tasks that can prevent digital failures that are costly in their consequences (Camillo, 2017, pp. 53–63). However, building technological capacity for security requires, first and foremost, a thorough assessment of the capabilities of institutions and their employees in terms of cybersecurity culture. So, it is critical to examine the threats and vulnerabilities that pose a potential threat to an increasingly digital public space.

Cyber threats are not only a negative phenomenon, but they can also be, under certain circumstances, an opportunity for change and certain innovations. They are therefore sometimes the impetus for changes in cybersecurity policy (Warikoo, 2014, pp. 172–178). The rise of cyber threats is forcing policymakers to take newer and more effective measures. The expansion of cyber threats can be understood by examining the phenomenon not only in a technocratic context, but also in a socio-political one. This is because cyber threats affect and strongly influence the quality of public space, and thus the way state institutions perform their tasks (Brenner, 2014, pp. 9–22). Often, the perception of cyber threats also affects the level of trust in public institutions and determines their cooperation with the private sector.

2. Methodology

The purpose of the article is to reflect on the sources of cyber threats, the nature of which is most often human behavior. The problem raised in the work generates the need to analyze the functioning of institutions responsible for security in cyberspace. Another purpose of the work is an attempt to indicate selected processes that occur between the sphere of politics and state security on the example of selected entities representing the public and private sectors of the region of Central European countries.

An important point of reference, indicating changes in the functioning of public services, is the experience of the COVID-19 pandemic, which forced people to intensify their interaction with each other in the virtual world. Thus, it is worth considering such a question, whether public entities emerge from the pandemic richer from new experiences, and whether they have the potential to strengthen the culture of cybersecurity among personnel in the public and private sectors.

As an illustration of the research conducted, the responses of staff working in the public and private sectors are captured using percentage data, so that quantitative analysis becomes possible. Presenting the results in this way makes it possible to characterize – in numerical terms – the scale of the processes taking place in terms of the attitudes of employees of the surveyed organizations regarding cybersecurity culture. The second research tool is qualitative analysis, which makes it possible to learn about the determinants of the cybersecurity culture model from the perspective of the causes and motives of personnel behavior towards possible digital threats. This, in turn, can clarify the causes of organizational problems from a social perspective.

Based on the analysis, conclusions can be made to minimize negative phenomena that may be a threat to the organizations under study and also to public policy. The study also uses a comparative method, which involves detecting differences as well as similarities between state institutions and institutions operating in the private sector area. A special opportunity to confront the data is provided by the answers given by employees representing the public and private sectors. The difference between the two groups of personnel in terms of interpreting the obligations arising from the use of cybertechnology, can show at the same time the difference in the perception of the culture of cybersecurity, which today is an important aspect of the public image of any institution.

The survey was conducted in January 2022 in public institutions as well as organizations operating in the private sector. The research site was conducted in Central European countries such as Poland, the Czech Republic, Slovakia and Hungary, and precisely focused on institutions located in cities such as Warsaw, Prague, Bratislava and Budapest. Employees from 22 public institutions and 22 employees from the private sector were surveyed. The total number of employees of the surveyed entities who responded was 459.

At this point, it should be noted that the survey results illustrating the perception of cybersecurity responsibilities by the staff of the selected institutions are not limited to this group of employees. The institutions participating in the survey collaborate with other public entities and subcontractors for specific and outsourced tasks. Therefore, the ability to maintain security in the protection of IT infrastructure and the mutual transfer of information is crucial to security policy more generally. Some of the data obtained from this survey indicates the challenges facing public institutions and the personnel employed in them. It is also important to reflect on such a question as whether the situation of the covid-19 pandemic, which has forced many institutions to make much more intensive use of digital technologies, has resulted in an increased awareness of cybersecurity.

