M. Górka, *Combating cyber threats as an element of the Visegrad Group's cybersecurity policy*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 20(2022), z. 1, s. 121-142, DOI: https://doi.org/10.36874/RIESW.2022.1.7.

Marek Górka*

Combating cyber threats as an element of the Visegrad Group's cybersecurity policy

Zwalczanie cyberzagrożeń jako element polityki cyberbezpieczeństwa państw Grupy Wyszehradzkiej

Summary: The Visegrad Group countries are taking actions that confirm their ambitions in the framework of cyber security policy. The tasks formulated both in strategic documents and in international forums are evidence of the active role of Central European governments in the area of cyber security. Many countries are facing a rising tide of cyberattacks, which are likely to intensify over time. Any such incident has the potential to inflict significant damage, undermining trust in government and causing unpredictable political consequences. For this reason, there is an apparent desire on the part of the V4 countries to build common cyber resilience based on close cooperation with the EU and NATO. Another way of describing the actions taken in the article is budget spending on cyber security, which is an important measure for assessing the development of the cyber capabilities of individual countries. The article is an attempt to summarize the actions taken by the V4 countries in the period 2013-2021 within the framework of cyber security policy, which for the most part remains in the sphere of mere political declarations. The research analysis undertaken can serve as a starting point for further consideration of V4 cooperation especially in the context of the military aggression of the Russian Federation after 24 February 2022. This event mandates consideration of the future of cooperation between Central European countries – in the broadest sense – on security policy.

Keywords: cybersecurity policy; Central Europe, Visegrad Group, cyber threats, cyberattacks

Streszczenie: Państwa Grupy Wyszehradzkiej podejmują działania potwierdzające ich ambicje w ramach polityki cyberbezpieczeństwa. Formułowane zadania zarówno w dokumentach strategicznych, jak i na forach międzynarodowych stanowią dowód na aktywną rolę rządów Europy Środkowej

[*] Marek Górka – PhD habil., Koszalin University of Technology, Poland, ORCID: https://orcid.org/0000-0002-6964-1581, e-mail: marek_gorka@wp.pl.

w obszarze cyberbezpieczeństwa. Wiele państw stoi w obliczu rosnącej fali cyberataków, która z czasem prawdopodobnie będzie się nasilać. Każdy tego typu incydent może wyrządzić ogromne szkody, podważając zaufanie do rządu i wywołując nieprzewidywalne skutki polityczne. Z tego też powodu widoczna jest chęć budowania przez państwa V4 wspólnej cyberodporności w oparciu o ścisłą współpracę z UE i NATO. Kolejnym sposobem opisu działań podejmowanym w artykule są wydatki budżetowe na cyberbezpieczeństwo, które są ważnym miernikiem oceny rozwoju potencjału cybernetycznego poszczególnych państw. Artykuł jest próbą podsumowania działań podejmowanych przez państwa V4 w okresie 2013-2021 w ramach polityki cyberbezpieczeństwa, które w większości pozostają w sferze jedynie deklaracji politycznych. Podjęta analiza badawcza może stanowić punkt wyjścia dla dalszych rozważań na temat współpracy V4 szczególnie w kontekście militarnej agresji Federacji Rosyjskiej po 24 lutego 2022 roku. Wydarzenie to nakazuje zastanowić się nad przyszłością współpracy państw Europy Środkowej w szeroko pojętej polityce bezpieczeństwa.

Słowa kluczowe: polityka bezpieczeństwa cybernetycznego; Europa Środkowa, Grupa Wyszehradzka; cyberzagrożenia, cyberataki

Introduction

Undoubtedly, the process of digitalization can be regarded as a factor contributing to the growth of economies and the development of society around the world. However, a negative feature of this process is the huge dependence of state structures on cybertechnology. This process in turn entails an increase in cyber threats. The consequences of negative actions in cyberspace can have a direct impact on the functioning of the state and its citizens. An example of this are cyberattacks, which aim, among other things, to restrict access to state resources and thus undermine trust in public institutions[1].

The main research hypothesis in the paper is that as the level of cyber threats increases, the level of integration and cooperation of the Visegrad Group (V4) countries in cyber security policy increases. One of the objectives of this paper is to present the scale and types of digital threats that have been recorded among the V4 countries between 2013 and 2021. The increasing growth in the frequency of cyber threats is forcing many governments to undertake a number of initiatives to improve their cyber security posture. Therefore, the next objective is to seek answers to the question of how V4 countries are building

[1] B.W. Wirtz, J.C. Weyerer, *Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats*, "International Journal of Public Administration" 2017, vol. 40, no. 13, pp. 1085-1100.

and developing their independent defence capabilities in the cyber area. Thus, the initiatives taken by the V4 states that are considered to strengthen the level of cyber security are examined, which include, among others, military and civilian spending in the area of cyber security, the creation of strategic documents and the formulation of policy statements included in the V4 presidency programmes. The activities thus described can also be used to assess the degree of cyber security policy development in the Central European region. Moreover, the analysis of perceived threats by policymakers will make it possible identify common trends in the cyber security policies of the V4 countries. The choice of the period 2013-2021 stems from the introduction of the *European Union Cyber Security Strategy: an open, safe and secure cyberspace* (2013) and the *EU Cyber Security Strategy for the Digital Decade* (2020). The EU is to a large extent the determinant of the policies of member states (including V4 countries) in the area of cyber security. In the analysed period, dynamic changes took place, both in terms of the internal policies of the V4 countries, as well as events taking place outside the EU's borders that created or perpetuated phenomena of a digital nature, and thus forced EU member states to make decisions in the area of cyber security policy.

