DOI 10.14746/ssp.2022.3.4

Marek Górka
Koszalin University of Technology
ORCID: 0000-0002-6964-1581

Cybersecurity in the V4 Policy in 2011–2022

Abstract: The Visegrad Group (V4) is one of the most intriguing examples of cooperation among countries in Central Europe. It unites the Czech Republic, Hungary, Poland and Slovakia. Together, these countries form a useful framework which facilitates policy coordination at the regional level. They also implement EU agendas by creating networks of cooperation with neighbouring countries. These networks are based on the countries' mutual security geography and a common strategic culture. When, in 2014, the most important political goals were achieved, there emerged a need to set a new direction for cooperation. It turned out that many issues in the field of public policy, such as transport infrastructure, natural environment, tourism, migration, culture or education, can be effectively implemented at the V4 level. Moreover, cooperation in a common cybersecurity policy is now a chance for deeper cooperation between the four countries. However, changes in the use and dissemination of cybertechnology in the public space began to gather momentum only in the first decade of the 21st century. Thus, the process of cyberrevolution was a harbinger of changes in state management. This study analyses the cybersecurity policy of the Visegrad Group countries from 2011–2022 from both military and non-military aspects.

Key words: Visegrad Group, cyber security policy, non-military policy, digital policy, technological innovation, digital development

Introduction

The idea of the Visegrad cooperation has been inseparably linked to the idea of a united Europe from the beginning. The framework of the Visegrad Group appeared as a result of a deeply rooted cultural concept of Central Europe, and the V4 was aimed at strengthening the region's identity. The European integration is declared in the title of the Visegrad Declaration – the document inaugurating the V4 group, signed by the presidents of Poland, the Czech Republic, Hungary and Slovakia in 1991 (Visegrad Group, 1991). One of the main objectives of the Declaration was the full participation of these countries in Europe's political, legislative, security, and economic systems.

The cooperation of the V4 group with the EU and NATO seems to be the best and the most important method to guarantee cybersecurity, as its countries do not have such advanced protective instruments. However, participation in the international structures requires obeying specific rules in relation to cybersecurity and acts as a catalyst for the attitudes and strategies of the Central Europe countries. Many initiatives introduced by the European Union Agency for Cybersecurity (ENISA), and focused on improving efficiency and capabilities to combat the growing number of possible cyberattacks, have turned out to be a great help for the V4 experts on cybersecurity.

Moreover, membership in the EU and NATO also constitutes significant support in case of an attack (Urbański, Dołęga, 2016, pp. 82–90). In such a case, determining an attacker is not as challenging as it would be if the affected country was not a member of these structures. In this situation, the wealthy countries, which own advanced digital infrastructure and are motivated to introduce cyber policy, may be helpful. However, the V4 countries cannot invest significant means into such investigations. In these circumstances, an attacked country may, directly or indirectly, ask its more powerful allies for help with cybersecurity issues, as this is the case with the Visegrad Group countries that direct such requests to the EU and NATO. This process is analogical to the events of 2007 when the Estonian government did not formally accuse Russia but passed their suspicions to the US and asked NATO to help them modernise their security system. The disproportion in the economy, technology and military power between Estonia and Russia gave them some thought to the proper and efficient actions that Tallin should have taken. A weak country may not be able to convince others that the alleged perpetrator was behind a cyber incident. Moreover, in case of not providing compelling evidence, an official accusation of a cyberattack may spark a diplomatic crisis and result in negative political and economic consequences on the international scale (Wierzbicki, 2015, pp. 134–148). The case of Estonia clearly shows how the escalation of conflict may affect essential supplies, for example, oil or gas products, which are the Estonian economic fundamentals.