Despite the assurance of anonymity in the survey questionnaires, the reliability of responses on the part of staff may seem problematic, especially in the case that the surveys were conducted in the workplace. This fact as well as the fear of making statements public may have distorted the survey results. Nonetheless, it is worthwhile to undertake an interpretation of the obtained results, as they will indicate a certain tendency as to the perception of cybersecurity culture, characteristic of the Central European region. In addition, the findings will also allow us to understand the obstacles that stand in the way of relations between the public and private sectors. This is particularly important, as in an increasingly digital reality, the two sectors are bound to cooperate with each other.

Also, due to the nature of the questions and the possible negative characterization of the image of the organizations participating in the survey, and for the sake of respondents' anonymity, the article does not specify the names of the institutions where the survey was conducted.

3. Culture of cybersecurity

In today's reality, it is impossible to define security culture without emphasizing the importance of the new phenomenon of cybersecurity culture. The development of information technology has a huge impact on political, economic, cultural and social aspects of life. Moreover, one can suppose that the process of socialization in the field of cybersecurity is a key condition for the smooth functioning of public institutions, whose responsibilities are heavily dependent on cyber-technology.

An important concept – already hinted at in the topic of the paper – is security culture. This term refers to how the state defines security, which actors are effective in this process and what tools it uses to combat threats.

Therefore, it can be said that it is difficult to analyze security policy without understanding the security culture, the basic element of which is the values passed down from generation to generation.

By its nature, the analysis of political processes is usually multidimensional and complex, so in order to deeply understand the logic of their existence and functioning, one also needs knowledge of the natural characteristics of the selected regions and the peoples who inhabit them. In other words, research analyses in the political or security spheres may present incomplete knowledge if cultural factors are not taken into account. This issue is particularly relevant in the context of the clash of disparate cultures and civilizations. The above observation corresponds with the assertion of Chris Barker, who emphasizes the close connection between values and the structure and functioning of societies (Barker, 2004, p. 206).

It is worth noting that security culture as well as security policy are areas that complement each other. Security culture is a kind of process of socialization and absorption of certain values, norms and principles, pertaining to security, which have been determined either by a selected collective based on, among other things, tradition, or by the pressure of the environment, which enforces the adoption of a certain attitude, behavior in the face of occurring or possible events. Enforcement of such actions is the subject of policy, which determines a specific model for managing the security sphere such as promoting selected values or controlling access to a selected body of knowledge or place. Such attitudes initiate public discussion of control policies, which necessitate the use of increasingly sophisticated procedures or tools such as biometric technology to help authenticate certain individuals. Digital identity is becoming an important research area, especially in the field of wireless communication using mobile devices.

Security culture is an immanent component of the work of institutions operating in sensitive areas of the state. The way such an entity is managed can have a key impact on, for example, the misuse and abuse of data resources in cyberspace. So, cybersecurity is not only a technology confined to the workplace, but also a concept relating to the social environment, which consists of norms, customs and rules governing the work of institutions that create a working atmosphere, building employee loyalty and satisfaction with their duties.

Theories, techniques and tools on the use of information by organizations are needed both at the level of state institutions and private sector entities. So, meeting the challenge of security culture (including information) requires cross-sector cooperation. So, data security awareness among employees of organizations operating in the private sector is of great importance in terms of the stability and sustainability of the state.

However, the security culture of many institutions is different, as it results, among other things, from the tasks that these entities perform, and in addition, in each organization the degree of security at the level of individual departments retains different specifics. An important aspect is also the requirements and pressures of the environment, which enforce specific behaviors. However, these often conflict with strongly ingrained cultural behaviors within the organization, which often leads to significant differences between institutions in interpreting threats and taking action against them. In addition, entities or personnel working together may exhibit low levels of loyalty and motivation to their duties at work. The goal, therefore, is to determine which places or stages of an organization's operations may be particularly vulnerable to failure or loss of valuable information.

Researchers such as Thomas Schlienger and Stephanie Teufel define security culture from the perspective of the importance of information as a socio-cultural element. They also point out that it is impossible to analyze the importance of knowledge today without technology-based activities (Schlienger, Teufel, 2003, pp. 46–52). Information security has become a natural aspect of the daily activities of an employee of any institution. There is a growing belief - most often resulting from the consequences of information systems failures - that security of, for example, databases should be the norm in every organization. Thus, it can be said that concern for the confidentiality of data in cyberspace is one of the elements of modern security culture.