Quantitative as well as qualitative data on the participation of the V4 countries in preventive measures against possible cyber threats is an important element in the description of cyber security policy. After presenting data illustrating the growth of cyber threats, a qualitative analysis is used to identify and assess which of the countries in the examined time period were more vulnerable to cyberattacks and in which specific areas of each state's functioning. The paper then goes on to describe, using a comparative method, the changes within each country and attempts to compare these phenomena between the V4 members. Using the methods mentioned above, the paper also describes the efforts made by the V4 countries in the field of cyber defence. Quantitative and qualitative analysis of cybersecurity spending is one of the metrics used to assess which of the V4 countries is conducting more advanced efforts to raise the level of cyber defence in both military and civilian areas. As part of the comparative research on cyber security policy, an analysis of both V4 presidency and cyber security strategy documents was also conducted to search for key passages on the topic of cyber threats.

One useful source of information on this subject is the set of data that has been collected since 2006 by the Center for Strategic and International Studies (CSIS) that provides not only quantitative data but also information on the characteristics of cyber incidents, such as: targets, means and potential damages caused by harmful acts (CSIC, 2020). Another source of information on cyber threats is a set of data created by the non-governmental organization The Council on Foreign Relations (CFR). The classification of cyber incidents included in its reports focuses mainly on operations sponsored by states (CFR, 2020). Official information and reports obtained from government agencies provided additional data on this topic. The analysis was based on the reports of the government computer incident response teams in the V4 countries.

However, no matter how much effort is put into demonstrating knowledge on the reported cyberattacks and into creating a corresponding complex data set on the subject, there is a risk that some incidents may pass unnoticed. Moreover, due to their confidential nature, most such incidents may be never revealed to public. Both the attackers and their victims may have their reasons to keep such events in secret. While the attackers maintain confidence in their offensive capability, the victims may be concerned about protecting such information from leaking[2].

We should also keep in mind that cybersecurity analysis is carried out with a limited scope of information. Research on cyber threats with the use of collected data is a great challenge, especially because the data come only from publicly accessible sources. Thus, a question arises whether the noted cyber incidents are sufficient to create a characteristic profile of threats within cybersecurity policy. For obvious reasons, some cyber acts fall under the responsibility of the secret services and information on them is protected as its disclosure might affect the services' further performance.

The article is structured as follows: the first part presents the nature and types of cyberattacks that were reported between 2013 and 2021; the second part analyses budget expenditures between 2013 and

[2] G. Simons, Y. Danyk, T. Maliarchuk, *Hybrid war and cyber-attacks: creating legal and operational dilemmas*, "Global Change, Peace & Security" 2020, vol. 32, no. 3, pp. 337-342.

2020 aimed at enhancing cyber security; the third part focuses on how V4 countries have presented opportunities to combat cyber threats in V4 presidency programmes and strategic documents.

1. Cyberattacks as a political problem

Cyberattacks have become an increasingly common tool of pressure used by both states and private actors since the events of 2007 in Estonia. Cyberattacks may have an indirect impact on the opponent through harmful acts aimed at the economy or critical infrastructure. In this context, a cyber conflict may be defined as a method of using digital technologies for the destruction of the chosen areas as well as a tool for changing political relationships between actors[3].

Such an approach indicates that cyber incidents may also be an important element of political communication. It appears that cyberattacks may be interpreted as a signal manifesting political attitudes and beliefs included in the scope of international relationships and shaped by the countries of different interests. Thus, cyber operations are methods used for obtaining political, military or economic dominance against a chosen country. In such circumstances, a cyber conflict becomes a real tool of policymaking[4].

Policymakers face a challenge when deciding how to react to incidents in cyberspace. Political dilemmas arise over whether a reaction should involve physical, conventional or diplomatic tools or cybertechnologies.

As well as the question of how to retaliate, there is also the question of the nature of a political cyber incident, i.e. the motivation and context in which cyber operations are carried out. It is often the case that even successful attacks cause only interim disruptions and system administrators can repair damage quickly and safely[5]. However, in such cases, we may presume that the main objective of harmful acts is not the unfavourable consequences but primarily the testing of the cyber

[3] F. Egloff, *Cybersecurity and the Age of Privateering*, [in:] *Understanding Cyber Conflict. 14 Analogies*, G. Perkovich, A. Levite (eds.), Georgetown 2017, pp. 231-247.

[4] M.D. Cavelty, A. Wenger, *Cyber security meets security politics: Complex technology, fragmented politics, and networked science*, "Contemporary Security Policy" 2020, vol. 41, no. 1, pp. 5-32.