Another reason for enhancing cooperation between the V4 and the EU/NATO is the nature of cyberthreats, which operate beyond political and geographical borders since computer systems create networks working above these levels. Therefore, the V4 countries, as members of the EU and NATO, must integrate their activities with the cybersecurity policy of both organisations. Their governments' cybersecurity policy is twodimensional. On the one hand, they must provide a permanent overview of strategic documentation considering current events. On the other hand, they strive to develop their cyber capabilities to be compatible with the standards of the EU and NATO. Some factors may shape a security policy in cyberspace, i.e., information on the existing or possible threats aimed at ENISA or EC3 (Christou, 2018, pp. 355–375).

The V4 countries follow a cybersecurity policy, which is still relatively new and raises many questions. In this part of the work, the author attempts to establish whether the Visegrad Group Countries actively participate in shaping cybersecurity policy, present their own solutions, or are only passive actors who accept the positions represented by the EU and NATO. The other question is related to the fact that all V4 countries are members of both structures, and as such, they should choose to pursue the policy corresponding to the objectives adopted by the EU or NATO. However, considering these two organisations, one is more economical and political, whereas the other is military. The response to this question may be found in analysing the V4 countries’ cybersecurity strategies and budget expenditures. Moreover, this also facilitates defining their cybersecurity policy activity in the military or civil context.

Due to the growing dependency on cyber technologies, the question of cyberspace often becomes a priority for guarantying security, which is visible in the activities of the countries, their official statements, declarations, strategies or regulations aimed at defining the processes within cybersecurity (Kacała, 2016, pp. 59–69). Another objective of this work is to outline the priorities and initiatives within cybersecurity, which are undertaken by the V4 countries during their subsequent presidencies at the international level. It may help in a better analysis of the methods of establishing cybersecurity policy or may be interpreted as their official stance on the phenomena occurring in cyberspace.

There is a growing view in scholarly circles that security should be defined not only by how states acquire military and economic power but also by how governments conduct public narratives to enhance cybersecurity. Therefore, an ever-present research challenge is a search for new theories to better understand states’ policies towards cyberspace.

The research analysis conducted in this paper is concerned with the characterisation of the discourse based on primary sources, such as strategic documents, declarations, and policy statements announced at the forum of cooperation of the Visegrad Group countries. That, in turn, will sufficiently explore and describe the main cyber security discourses among V4 members. Each country has the potential to shape its own cyber security policy not only internally but also in a broader international sense. In this context, an analysis of the cyber security discourse is required to clarify the sources and nature of the actions taken and changes taking place in the area of cyber security policy among Central European countries.

The article covers two main research areas: the description of activities implemented by the member states of the V4 in relation to the priorities accepted during their rotating presidencies, the separation and determination of the most important international initiatives introduced by them, and the corresponding documentation. Moreover, when we get a closer look at the documentation, we will be able to define the cybersecurity policy of the V4 countries.

Cybersecurity in the Priorities of the V4 Countries Presidency

As a result of the extended and dynamic development of cybertechnologies, many political declarations and legislative regulations are being left behind in the enhancement of the processes in cyberspace. It raises discussions about the need for regional and international cooperation. The establishment of the International Visegrad Fund in 2000 strengthened cooperation in mutual cultural, scientific and educational projects. (Czyż, Kubas, 2014, p. 172). Subsequently, as cybertechnologies were getting more and more common, more projects related to cybertechnologies appeared and were implemented at the international level (Olszewski, 2016, pp. 203–215).

Another significant fact in the development of the V4 was the signing of the Kroměříž Declaration in 2004, when all four countries declared their determination to continue cooperation within the Visegrad Group as the Member States of the European Union and NATO. The accepted guidelines stipulated the future areas of the Visegrad Cooperation, such as infrastructure, natural environment, tourism, migration, culture, and education. The countries underlined their active participation in developing the Common Security and Defence Policy (CSDP) as their contribution to tightening cooperation with the EU and NATO and building a productive dialogue between these organisations. Even though cybersecurity was not directly mentioned in the Declaration, due to the extended use of cybertechnologies, further cooperation within these areas also took on a digital character (Kacała, 2016, p. 66). In no time did that fact become a key factor in the current affairs within the V4 countries.