With the advent of the Internet, it has become even more important to protect data and information from unauthorized access. This is due, among other reasons, to the fact that many people now have almost unlimited access to the data of many institutions. Therefore, it becomes crucial to put in place an effective mechanism for securing information and applications. Recent developments in information technology have led to many of its applications in various business areas. Data has become a critical source for most institutions. Effective access, sharing, mining and use of information has become an urgent need for many entities operating in a highly competitive environment. To this end, organizations are making a number of efforts to build comprehensive knowledge consisting of various data sources that are scattered in many places.

Information system security has become an important component of security culture. Data management is much broader and goes beyond the operation of systems and databases. Today, security also encompasses handling complex security, including granting access to data based on roles and functions performed by specific personnel. In addition, the area of information security culture has grown in importance with the emergence of new information systems in medical services, social security or e-commerce.

Many organizations, both public and private, are building and expanding their databases electronically. At the same time, they are making various information available to their users. An illustration of this is the situation during which a person in a managerial position in an organization has access to data on, for example, sales, while another person who is the head of a department may want to see daily sales numbers for presentation to colleagues, customers or representatives of other organizations. Such a situation poses a risk of confidential data being made public.

Managing data security has become a major challenge for both organizations and ordinary citizens. Since there is so much activity online, it is important to keep cyberspace safe from unauthorized intrusion, which obviously intensifies the need to protect information. Many institutions are using or modifying already existing methods of information transfer security. It should be noted that the challenges facing many public organizations will increase in parallel with advances in Internet technology.

The acquisition of data by state as well as private institutions increases the problem with the sense of privacy and, above all, personal freedom. This is because the person hired to do so can use various data retrieval tools, and can combine various pieces of information and, with their help, build knowledge about the selected target based on sensitive data. So nowadays, the information security culture faces a huge challenge on how to use knowledge and skills that will help solve problems in detecting cyber threats and conducting audits. But at the same time, this type of information can negatively affect the image of the institution that discloses this type of data. So, the culture of an organization within the framework of security in the broadest sense is a set of values and principles, which are also a kind of guidepost to help take action in this type of situation.

One should also not forget the role of cyberspace in everyday life. Ubiquitous social networks have become indispensable tools for connecting people who live on different continents as well as adhere to different cultural, political and religious values. At the beginning of the 21st century, Internet applications, including Facebook and Twitter, contributed to the further development of the public sphere. It can be seen that the use of information technology has helped bring about political change in many countries. Currently, one of the most politically sensitive topics is the impact of cyberspace on the functioning of the state. Social media, which are based on cybertechnology, are now an important communication tool for many people in everyday life as well as in exceptional situations, the best example being the US election campaign in 2016 (Allcott, Gentzkow, 2017, pp. 211–236). The manipulation of information, as well as the suspicion of foreign interference in internal US politics, is a serious allegation that directly undermines the legitimacy of the electoral system that resulted in Donald Trump winning the presidential election.

The goal of cybersecurity is therefore to protect the confidentiality, integrity and availability of information systems. It is worth noting that messages are handled by people who come from different backgrounds and have different political beliefs and technological expertise. Again, the culture of cybersecurity is key in determining the adoption and perception of innovations in the area of technology, among other things. Culture is also the key to understanding how, in selected state institutions, staff perceive their responsibilities. So the presence of culture – as a set of rules and norms – can have a positive impact on information security (Vroom, Solms, 2004, p. 191–198). With the development of cybertechnology, mankind has entered the information age, in which culture is becoming an increasingly important element of policy on a transnational scale, and security in the field of national culture is becoming the focus of attention of civilian authorities as well as military forces. Information systems are now considered an important and strategic part in most organizations.