[5] R. Axelrod, R. Iliev, *Timing of cyber conflict*, "PNAS" 2014, vol. 111, no. 4, pp. 1298-1303.

capabilities of the enemy in relation to resolving the problems caused by a cyberattack. The selection and usage of retaliatory measures depend on who has perpetrated the attack, whether it has been a politically motivated individual, a state or a group of people ordered and/or controlled by a state[6].

A state which is the target of an attack should not remain indifferent to this form of aggression as it might be viewed as a weakness, especially by its own citizens. On the other hand, the reaction to an attack can reveal the country's defensive potential in cybertechnology. The decision about the nature of the response to the threat is equally important, since overreaction may result in escalation of the conflict. In this context, special consideration should be given to interpretation of harmful acts by actors participating in political events.

Most cyber incidents are of low intensity and do not lead to escalation of the conflict either in cyber space and the real world, which means that policymakers have adopted an attitude of restraint (until now). This thesis corresponds with opinions based on the observations of Western researchers who have analysed cyber incidents that have occurred in the international space[7]. It should be noted that no cyber incident has caused the outbreak of hostilities in the real world so far.

Another group of researchers is against this stance as they believe that modern societies, including the military forces of many countries, depend on communication and information networks and a destructive attack on key systems may lead to military conflicts or to decisive acts giving one of the involved parties a significant advantage over the other[8].

On the basis of an interview with staff of the services responsible for cybersecurity in the V4 countries, it may be noted that there may be a third approach and they are not mutually exclusive. It may be presumed that two opposing countries may tolerate cyber operations as far as they do not cross certain boundaries or lead to unintended,

[6] K. Mačák, *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-state actors*, "Journal of Conflict and Security Law" 2016, vol. 21, no. 3, p. 408.

[7] B. Valeriano, R.C. Maness, *The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011*, "Journal of Peace Research" 2014, vol. 51, no. 3, pp. 347-360.

[8] E. Goldman, M. Warner, *Why a Digital Pearl Harbor Makes Sense… and Is Possible*, [in:] *Understanding Cyber Conflict…*, pp. 147-158.

damaging consequences. Further events may result in a situation of tolerance to cyberattacks unless they are accompanied by offensive and aggressive actions that destroy energy networks or infiltrate and take control over the military units of the targets.

Types of cyber incidents reported in the Visegrad Group countries (see Appendix, Table 1)

The first data set reveals a not very high level of computer crimes in relation to direct financial scams or theft of confidential information. Identity fraud or identity theft are also included in this set, since they are used for obtaining private information or stealing intellectual property. The greatest number of this type of crime was reported in Slovakia and Hungary – above 50% of all harmful incidents in cyberspace. Meanwhile, Poland and the Czech Republic reported a lower number of such acts – above 40%, although this number also seems to be quite significant.

Clear growth was also noted in relation to offensive and illegal contents, especially during election campaigns led in all of the V4 countries. Such behaviours may include hate speech targeted at politicians or other public individuals at a specific time. This was the case with Hungary in 2014 during campaigning for a national election as well as elections to the European Parliament, when hate speech increased from 7.2% to 9.9%.

A similar phenomenon was reported in the Czech Republic in 2013 during elections to the Chamber of Deputies, when verbal aggression reached as high a level as 10.3 %, and in 2016 during elections to the Senate, when verbal aggression rising to 12.8%.

In Slovakia, in 2014, during the presidential election as well as elections to the European Parliament, the number of aggressive behaviours in cyberspace rose from 8.2% to 9.7%. That situation repeated itself in 2016, when during parliamentary elections the increase was from 10.1% to 12.7%.

These correlations were also confirmed in the case of Poland in 2015, when elections to Parliament and the Senate took place at the same time as the presidential election, and the change in hate speech was significant, rising from 6.9% to 12.2%. All in all, political competition evokes much emotion which may be transferred to communication in cyberspace, intensifying offensive and illegal content.

The third classification concerns the damaging phenomena of when there is a primarily unnoticeable, remote breaking into the area of activities conducted by a specific institution. Such attacks usually occur with the use of digital malware such as viruses, worms or logic bombs[9]. They aim not only to paralyse the institution's activities, but also to infiltrate and steal confidential data, which may lead to a loss of confidence when such a situation is disclosed and to other serious problems in the institution's functioning. The cases of the V4 countries show that in allall four incidents mentioned above, neither the number of malware attcks detected in 2013-2021 nor the instruments used for cyberattacks changed, which may imply that only their targets differed.

Cybersecurity, at the most basic level, involves protecting computer systems against cyberattacks, data breaches or destruction. The fourth set of data is related to these categories of breaches that illustrate the level of each state's resistance to cyber threats. Some attacks targeted at paralysing communication and information networks in transport, power provision, emergency services, health services, water management, the food industry and farming, financial markets and public services have been reported since 2013[10].

This phenomenon has increased in all the V4 countries as the number of cyber incidents and attack attempts is constantly growing. Notice must be taken that in the case of Poland and the Czech Republic, the number of successful attacks on a specific actor's cyberspace was half the number of the attempts made. While, with regard to Slovakia and Hungary, the difference between the number of attempts and successful attacks is not as great. This may be evidence of weak cybersecurity systems operating in these countries.