The moment when many governments and world organisations, i.e., the EU and NATO, realised the role of cybertechnology in the functioning of a state was, as mentioned, the cyberattack in Estonia in 2007. That event was also a matter of attention for the countries of Central Europe. The need for introducing laws and regulations related to international cooperation and developing individual strategies within cybersecurity was pronounced in the same year, during the Czech presidency of the Visegrad Group.

The growing number of cyber incidents in the public space motivated many governments to initiate a debate on security policy in the EU and enabled the V4 countries to submit their own ideas on the political context of cybersecurity (Botond, 2017). The rotating presidency was a great opportunity for each member state to exchange views and present their proposal for cybersecurity policy.

Most social and political processes depend on information and communications technology (ICT). Although cyberspace has offered numerous possibilities for social and economic interactions, it has also made state institutions more susceptible to harmful actions (Samoilenko, Osei-Bryson, 2015, pp. 94–96). The multilateral cooperation on cybersecurity issues was heatedly discussed during the Polish presidency in 2008–2009. It was emphasised that cyberthreats were increasingly detrimental to the economy, which was especially important for the V4 countries, which were in the period of transition in the 1990s. With time, many changes appeared consequent of the extended use of cybertechnologies and many public and private actors started using them to affect the global economy and nations’ security.

A debate on the impact of cybertechnologies on military and non-military systems was one of the main objectives of the Hungarian presidency in 2009–2010. The strategy of NATO, announced in Lisbon in November 2010, enabled policymakers to plan actions based on the overall assessment of the strategic environment. The undertaken subject, concerning the influence of cybertechnologies on national security, largely reflected the urgency of shaping cybersecurity policy in the future.

The further growth of the cybersecurity concept was continued during the Slovak presidency of the V4 in 2010–2011 when special attention was given to the global and transborder nature of cyberthreats. It was emphasised that international cooperation and support from the EU and NATO should be enhanced.

The Slovak presidency coincided with the Bratislava Declaration of the Visegrad Group Heads of Governments announced by the Prime Ministers of Poland, the Czech Republic, Hungary and Slovakia on the 20th anniversary of the Visegrad Group. That document reconfirmed their declarations related to cybersecurity policy and efforts to enhance cooperation with the EU and NATO as an indispensable condition for the long-time security of the V4 countries (Senate of the Republic of Poland, 2012).

The main concern for the Czech presidency in 2011–2012 was innovation as a key element in promoting cooperation in cybersecurity. By acting accordingly, the digitalisation of the economy became a significant source of economic growth. Moreover, it became clear that the V4 countries need to introduce extended research and innovation to stimulate further cybersecurity development and succeed in that field.

Another significant moment during the Czech presidency was adopting the joint V4 declaration *Responsibility for Strong NATO*, in which the Visegrad countries declared their intention to promote regional security and the development of defence capabilities. They knew that NATO might support them in successfully implementing the security policy (Valášek, 2012). It should be noted that the V4 countries emphasise their consistent position and coordination in defensive planning since their final objective in security policy is a more efficient use of military resources and capabilities consequent to their membership in NATO.

There was a further development of security policy based on the cooperation of the Visegrad countries during the presidency of Poland in 2012–2013. Their main objective was the coordination of mutual positions of the V4 countries with the Baltic states, Romania and Bulgaria. One of the objectives of that program was to raise the interests of those countries in cybersecurity issues (Ministry of Foreign Affairs Republic of Poland, 2012–2013). Poland emphasised the need to cooperate with the EU regarding security and defence and to ensure a complementary partnership with NATO. Moreover, special attention was paid to the close bonds of foreign policy with security policy, which might indicate the ambitions of the Polish authorities to step into the role of a regional representative.