Security is only one of several external state policy challenges. It is also difficult to comprehensively understand in the context of uninterrupted technological progress and the resulting evolution of threats. To date, few studies have been conducted to help understand and manage the information security culture in selected organizations. However, it is worth noting that an awareness of the importance of the value of information allows for a better understanding of the role that cybersecurity culture plays in society.

4. Research analysis

Respondents were asked to identify the specific impact of cyber technology on the way they do their jobs and the impact on the operation of the organization where they are employed.

Table 1. Staff atti tudes in the public and private sectors toward cyber security (data in percentage)

	Public sector	Private sector
Perception of a shortage of knowledge and skills related to possible cyber threats	29	34
Over-reliance on cyber technology for its tasks	37	67
Training in cyber security and information protection is inadequate (specialized language, content of meetings not quite relevant to daily duties)	39	44
New technology significantly affects the implementation and success of assigned tasks	78	89
Use of cyberspace during working hours for purposes unrelated to the duties of the position	43	21
Errors occurred as a result of performing duties at work in the area of using cyber technology	14	8
Concern for protecting customer information	53	71
The organization should provide much more training to keep up with current trends in cyberspace	46	38
Developments in cyber technology have led to increased workload for existing staff	32	77
Cyber security skills are sufficient to perform the duties of the position	64	73
Positive evaluation of cybersecurity personnel	79	83

39% of government employees and 54% of private sector personnel reported feeling a shortage of knowledge and skills related to possible cyber threats.

37% of people in budgetary units and 57% of employees in private entities indicated an over-reliance on cybertechnology for their tasks. The majority of people at 72% in state institutions were skeptical, distrustful or critical of cyber communications. Characteristically, those surveyed giving such a response are among those over 45 years of age. As for the private sector personnel surveyed, they are mostly between the ages of 25 and 40. However, in the case of responses assessing the usefulness of cyberspace as a work tool, the opinions expressed were often contradictory. This is because it turned out that cybertechnology during working hours is a great convenience for fast and efficient communication, while in free time it is a mental burden and the cause of often irregular working hours.

31% of those working in public institutions reported that the training they receive on cybersecurity and information protection is inadequate, as the personnel conducting the training are too busy with their own duties, use overly specialized language, and the content of the meetings is not quite relevant to their daily duties. Staff of private sector institutions are much more satisfied – at 56% – with the cybersecurity courses and training provided, while, according to 43% of respondents, there is a lower assessment of their usefulness in carrying out daily duties at work.

78% of civil servants admitted that the possibility of lacking skills or knowledge in new technologies would affect their ability to learn and obtain information about the environment. 68% of public employees said that their prior knowledge of using cyber technology was acquired through courses and training provided by their employer. A different response of 89% was given by employees of private entities, stating that new technology significantly affects the implementation and success of assigned tasks. However, when it comes to the second answer, it turns out that personnel coming to work in the private sector (as opposed to the state sector) are much better prepared - answers at 94% - to use new technologies.

93% of those working in government also admitted to using cyberspace during working hours for purposes unrelated to the duties of their position. The most frequently visited websites are social networking sites, auction sites and news sites. A small 7% of respondents admitted to visiting sites with erotic content. For employees of private entities, the use of sites not directly related to work duties is only 31%.

19% of public sector personnel reported that they had knowledge of human error occurring as a result of their duties at work in the area of using cyber technology. Respondents said these were mostly mechanical failures. In the case of those employed in private institutions, only 8% admitted to knowledge of ambient errors resulting from the misuse of IT equipment.

None of the respondents stated that their organization where they work has problems with cybercrime. However, the response of private sector employees is characteristic, indicating that 71% of the responses state that the focus is on protecting information regarding customers. In the case of state institutions, the result regarding concern for the security of citizens' data was 43%.