The research has revealed a great deal of disinformation existing in cyberspace and undermining the credibility of government policy or manipulating public opinions. Internet users may (purposely or not) create and spread false information while hiding their real intentions. The intensity of this phenomenon depends on the specific country, and as may be noted, in Poland in 2013-2021 this indicator almost doubled:

[9] D. Lisiak-Felicka, *Information Security Incidents: A comparison between the Czech Republic and Poland, 20th International Scientific Conference*, "Economic and Social Development" 2017, vol. 20.

[10] J. Warner, E. Chapin, H. Matfess, *Suicide Squads: The Logic of Linked Suicide Bombings*, "Security Studies" 2019, vol. 28, no. 1, pp. 8-9.

from 4.3% to 8.5%. An equally high increase in the level of harmful acts was noted in Slovakia (from 3.4 % to 5.3%) and in Hungary (from 3.2% to 5.9%), while the lowest increase was recorded in the Czech Republic (from 7.6% to 9.4%).

The research has shown that in each country of the V4 in the described period, there was an increase in the number of harmful acts targeted at the security of information resources of public institutions. This phenomenon emphasizes the importance of information security for the stable development of the country.

Cyber activities are more and more frequently aimed at affecting public opinion, which leads to undermining the enemy's credibility. They comprise such acts as: leaking of confidential information, critical and harmful publications on the Internet, and creating special websites promoting the ideology of political groups, often representing extremist views. Cyber threats may be perceived as the use of technology for destructive actions influencing or modifying political processes[11]. The consequences of attacks on communication systems determine political attitudes and emotions, especially in democratic systems[12].

2. V4 budget expenditure on cybersecurity

Therefore, there is a need to apply more specific data, which could verify political plans. This may be done by using information about financial means that are an important element of a state's security strategy, regardless of its status and role in international society.

Financial resources of the state are needed for preparing an appropriate reaction to any tensions, crises and conflicts influencing directly or indirectly the condition of the state or resulting from its individual policies or political interests existing within political and military alliances[13]. Moreover, the state finances play an important role in the modernization of critical infrastructure as well as in everyday

[11] H. Lin, *Escalation dynamics and conflict termination in cyberspace*, "Strategic studies quarterly" 2012, vol. 6, no. 3, p. 48.

[12] S.M. Hersh, *The Online Threat, Should we be worried about a cyber war?*, New Yorker, 1 November 2010, https://www.newyorker.com/magazine/2010/11/01/the-online-threat [29.01.2022].

[13] J. Antczak, *Nakłady na cyberbezpieczeństwo państw Grupy Wyszehradzkiej*, Warsaw Institute, 24 September 2018, https://warsawinstitute.org/pl/naklady-na-cyberbezpieczenstwo-panstw-grupy-wyszehradzkiej [29.01.2022].

use of ICT[14]. Another component is expenditure on research and development, which has a significant impact on the level of the state's economic, scientific and technological advancement in the international sphere.

Therefore, finances are important in pursuing cybersecurity policy since they determine the range and scope of the tools used by the state[15]. The scale of the state funds invested in military and civil sectors may define their approach to one of these fields of cybersecurity. What is more, such a perspective is a useful tool for analysing the cyber potential of a given country and for characterizing cybersecurity on the base of the chosen phenomena or processes occurring in this area. The compilation of data on the financing of cybersecurity policy helps to show how policymakers perceive the scale and range of this phenomenon (see Appendix, Table 2)[16].

Obtaining information about state expenditure on cybersecurity may be, in some respects, a significant research challenge. Firstly, due to the legislative regulations regarding the classification of the state budget categories, the budget data in each of the V4 countries do not include the category of cybersecurity as they do not have a separate allocation of spending under this name. Secondly, another research barrier is the fact that the data on the expenditure incurred on cybersecurity can be found in numerous budget sub-categories, and their names and classifications are frequently not explicitly directly related to cybersecurity.

This phenomenon is partly consequent to the fact of cybertechnology existing in many economic, industrial, educational or cultural processes. Thus, the difficulty in classifying expenditures at the budget level results from the advanced digital integration in other areas of so-

[14] *Cyber Threat Report CEE 2018*, Instytut Kościuszki, 14 June 2018, https://ik.org.pl/publikacje/cyber-threat-report-cee-2018 [29.01.2022].

[15] K. Stańczyk, *Zarządzanie bezpieczeństwem zewnętrznym państwa przy wykorzystaniu instrumentów planowania budżetowego*, [in:] *Współczesne zagrożenia w zarządzaniu i bezpieczeństwie*, Z. Grzywna (ed.), Katowice 2014, pp. 535-548.

[16] Specific data may be found in the Appendix, table 2: *Budget expenditures on security and cyber security policy incurred by the V4 countries in 2013-2020.*

cial and economic life. It may be concluded that it is not possible to completely eliminate cybertechnology from our everyday lives[17].

A similar problem is the initiatives undertaken in education for cybersecurity by public institutions and the private sector. Different subjects are presented, i.e. during workshops or lectures, and the costs incurred may be covered from financial reserves. Also, the promoters may include such events in their reports under various names. Likewise, such dilemmas also apply to analyses of expenditure incurred by military forces that are equipped with the latest technologies. In this situation, it is not possible to separate cybertechnology from other areas and to estimate its value accurately. The same applies to other means and tools used by the army which integrate cybertechnology with military equipment. Thus, the question arises of whether it is possible to provide a clear classification of state expenditure on cybersecurity as one category. To answer this question, only expenditure whose purposes have been clearly determined are included in the table.