Such cybersecurity policy continued during the Hungarian presidency in 2013–2014, when the priority was given to cooperation in education, consulting, information exchange, research and collaboration of scientists for implementing cyber technologies. At the same time, the V4 focused on combating cybercrimes and developed a closer partnership with their regional neighbours, including the Baltic and the Western Balkans states. It must be noted that the exchange of knowledge, enhanced dialogue and collaboration at the operational and political levels played a special role in that period.

Concurrently with the Hungarian presidency, there appeared a regional initiative called Central European Cybersecurity Platform (CECSP), aimed at increasing the efficiency of actions undertaken against cyber threats (Berzsenyi, 2015). An exceptional fact about the Platform was that it worked as “V4 plus” and comprised five countries presenting their mutual stance on international defence issues: the member states of the V4 and Austria. Moreover, the formula of their cooperation turned out to be a special platform for debates and the exchange of experiences in cybersecurity policy, which was a matter of interest for each of the states who took over the Presidency of the Visegrad Group. The objective of that initiative was to strengthen the role of this region of Central Europe and to promote security-building measures by access to information, the best practices and experiences related to cyberthreats.

Another important initiative during the Hungarian presidency was when on March 12, 2013, the V4 Ministers of Defence signed three documents of strategic importance known as „The Long-term Vision of the Visegrad Countries on Deepening their Defence Cooperation”. That was a direct response to breaking security principles and the escalation of the political crisis in Ukraine since the V4 countries jointly declared their intentions to tighten cooperation with this country in the field of defence and security (Kříž, 2018, p. 361). In order to confirm their decisions, the countries planned to create a joint forces group, the convergence in military domain and military interoperability, which were expected to create a mutual security identity within the Visegrad Group.

The Slovak presidency in 2014–2015 opened a new chapter in cybersecurity issues by focusing on increasing the resilience to cyberattacks in computer systems and combating cybercrimes. The program adopted by the government defined the priorities and objectives of cyber security policy in the context of the digitalisation of the economy. The priority of that presidency was also the development of specific activities within the digital economy that affects retail trade, transport, financial services, production of goods, education, health services, media etc., and goes beyond the ICT sector (Ministry of Foreign and European Affairs of the Slovak Republic, 2014–2015). The Slovak presidency was an opportunity to emphasise the benefits of using new technologies and focused on data security in cyberspace and improving the management of information and communication infrastructure. In addition, the digital economy and its wide range of capabilities, seen as a risk for the sustainable functioning of the state and society, was also in their sphere of interest.

The Czech Republic held the next presidency in 2015–2016 and comprised further enhancement of cooperation within CECSP. Thus, it was a continuation of the previous programs related to cooperation in cybersecurity with neighbouring member countries and the development of information systems (Ministry of Foreign Affairs of the Czech Republic, 2015–2016). These issues should be compatible with the regulations and standards imposed by international organisations, whose members are the V4 countries. Implementing standards and channels for secure communication between CECSP countries aimed to build a mutual position among the member states.

The Polish presidency in 2016–2017 showed a growing interest of the governments in cybersecurity and in raising the complexity of cyber policy. That might imply that the Visegrad countries tried to provide as extended definitions of cyber phenomena as possible. Moreover, there was a need to continuously upgrade the knowledge on cybersecurity policy and correct the activities related to the new forms of cyberthreats. It was emphasised that each of the areas connected with the government, military forces, industry, private sector or academics might contribute to enhancing cybersecurity (Ministry of Foreign Affairs Republic of Poland, 2016–2017).

The technological and social challenges consequent to digitalisation and newly-appearing cyberthreats were the area of interest of another Hungarian presidency in 2017–2018. They paid special attention to the exchange of experience in cyber defence and hybrid war, which acquired new meaning in the face of the lasting conflict in Ukraine. In this connection, a new role of the civil defence tasks appeared to strengthen the resilience of critical infrastructure to reveal and combat cyberattacks. That was also the period of further cooperation of organisations involved in cybersecurity, acting in line with the objectives previously formulated by CESP and based on meetings with experts, joint exercises and training courses in relation to cyber incidents. Those initiatives helped to increase mutual trust between the V4 countries and mutual recognition of cybersecurity policy (Ministry of Foreign Affairs and Trade of Hungary, 2017–2018).