The lack of sufficient attention and concern and cybersecurity skills on the part of staff as can be seen varies. This is perhaps due to a lower degree of loyalty and attachment to the institution where respondents work. This result is also influenced by the issue of the quantity and quality of cybersecurity training. It is also worth noting that both groups, although working in institutions of a different nature, tend to disseminate information outside of working hours. It also turns out that the smaller the locality in which the surveyed institution is located, the greater the propensity of its employees to talk about tasks and responsibilities at work. Therefore, in spite of the key and fulfilling IT and technological barriers that guarantee a high degree of data security, the human aspect is also important, whether due to a lack of awareness, knowledge, motivation to work or personal character traits.

38% of employees of institutions in the private sector and only 26% of employees of state-owned entities opined that the organization should provide much more cyber training so that the staff – according to the respondents – can keep up with current trends, fashions in cyberspace. The differences in the answers given - as can be assumed - are primarily due to the fact that private entities operate in a much more competitive market than state entities, whose tasks performed are based on statutory rather than economic obligations.

29% of personnel in budget institutions and 39% of employees in the private sector say that the lack of cyber skills has had a significant impact on their organization. Respondents were asked to identify the specific impact on their organization. In the case of government offices, they emphasized the streamlining of the administration, the transparency and transparency of the institution to citizens, as well as the positive impact on the image of the office and the process of communication with citizens. These are the main factors linking the above changes to cyber technology in the responses received. On the other hand, employees in the private sector see the development of cybertechnology in easier contact with customers, greater opportunities to reach out with the proposed offer, as well as the improvement of promotional and marketing tools. With this observation, however, most personnel at this point stressed the importance of the confidentiality of the data on which individual offers are made.

32% of local government employees and 77% of professionals in private sector organizations reported that the development of cyber technology has led to an increased workload for existing staff. This is perhaps due to the fact that private institutions are looking for more and more opportunities to use technology. In other words, competitiveness somehow forces the use of innovative ways of using promotional and marketing tools or implementing improvements in communication with the public. State entities, on the other hand, are oriented much more towards performing their core tasks, in which compliance with the law overrides the processes of evolution and innovation.

88% of local government officials and 92% of employees of private entities rated the cybersecurity skills of their environment as sufficient to perform the duties of their positions.

Only 37% of budget employees and 56% of private sector personnel believe that they are forced to combine and use cybersecurity skills with their daily job duties.

An interesting situation emerged for both groups of institutions when responding to the evaluation of cybersecurity personnel. It turned out that, according to employees of state-owned entities, 79% thought it was sufficient, while in the case of private sector organizations, only 32% said that the staff responsible for cybersecurity were fulfilling their duties based on the needs of the institution's operation.

In conclusion, the surveyed employees of state institutions mostly believe that they are sufficiently fulfilling their duties related to cybersecurity.

However, on the other hand, they believe that they do not devote enough time to training in the use of new technologies. They also often perceive mistakes made in the work environment due to improper use of computing devices.

The case of employees working in state institutions shows that they are overconfident that their knowledge of cybersecurity is mostly sufficient for their daily duties at work. They are also characterized by a much greater distance from the use and adoption of new technologies relative to public functions. It is worth noting in passing a kind of paradoxical phenomenon. Well, those countries that have been most successful in adopting and exploiting the opportunities offered by information technology are also the most exposed to a number of risks that accompany this process. So, the concern for introducing innovation in the operation of critical infrastructure, should not only focus on digital technology, but also on leaving the existing analog, traditional and proven ways of managing public space.

However, as it turns out, private sector employees are much better prepared for public functions, as evidenced by the fact that they are more flexible in the face of technological change, they are also much more likely to see the evolution of cyberspace as an opportunity for growth rather than a threat, and they are much more attentive to the principles of data confidentiality for fear, one would think, of losing revenue to competitors. Increasingly, security policies are seen in the context of protecting information such as personal data, financial and banking information, citizens' data, etc. It is therefore important to emphasize the importance of data and its protection, given that it often flows freely in cyberspace between institutions or is unknowingly made public. It turns out, then, that there is much greater motivation and identification of the institution's interest with one's own professional success in the private sector employee community.