The third obstacle to the research, and one that is fairly significant in the gathering of accurate data, was the confidential nature of information. This was often accentuated by the personnel responsible for military cyber security.

The data collected in the categories of military or civil expenditure were obtained on the basis of interviews with the personnel of the Ministries of Finance in all four countries of the V4 and complemented by numerous conversations with representatives of the Communications and Information Systems Agency (CISA) of the Czech Republic, the National Agency for Network and Electronic Services established by the Government Office of the Slovak Republic, the Hungarian Military Computer Emergency Response Team (MilCERT) and two Polish units: the National Security Bureau and the National Centre for Cryptology[18].

Civil expenditure related to cybersecurity comprised purchasing technologies, software and training ordered by state actors, local government bodies, the banking sector, technical infrastructure (respon-

[17] D.J. Lonsdale, *The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios*, "Journal of Military Ethics" 2020, vol. 19, no. 1, pp. 20-39.

[18] The research was conducted in 2015-2017, within the international project „Visegrad Group and the Central European Cooperation" (No. 61450025) financed by International Visegrad Fund.

sible for providing power, gas, water, heating) transport infrastructure. This category also includes spending by schools on cybersecurity as well as research projects financed by budget or investments in police activities (at the level of the local or regional administrative area).

The military expenditure incurred on cybersecurity comprised purchasing cyber technologies, training, operations and tools related to intelligence services, data protection, and research projects in the field of cyber defence.

The largest increase in military cybersecurity spending between 2013 and 2020 was recorded in Poland, where spending rose by nearly €12 million. For the other countries, the increase in spending was respectively €1 million in the Czech Republic, €2 million in Slovakia and over €2 million in Hungary.

The second variable affecting the growth rate of cybersecurity spending relates to the civilian sector. In this case, the percentage share of government spending in Poland between 2013 and 2020 did not change significantly and ranged from 0.5% to 1%. Within this range, there was also not much variation in spending on cyber security policy in the civilian sector in the Czech Republic where the maximum difference was 0.8%, in Slovakia 0.5% and in Hungary 0.6%. However, in the case of the last country, there was a difference that in the period studied, a trend of decreasing spending on digital activities in the civilian sector can be observed. Nevertheless, the incurred costs for non-military cyber security allow us to conclude that the expenditures of all V4 countries remained almost unchanged in the level of investment on cyber security.

It may be noted that the V4 countries followed a stable financial policy in relation to cybersecurity and there were no significant changes in the period of investigation. However, it is only by comparing the level of investment between the civilian and military sectors that characteristic differences in the cybersecurity policies pursued by these countries become apparent. Comparing the data, one can see a large difference between the two areas (civilian and military). The case of Poland is significant. Such a difference in the structure of expenditure resulted from a general tendency to raise funds for military forces due to the unstable situation across its eastern border. Another reason was the increasing number of cyberattacks directed towards critical infrastructure in Poland. Thus, it may be concluded that each subsequent Polish government tried to raise expenditure to secure the country's cyberspace in the period considered.

However, that distinction was not so visible in the case of the other V4 countries. The military sector in cyberspace was also financed at a higher level but the contrast was not as clear as was the case with Poland. From the data for the Czech Republic, one can see disparities in spending ranging from €1.5 million in 2013 to almost €2 in 2020. A similar trend continues for Slovakia and Hungary; in both countries, there is an increase ranging from one million in 2013 to two and a half million euros in 2020. It should be noted that in 2013, Hungary, as well as Slovakia, had higher spending on cybersecurity in the civil than in the military sector.

The contrasts in expenditure also manifest the different level of military power of Poland, who spent almost 2% of GDP on military sector, and other V4 countries, whose expenses on security were from 1% to 1.18% of GDP in the period considered. The Czech Republic, Slovakia and Hungary conducted a low spending policy in relation to security and participated in such operations that are of low military potential and do not generate high costs. In this context, there appear to be some doubts whether these countries will enhance their defence. Between 2011 and 2017, these countries' defence spending was on average 1%, 1.1% and 0.8% of their GDP, respectively, and only 10% of that budget went to modernization of military forces. That phenomenon restricted other initiatives, i.e. enhancing of cybertechnological potential[19]. A noticeable shift has only occurred since 2018. This, in turn, may herald an evolution towards the military aspect of a country's cyber security policy. So far, the only country with a clear perception of cyber security as a military domain is Poland. The other countries rather try to balance both dimensions, however, putting more emphasis on civilian issues.

This is evidenced by the relationship that emerges in the context of the juxtaposition of military and civilian spending on cybersecurity. To sum up, the existing differences between the V4 countries highlight not only a disproportion between military and civilian re-

[19] K. Gawron-Tabor, *New Quality of Defence Cooperation within the Visegrad Group in 2010-2014*, "Obrana a Strategie" 2015, vol. 1, p. 70.

sources in the area of state cyber security policy, but also the way cyber security is perceived as an aspect belonging to either military or non-military state policy.