The Slovak Presidency falling 2018–2019 also directed the attention of the V4 countries to cooperation in the areas of hybrid and cyber threats and strategic communication at both European and national levels. This goal was to be achieved with the support of activities under the Slovak Chairmanship of the OSCE falling in 2019.

A distinctive feature of Slovakia's cybersecurity policy was its attention to new forms of cybercrime. The agenda of Slovakia's V4 presidency strongly emphasised the economic nature of cyber threats related to the misuse of cryptocurrencies, especially bitcoin. It was also noted that the fight against cyber threats initiates a discussion on the protection of personal data, the possibilities and conditions of storing data for criminal proceedings and the simplification of access to electronic evidence to obtain it more quickly or use it later in court.

The role of state institutions in relevant topics such as hate speech and new forms of cybercrime is also pointed out. With the influx of extremism in Europe, not excluding V4 countries, it is necessary to focus efforts on its prevention. Emphasis has also been placed on enhancing cooperation using cybertechnologies in crisis management and cross-border cooperation (Ministry of Foreign and European Affairs of the Slovak Republic, 2018–2019).

The developing cooperation of the V4 countries in the digital sector was repeated during the Polish Presidency in 2020–2021. However, compared to the previous goals formulated by the other V4 countries, Poland presented the cyber security policy through the prism of innovation development, especially the development of the application of artificial intelligence (AI), robotics, and e-commerce. This process would take place through cross-border initiatives and the promotion of cooperation between regional private and public entities.

Poland also maintained the need to carry out tasks in combating cyber threats, especially those of a cross-border nature, through international exercises, education for cybersecurity, research and development, and the development of unified international law in cyberspace operations. The digital economy was also assigned a huge role in mitigating the effects of the global pandemic crisis, seeing the use of digital tools as an opportunity to support the functioning of private and public institutions across the region (Ministry of Foreign Affairs Republic of Poland, 2020–2021).

Hungary assumed the next chairmanship of the V4 group for the years 2021–2022, and in addition to cybersecurity, it pointed to other equally important challenges, such as migration, Schengen border protection, combating pandemics, and crisis management. From the Budapest government’s perspective, the policy on combating cyber threats was shifted to the country’s internal security. In contrast, the international accent in digital policy was defined as two main tasks. The first referred to the issue of coordinating cyber activities within the EU AND NATO agenda. The second focused on the V4+ cooperation on cyber security with interested external partners such as the UK (Ministry of Foreign Affairs and Trade of Hungary, 2021–2022).

Summarising this part of the analysis, it should be noted that each country during the V4 presidency devoted more and more attention to the issue of cyber security. However, some countries, such as Poland, emphasise international threats more strongly, especially in the military aspect, while others balance military and non-military threats on the cyber level or devote much more space to economic and social aspects. Nevertheless, in recent years, the perspective on cyber security has been evolving in a non-military direction. Still, the position among the V4 countries, indicating both spheres as crucial for the region’s security, is present with varying intensity.

The Visegrad Group is an active actor in cybersecurity policy, and its role mostly relies on defining strategic goals corresponding to the EU strategies. The programs of the V4 presidencies have followed the main assumptions of cybersecurity concepts stipulated in 2013. They are also an important element of relations with the EU as proof of the active involvement of all the Visegrad Group member states in cybersecurity strategies. It is difficult to estimate which countries are more effective in defining cybersecurity problems since their governments try to identify the issues individually. However, it shall be noted that during the Polish and Hungarian presidencies, more attention was paid to the militarisation of cyberspace, whereas the Czech Republic and Slovakia mostly focused on the digital economy. Moreover, the main factors determining the perception of cybersecurity are the existing and ongoing international events. In other words, a presidency of one of the V4 countries is an opportunity to define the tasks which allow them to adjust their cybersecurity policy to cyber reality.