It is also worth making such a remark, that the results of the study are a kind of generalization. This is because it is important to note that the research was conducted among institutions and employees coming from agglomerations, which are the capitals of the Visegrad Group countries. This is a rather distinctive region that has felt - as one of the few - the effects of socio-political and economic transformation so painfully. For this reason, it is worth being aware that the results of research on the perception of cybersecurity by personnel of state and private institutions in other smaller localities, as well as among other European countries with greater scientific, technological and economic potential, may be significantly different.

5. Public-private partnerships

Given the perceived shortcomings in guaranteeing security in cyberspace, public institutions may have serious problems in protecting themselves. It is also worth emphasizing that security is a common goal that also carries a common responsibility. As a result of the strategic partnerships that have been taking shape between public and private sector players over the past two decades, such cooperation has never been more important than it is today. In addition to a strengthened commitment to improving cybersecurity, the literature emphasizes enhanced dialogue between all stakeholders. Thus, there must be cooperation between business and government (Etzioni, 2017, pp. 53–62).

Public-private partnerships (PPPs) are only one part - albeit a key part - of broader governance processes in cybersecurity policy. In this context, the partnership can be viewed in terms of the relationship between the state and the private sector performing contracts for public institutions or on special orders placed by the armed forces. The nature of this partnership is, as with budget outlays in the area of cybersecurity, confidential. The interview conducted with cybersecurity personnel allows us to estimate the degree of sophistication of the public sector in cybersecurity cooperation as significant for the development of technological innovation.

The information obtained shows that in the implementation of public-private partnerships in the case of Poland, the emphasis is clearly on the creation and improvement of tasks of a military nature. In contrast, the authorities in the Czech Republic and Slovakia, when implementing PPPs, try to maintain a broader view of guaranteeing security, so that cooperation with the private sector includes much more frequent programs that ensure security in a social and economic context. In Hungary, cybersecurity cooperation is done in analogous areas, but due to a lack of trust and out of concern for the loss of sensitive information on the part of both the state and private sectors, the scale of this partnership is lower by at least a third of the total number of contracts signed compared to the rest of the

Visegrad Group countries in 2017–2020 (Osei-Kyei, Chan, Dansoh, 2020, pp. 555–566).

In the literature, the concept of public-private partnerships is defined as "institutionalized relations of cooperation between public entities and private entities for the purpose of managing public space" (Bures, 2017, pp. 289–312). Today, it is impossible to maintain a stable cybersecurity system without private sector participation. Critical infrastructure within the EU is most often operated by private companies, which tend to prioritize economic issues at the expense of social issues. On the one hand, private companies tend to be very flexible in adopting security measures, but on the other hand, their profit-oriented attitude can sometimes result in costly consequences for citizens. Such actions are difficult to accept from the state's perspective when it comes to the security of its citizens. The result is a conflict of interest between critical infrastructure operators and government policy. Therefore, it is worth emphasizing that private and public entities that interact in the field of security, however, represent values that represent significant differences between their fundamental interests.

Most of the EU countries' policy documents emphasize the importance of private sector involvement and the need to increase and strengthen cooperation with state institutions to improve the information sharing process. This also provides an opportunity for deeper consultation with private sector experts. However, these forms of cooperation often remain at the rhetorical level because the discrepancies in defining common interest are too great. A case in point is the 2021 ENISA report, which revealed that public-private partnerships on V4 countries have not yielded significant results due to the existence of many disparate factors regarding, among other things, costs as to mandatory security measures and data confidentiality (Enisa, 2021).

However, cooperation with the private sector seems essential, as IT infrastructure is most often in the hands of the private sector. It is also clear that not all entities are making the necessary investments in security. Therefore, the main benefit of such cooperation is that the public sector does not have to commit its own capital resources.

Joint cybersecurity activities with private entities can contribute to a situation in which public entities gain access to a previously unimaginable range of information, and in turn, businesses will have greater insight into the state's practices in combating cybercrime. The benefit of private sector participation in security management is that it encroaches on the state's conduct of security policy. For example: it may be easier for a private ISP to block reported content than to develop a balanced assessment of the legitimacy of each such request in accordance with state and international legal standards.