The discrepancy between the budgets of the V4 countries shows the inequality of the partners in regard to their resources and capabilities. The difference at the level of expenditure on defence by individual countries has a negative impact on the implementation of alliance commitments between these four countries. Investments in the civil sector are significantly higher than in the military sector. Therefore, it may be concluded that in reference to cyber defence policy, these countries pay more attention to social and economic objectives than to those related to defence.

The differences between the V4 countries have political causes. The government of each Visegrad country represents its own political doctrines and political plans dependant on election cycles, and cybersecurity issues are differently perceived. Each country is at a different level of development in this area. However, this factor depends on the moment of adopting and implementing cyber initiatives, on institutional contexts and the state budget capabilities.

3. Cyber threats on the agenda of the Visegrad Group Presidency

The increasing prevalence of cyber incidents in the public sphere became a motivation for governments to initiate a debate on cyber threat policy in the Visegrad forum, with a particular impulse to present their own ideas on the political context of cybersecurity. The Visegrad Group Presidency proved to be an excellent opportunity to put forward cyber security policy proposals and to have an exchange of views in this regard[20].

The Hungarian Presidency in 2013-2014 pointed to the need to raise awareness of cyber threats. The ideas and formulated goals were educational in nature, and sought to bring the V4 countries together in a common project.

[20] C.M. Bedea, V.O. Kwadwo, *Opportunistic sub-regionalism: the dialectics of EU-Central-Eastern European relations*, "Journal of European Integration" 2021, vol. 43, no. 4, pp. 385-402.

The next presidency in 2017-2018 was a continuation of this approach to cooperation between V4 countries in building cyber defence capabilities. Practical activities (with foreign partners) in the field of cyber security were mentioned, such as: the implementation of workshops, training and conferences which would create a practical forum for the exchange of ideas, reflections and experiences, thus strengthening the digital resilience of the V4 countries.

The Slovak presidency in 2014-2015 also strongly highlighted the aspect of community between the V4 countries and the EU, which, according to the authors of the document, in practical terms depends on the standardization of cybersecurity procedures.

It is noteworthy that the Slovak side took up the difficult topic of determining the boundary between cyber security and the protection of human rights and fundamental freedoms. As it turned out, the introduction of new technologies relating to ensuring security against cyberattacks raises many threats to the democratic system.

The next presidency of Slovakia in 2018-2019, reinforced the idea of strengthening cyber defence activities, pointing to the financial dimension. This was prompted, as it turned out, by the increasing number of cyber threats of an economic nature.

The 2015-2016 Czech Presidency continued the objectives previously expressed by the Hungarian and Slovak partners regarding cooperation, while emphasizing the key role of public-private partnerships in the area of cybersecurity.

The programme of the Polish Presidency of the Visegrad Group in 2016-2017 also emphasized the value of cooperation between the V4 countries, but shifted the emphasis to the issue of greater integration with the scientific community to strengthen cyber defence based on building scientific networks.

The educational and scientific aspect was also empasized under the next Polish presidency, which ran from 2020 to 2021. Education was an important element, which was treated as a preventive factor against cyber threats. In addition, joint projects among the V4 countries, which provide opportunities to exchange experience and share knowledge about existing or possible cyber incidents, were also highlighted.

Tracing the changes in the perception of cyber threats by individual state helps to understand the evolution of the Visegrad Group's political goals, which translate into policymaking on the EU forum and the formulation of strategic objectives in the area of cyber security. Despite the declarative nature of many of the V4 presidency programmes, one can see strongly articulated objectives in the area of cyber security, which relate to the deepening of cooperation in the field of cyber defence, but also present practical tips and projects to be implemented to help raise the level of cyber security.

The governments of individual countries are trying to approach the problem of cyberattacks in a comprehensive way. It should be noted, however, that in their presidency programmes, Poland and Hungary devoted more attention to issues related to the militarization of cyberspace, unlike the Czech Republic and Slovakia, which place more emphasis on the economic consequences of cyber incidents. However, the main factor determining the perception of cybersecurity is events occurring in the international environment. In other words: the V4 presidency provides an opportunity to emphasize tasks that will adapt the cyber security policies of the V4 countries to the cyber reality.

4. Cyber threats in selected cybersecurity strategies of Visegrad Group countries

The hierarchy of priorities in the field of cybersecurity policy varies from country to country. The strategy documents present a vision of the cyber environment which corresponds both to the existing threats in it and reflects the subjective attitude of the state authorities, thus giving an individual character to cybersecurity strategies. For all four states, the multifaceted nature of digital threats is highlighted:

> *These can take several forms, including critical infrastructure attacks, cyber espionage, intellectual property theft, cybercrime and cyberattacks as part of hybrid threats* (Slovakia 2021-2025, p. 5).