In addition, cooperation and continuation of previously accepted strategies dominate in official declarations related to subsequent presidencies, which is visible in the relations between Poland and Hungary. All in all, the challenges concerning cybersecurity undertaken during the presidency of one of the member states are compatible with those undertaken in the framework of activities accepted by its predecessor.

The Problem of Cybersecurity and Political Declarations

The official information issued during international meetings and conferences is another manifestation of the political activities of the V4. The cooperation also occurs through less formal events in education, science and culture and is aimed at consulting and exchanging cybersecurity-related knowledge and experience. Concerning the political activities listed below, we may obtain some information on their intensity and range, which should be sufficient to keep up with the dynamic growth of the virtual network threats.

The declarations given by the governments of the V4 member states show that their policymakers realise that cyberspace is a global phenomenon which needs global cooperation for solving problems consequent to its dominant role in the public space. The Hungarian government initiated the Declaration of October 4, 2012, which emphasised the necessity of establishing international cooperation in shaping cybersecurity policy (Foreign & Commonwealth Office, 2012).

The mentioned the Visegrad Group Heads of Governments signed Bratislava Declaration on February 17, 2011 to commemorate the 20th anniversary of their cooperation and referred not only to the mutual political and economic goals but also to the threats consequent to the use of digital technologies. Those new challenges were interpreted from the perspective of the threats to the existing democratic principles on which the EU is founded.

The perception of cybersecurity in the context of military threats was a matter of interest for the V4 Ministers of Defence. It was on May 7, 2012, when they jointly declared that membership in NATO structures is a basic factor ensuring the quality of cyber defence (Visegrad Group, 2012).

Another factor positively influencing cybersecurity policy is numerous international conferences, workshops and meetings with representatives of the V4 countries, experts in the industry, private sector, and nongovernmental organisations expected to cooperate in providing a safe and reliable digital environment. The conference of October 5, 2012 in Martonyi (Visegrad Group, 2013a), Hungary or regular conferences in Krakow, Poland, are good examples of the initiatives that are opportunities for the exchange of knowledge, mutual dialogue, and help in increasing mutual trust between the V4 countries.

Moreover, the Defence Ministers of the V4 countries meet annually to sum up their defence cooperation, including cybersecurity and plan mutual priorities for further security policy. Their Declaration of September 12, 2013 (Visegrad Group, 2013b) indicated the need for tightening cooperation in combating cyberthreats based on the complementarity of actions of individual countries. Their efforts should be closely related to the multinational program of developing military capabilities *NATO Smart Defence* and to *Cyberdefence* – a project team of EDA (European Defence Agency). The implementation of that idea started in the context of a serious imbalance in the defence expenses of NATO states. The program was designed as a cooperative way of generating and complementing different defence capabilities and sources to reach a better efficiency at a smaller risk to the security of NATO members.

It was on June 19, 2015, in Bratislava, the Czech Republic, when the Prime Ministers of the Visegrad countries issued a joint statement in which they declared a need for a new European strategy for security and foreign policy until the first half of 2016 (Office of the Government of the Czech Republic, 2016). They emphasised the meaning of deeper relations between the EU and NATO necessary for fighting contemporary threats such as hybrid conflicts, organised crime, terrorism, illegal migration and cybersecurity.

The next event was a joint declaration of June 8, 2016, when the V4 Prime Ministers confirmed their mutual position before the NATO Summit in Warsaw and efforts aimed at strengthening their cooperation with the EU and NATO, especially in cyber defence and counteracting cyber threats. Special attention was also given to the need for a more complex approach to transatlantic security that might effectively respond to various challenges and threats flowing from different directions.

The next joint statement of September 19, 2016 underlined the need to enhance security in the Schengen Area and protect the EU’s external borders (Office of the Government of the Czech Republic, 2016). Another issue was to ensure the effectiveness of border security, which was directly related to computer tools and improving the interoperability of computer systems working in each of the EU’s countries for processing personal data.