Assuming that one of the main motivations of private companies is profit, it can be assumed that such entities will have a strong interest in restoring business as quickly as possible in the event of a cyberwar, otherwise they will also suffer losses. The Visegrad countries, therefore, have adopted a liberal policy model that emphasizes individual adaptability and mobilization of private sector actors. As it turns out, therefore, it is essential in a rapidly changing cyber environment in which the state is not entirely effective in formulating responses to the required security changes (Bossong, 2018, p. 240). As a result, businesses are seen as entities that are increasingly taking over the responsibilities and traditional tasks of government in political and social regulation and management of public goods. It is worth noting that private entities are simultaneously fulfilling critical infrastructure tasks and using a wide variety of technological solutions that are beneficial from their point of view. However, it is difficult to introduce uniform standards when cyber threats occur, which affect not only the area of one country, but bring consequences for many political entities. The challenge for governments, therefore, is to build a coherent cybersecurity policy that includes the private sector in addition to state institutions.

The differences between countries in PPPs are primarily due to the level of government support, the quality and number of specialized institutions and agencies, as well as the more informal norms relating to politics and history that have shaped economic structures and social values (Zagozhon, 2016, p. 51). These actors have very different levels of human resources and technical capabilities that are used to engage in cybersecurity. Among Central European countries, a characteristic phenomenon is that public entities entering into cooperation with the private sector often prove to be weaker partners (Törő, Butler, Grúber, 2014, p. 383). Examples of this include outsourcing to specialized IT companies to assess their own level of vulnerability and identify appropriate countermeasures against advanced cyber threats. This weaker position of the Central European countries is mainly due to underdeveloped cyber infrastructure, low investment in cybersecurity research and development, an insufficient number of experts, and other factors resulting from political culture, as well as historical experience still present.

As indicated earlier, the human factor plays a large role in the process of resolving cyber incidents. In order to introduce innovative measures in the area of cybersecurity policy, national governments must take into account a broad spectrum of factors determining the functioning of cybersecurity institutions, including the skills and expectations of their employees.

Within each Central European country, there is a noticeable difference in the level of remuneration of personnel employed in the private and public information technology sectors. Adopting this division, one can also see a disparity in salaries, particularly evident in private companies, where salaries are three times higher than among employees of public, state-funded institutions (Bruszt, Lundstedt, Munkacsi, 2020, pp. 1170–1191).

There is also a noticeable difference in wages between workers in EU countries, which is one of the main reasons for taking jobs in regions offering higher wages. Thus, the phenomenon of labor migration initiates negative factors, especially for the less developed countries of Central and Eastern Europe, causing a shortage in the labor market of IT experts. As a result, in the long run, all V4 countries may lose cybersecurity specialists, to be replaced by personnel responsible only for protecting critical infrastructure.

6. Conclusion

The problem of cybersecurity has been present in public discourse for many years now. In particular, it is present in the context of the operation of institutions whose quality of tasks performed directly affects the daily lives of citizens. Although cyber awareness training for employees is important, it does not provide the necessary skills to better protect against the increasing frequency of cyber attacks. Public institutions must invest in building cyber skills at all administrative levels. These activities, can be viewed as an investment that, in the event of a cyber-war, can reduce a company's financial costs and help preserve citizens' trust in institutions.

There are many challenges facing governments and private organizations around the world in keeping information systems secure. Despite this, much of the discussion on cybersecurity still focuses on the technological aspects, and little on the social issues, including motivation for the job, loyalty to the employer and supervisor, or a sense of mission and responsibility. It turns out, then, that the lack of cybersecurity skills needs more attention, as it is a problem at the intersection of security policy, sociology and pedagogy.

Shared resources and security expertise provide increased defense against the growing threat of cybercrime. It enables actors to engage in joint activities to address specific cybercrime problems and threats, and also provides an opportunity to share best practices, as well as exchange non-operational data related to cybercrime.