Cyberspace is an area of political, economic and military competition, which means that, in the opinion of the authors, any one incident can affect the functioning of many areas of the state. For this reason, attention is drawn to the need for changes that are to be adapted to the process of digitization. There is a strong connection between innovation in the public sphere and cyber security. One of the priorities is the issue of updating technology, which also implies progress in research and development. Cooperation with the scientific community is therefore one of the main elements supporting the state's efforts to prevent harmful cyber incidents. This will make it possible to:

> *(…) assess the effectiveness of protections and resilience to cyber threats; assess the effectiveness of responding to incidents; develop methods of detecting and [analysing] new types of cybercrime, cyberterrorism and cyberespionage; study methods of attacks (including attacks of a hybrid nature) and measures to counteract these attacks and mitigate their effects; protect democratic processes against disruption by cyber threats* (Poland 2019-2024, p. 23).

Cyber security is therefore treated as one of the conditions for economic development and efficient functioning of the state.

> *This Strategy indicates that Hungary is ready to perform and take responsibility for cyberspace protection tasks and intends to develop the Hungarian cyberspace as a key element of Hungarian economic and social life into a free, secure and innovative environment. By way of efficient protective measures based on prevention, the primary objective is to manage the threats and risks emerging in and coming from the cyberspace, as well as to reinforce government coordination and measures* (Hungary 2013, p. 2).

In all strategies, attention is paid to the social aspect, and with that, competence, skills and awareness in cyber security. Education and public awareness of cyber threats are also indicated and prioritized here as preventive measures.

> *With regard to cyber defence of the Czech Republic, it is necessary to mention only poor knowledge of behaviour rules in cyberspace and proper operation of the cyberspace among senior state or military officials* (Czech Republic 2018-2022, p. 6).

The need to adapt to dynamic changes in the cyber environment is recognized. One of the prerequisites for building an effective cyber defence is to standardize both legal and non-legal responses towards cyber incidents.

> *Implementation of security measures is a standardized operation that is determined by law, implementing regulations or a non-legislative standard. An insufficiently serious approach to such requirements leads not only to incomprehension of the existence of security measures, but also to the emergence of a weak spot*

> *of the organization, which then becomes more vulnerable to attacks both from the outside and the inside* (Slovakia 2021-2025, p. 10).

The authors of the strategy recognize the complexity of the concept of cyber threats and their effects:

> *Primary targets of these cyberattacks can be especially systems closely interconnecting the computer environment with the real infrastructure, for example in water management, energetics, etc. The attacks can even directly target components of the defence infrastructure.* (Czech Republic 2018-2022, p. 4).

Therefore, one way to ensure a high level of cyber security is international cooperation. It is seen as being the responsibility of international structures to offer a guarantee of security and this provides an impetus for increased development in the field of cyber security policy.

> *Poland's membership in the North Atlantic Treaty Organization is an important pillar of the country's security, as well as the security of entire Euro-Atlantic area. Ever more intensive attacks of a hybrid nature make it essential to invest in deterrence and defence capabilities, including increasing of the resilience and ability to respond quickly and effectively to cyberattacks* (Poland 2019-2024, p. 27).

While outlining possible cyber threats, the authors of the strategy also point to entities whose potential and international importance makes them partners and allies in reducing digital threats. The idea of commonality in terms of cyber security with such organizations as the EU, NATO, the Organization on Security and Cooperation in Europe (OSCE), the UN and the Council of Europe is emphasized. Membership in these organizations is supposed to offer a guarantee of cyber security.

> *Hungary aims at establishing and maintaining trust-based cooperation with all public and private actors of the global cyberspace sharing the same set of values with Hungary, and endeavours to guarantee free and secure use of the global cyberspace through its allies and international relations, particularly the EU and the NATO, the OSCE, the United Nations, the Council of Europe and other international organizations in which the country is a member* (Hungary 2013, p. 3).

A wide range of cooperation in terms of institutions as well as form, this can be seen as preventive measures, which are of course important, but are nothing new, as they echo the ideas contained in both EU strategy documents, i.e. The EU's Cybersecurity Strategy for the Digital Decade (2020) and Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace (2013).

Each of the V4 countries has progressively acknowledged the growing importance of the issue of cyber threats and the urgent need to take a comprehensive approach to address them in order to protect critical infrastructure that is increasingly integrated with cyber technology. All V4 countries recognize the link between cyber security and national security and are aware that events such as the failure of information and communication technologies or critical infrastructure can harm national security and affect the lives of citizens, as well as threaten the proper functioning of the economy and the delivery of public services.

The V4 countries in their strategy documents emphasize the compatibility of their standards with the concepts found in the strategic programmes developed by NATO and the European Union. This review of the Visegrad countries' cybersecurity strategies reveals that the documents are comprehensive and integrated. There is a holistic approach to cyber security that includes economic, social, legal, as well as military and intelligence issues.

Conclusions

The characteristic features of cyber threats are: a pace of change and innovation that is much faster than in the case of harmful phenomena reported in physical world; technology that is much more decentralized at present and may constitute an instrument of destabilization in a country; and last but not least, many more actors involved in harmful acts in cyberspace than in real-world conflict. Reacting to various cyber threats or the attempts to minimize them is not only a challenge for many governments but also will generate difficult problems. Considering the data related to the most frequent cases of cyber incidents, we may find appropriate preventive measures. However, the comparative analysis of data is quite complex due to the lack of both standardization of reports and classification of incidents in the Visegrad Group countries.