Public-private cooperation can be an effective defense against cyber threats. What is required, therefore, is increased investment in modern and secure information technologies to help protect public institutions and effectively utilize the knowledge and skills of cybersecurity specialists, who typically find high salaries in the private sector. There is therefore a need for more cybersecurity experts who are able to cover all industries, from financial services, manufacturing and utilities to healthcare and retail. However, in the Central European countries indicated, there is a shortage of cybersecurity experts in government, mainly due to low salaries in the public sector than in the private sector, and an education system that does not meet the needs of the labor market.

PROF. MAREK GÓRKA

Institute od Social Policy and International Relations
Faculty of Humanities
Koszalin University of Technology
Kwiatkowskiego 6e, 75–343 Koszalin
marek_gorka@wp.pl

References

Allcott, H., Gentzkow, M. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives, 31*(2), 211–236.

Arlitsch, K., Edelman, A. (2014). Staying Safe: Cyber Security for People and Organizations. *Journal of Library Administration*, *54*(1), 46–56.

Barker, Ch. (2004). *The SAGE Dictionary of Cultural Studies*. London-New York: Routledge

Bossong, R. (2018). A Typology of Cybersecurity and Public–Private Partnerships in the Context of the European Union. In: O. Bures, H. Carrapico (Eds). *Security Privatization. How Non-security-related Private Businesses Shape Security Governance* (p. 240). Springer.

Brenner, S.W. (2014). *Cyberthreats and the Decline of the Nation-State*. London-New York: Routledge.

Bruszt, L., Lundstedt, L., Munkacsi, Z. (2020). Collateral benefit: the developmental effects of EU-induced state building in Central and Eastern Europe. *Review of International Political Economy, 27*(5), 1170–1191.

Bures, O. (2017). Contributions of private businesses to the provision of security in the EU: beyond public-private partnerships. *Crime, Law and Social Change, 67*(3), 289–312.

Camillo, M. (2017). Cyber risk and the changing role of insurance. *Journal of Cyber Policy*, *2*(1), 53–63.

ENISA (2021, 26 June). *Consolidated Annual Activity Report 2020*, Retrieved from: https://www.enisa.europa.eu/publications/corporate-documents/enisa-annual-activity-report-2021.pdf.

Etzioni, A. (2017). The fusion of the private and public sectors. *Contemporary Politics*, *23*(1), 53-62.

Hicks, D.A., Nivin, S.R. (2000). Beyond Globalization: Localized Returns to IT Infrastructure Investments. *Regional Studies*, *34*(2), 115–127.

Korpela, K. (2015). Improving Cyber Security Awareness and Training Programs with Data Analytics. *Information Security Journal: A Global Perspective*, 24(1–3), 72–77.

Marszałek-Kawa, J., Plecka, D. (2019). *The Dictionary of Political Knowledge*. Toruń: Wydawnictwo Adam Marszałek.

McCrohan, K.F., Engel, K., Harvey, J.W. (2020). Influence of Awareness and Training on Cyber Security. *Journal of Internet Commerce*, *9*(1), 23–41.

Osei-Kyei, R., Chan A.P.C., Dansoh, A. (2020). Project selection index for unsolicited public–private partnership proposals. *International Journal of Construction Management*, *20*(6), 555–566.

Schlienger, T., Teufel, S. (2003). Information security culture—From analysis to change. *South African Computer Journal, 31*, 46–52.

Törő, C., Butler, E., Grúber, K. (2014). Visegrád: The Evolving Pattern of Coordination and Partnership After EU Enlargement. *Europe-Asia Studies, 66*(3), 383.

Vroom C., von Solms, R. (2004). Towards information security behavioural compliance. *Computer and Security*, *23*, 191–198.

Warikoo, A. (2014). Proposed Methodology for Cyber Criminal Profiling. *Information Security Journal: A Global Perspective*, *23*(4-6), 172–178.

Zagożdżon, B. (2016). Partnerstwo publiczno-prywatne – uwarunkowania rozwoju. *Optimum. Studia Ekonomiczne, 6*(84), 51.