The analysis conducted in the paper only partially confirms the research hypothesis. Digital threats lead to a common position and thus a common strategy of the V4 countries in the area of cyber security. This consists of state budget expenditure on digital defence, joint strategic thought-building within the framework of the cyber security strategy, and articulation of goals during the V4 presidency. However, this is not a unique phenomenon; such initiatives can also be seen among other EU countries. The factor undermining the idea of the commonality of V4 countries is the conflict in Ukraine, which does not fall within the time period given in the title of the paper. However, it is worth noting that this event has significantly deepened the divisions between the Central European countries. The situation is bound to change and reshape international politics. Going forward, it is reasonable to believe that the conflict in Ukraine will usher in a new chapter in the cooperation not only of the Visegrad Group but also in the cyber security policy of the EU and NATO.

The application of new technologies in the areas of state, economy and society has led to an increase in the risk of cyber threats over the past decade. In such an environment, ensuring cyber security is critical to the performance of the core functions of the state and its citizens. A noticeable trend is the acceleration of the V4 countries' activity in initiatives aimed at improving cyber security. The description and comparative analysis of practices adopted by V4 countries, based on selected categories, makes it possible to identify the status as well as critical areas of cyber security policy development.

The above analysis of strategic documents and political declarations at the level of V4 presidencies indicates that policymakers are aware that in order to achieve a sufficient level of cyber security, the V4 countries must implement appropriate measures for priority areas of state and economic development. It is also crucial to adjust the resources of many areas of the state and its institutions, as well as to develop and implement measures in line with strategic documents developed at the national and international level.

References

Antczak J., *Nakłady na cyberbezpieczeństwo państw Grupy Wyszehradzkiej*, Warsaw Institute, 24 September 2018, https://warsawinstitute.org/pl/naklady-na-cyberbezpieczenstwo-panstw-grupy-wyszehradzkiej.

Axelrod R., Iliev R., *Timing of cyber conflict*, "PNAS" 2014, vol. 111, no. 4.

Bedea C.M., Kwadwo V.O., *Opportunistic sub-regionalism: the dialectics of EU-Central-Eastern European relations*, "Journal of European Integration" 2021, vol. 43, no. 4.

Cavelty M.D., Wenger A., *Cyber security meets security politics: Complex technology, fragmented politics, and networked science*, "Contemporary Security Policy" 2020, vol. 41, no. 1.

Cyber Threat Report CEE 2018, Instytut Kościuszki, 14 June 2018, https://ik.org.pl/publikacje/cyber-threat-report-cee-2018.

Czech Republic 2018-2022 (2018): Cyber Defence Strategy of the Czech Republic 2018-2022, https://ccdcoe.org/library/strategy-and-governance.

Egloff F., *Cybersecurity and the Age of Privateering*, [in:] *Understanding Cyber Conflict. 14 Analogies*, G. Perkovich, A. Levite (eds.), Georgetown 2017.

Gawron-Tabor K., *New Quality of Defence Cooperation within the Visegrad Group in 2010-2014*, "Obrana a Strategie" 2015, vol. 1.

Goldman E., Warner M., *Why a Digital Pearl Harbor Makes Sense… and Is Possible*, [in:] *Understanding Cyber Conflict. 14 Analogies*, G. Perkovich, A. Levite (eds.), Georgetown 2017.

Hersh S.M., *The Online Threat, Should we be worried about a cyber war?*, New Yorker, 1 November 2010, https://www.newyorker.com/magazine/2010/11/01/the-online-threat.

Lin H., *Escalation dynamics and conflict termination in cyberspace*, "Strategic studies quarterly" 2012, vol. 6, no. 3.

Lisiak-Felicka D., *Information Security Incidents: A comparison between the Czech Republic and Poland, 20th International Scientific Conference*, "Economic and Social Development" 2017, vol. 20.

Lonsdale D.J., *The Ethics of Cyber Attack: Pursuing Legitimate Security and the Common Good in Contemporary Conflict Scenarios*, "Journal of Military Ethics" 2020, vol. 19, no. 1.

Mačák K., *Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-state actors*, "Journal of Conflict and Security Law" 2016, vol. 21, no. 3.

Simons G., Danyk Y., Maliarchuk T., *Hybrid war and cyber-attacks: creating legal and operational dilemmas*, "Global Change, Peace & Security" 2020, vol. 32, no. 3.

Stańczyk K., *Zarządzanie bezpieczeństwem zewnętrznym państwa przy wykorzystaniu instrumentów planowania budżetowego*, [in:] *Współczesne zagrożenia w zarządzaniu i bezpieczeństwie*, Z. Grzywna (ed.), Katowice 2014.

Valeriano B., Maness R.C., *The Dynamics of Cyber Conflict between Rival Antagonists, 2001-2011*, "Journal of Peace Research" 2014, vol. 51, no. 3.

Warner J., Chapin E., Matfess H., *Suicide Squads: The Logic of Linked Suicide Bombings,* "Security Studies" 2019, vol. 28, no. 1.

Wirtz B.W., Weyerer J.C., *Cyberterrorism and Cyber Attacks in the Public Sector: How Public Administration Copes with Digital Threats*, "International Journal of Public Administration" 2017, vol. 40, no. 13.