The V4 countries are also interested in knowledge-based economic development. Each aspect of a country’s security comprises cybertechnologies that may be found in politics, economy and military issues. Their main objective declared on November 18, 2016 (UaPosition, 2016), was to increase the capabilities of the V4 region for modernising its infrastructure and economy. Like in the other cases, they emphasised the role of cooperation in exchanging the best experiences and practices that would popularise ICT and reduce the gaps between the countries within the EU.

The V4 Prime Ministers underlined their involvement in strengthening mutual security and defence policy in the EU in the statement of December 15, 2016 (Visegrad Group, 2016). In their opinion, the main problem for security policy was to face the challenges consequent to cyber – and hiber – threats and develop and maintain defence capabilities by supporting innovations in technology and industries related to defence. Moreover, they indicated the role of public and private sectors in the economic growth and overall development of the whole EU, which positively affects the abilities to act in cybersecurity.

There also appeared the compilation of examples of cyberthreats which are both a challenge and a factor in shaping the existing cybersecurity policy included in the exceptional document of March 29, 2017, entitled „Joint Declaration of Intent of Prime Ministers of the Visegrad Group on Mutual Co-operation in Innovation and Digital Affairs” (Visegrad Group, 2017). The tasks formulated in that document were based on the belief that states rely on computer and communication systems, which create a vast space for privacy, the freedom of speech, communication, education, economy, and political and diplomatic practices. Managing so many areas and processes is a great challenge for the state as its bodies are responsible for introducing regulations to ensure security for the state institutions, local authorities, self-governments, or private actors involved in providing internet services.

It shall be noted that building up a mutual position in cybersecurity policy goes beyond the V4 countries. In order to support the development and implementation of new digital technologies as well as the management and protection of data, their Ministers of Foreign Affairs signed a joint statement with the representatives of Austria, Croatia and Slovenia on July 10, 2017 (Ministry of Foreign Affairs and Trade of Hungary, 2017). Their objective was to exchange information and experience indispensable for shaping cyber policy and building mutual cyber potential through joint exercises, training and research. Regional cooperation appeared to be a permanent element of the V4 policy and a core factor for future projects related to cybersecurity. The Ministers of Defence issued another joint declaration on March 29, 2018. They expressed their positive opinion on the extended cooperation between NATO and the EU. That was the first official statement of the V4 since the Warsaw Summit, when they presented their position on the key areas of politics, including cybersecurity (Visegrad Group, 2018a).

Since at least 2018, digitalisation has been recognised by V4 members as an important factor supporting the process of further European integration in the area of the Single Market and Economic and Monetary Union. Moreover, it is one of the pillars of the EU cohesion policy. In the declarations of the Visegrad Group members, the need for economic structures to adapt to the ongoing digital transformation resonates strongly (Visegrad Group, 2018b).

In the declarations, the Visegrad Group emphasises its position as one of the leaders in the EU forum in the discourse on the challenges facing the European community. A particular area requiring harmonious European cooperation is the security (Visegrad Group, 2018c).

The joint statements also note the deepening cooperation between the EU and NATO in areas such as countering hybrid warfare, cybersecurity, or operational cooperation in the Mediterranean Sea to tackle irregular migration (Visegrad Group, 2018d).

Worth noting is the link between cybertechnologies and the phenomenon of innovation, which determines their development in many areas of life. The need to involve resources from the International Visegrad Fund as support for joint digital projects is also indicated (Visegrad Group, 2018e).

The statements emphasise the need for a strong position of the EU in relations with external countries and organisations. However, a necessary condition for the EU to play a significant role in the global space is, according to V4 members, keeping up with the technological changes that are a condition for competitiveness in economic competition. The second area of the region’s potential is cooperation in V4 security and defence policy. Also, cybertechnology is seen as an effective tool against hybrid threats (Visegrad Group, 2018f).

Security cooperation of Central European states with EU institutions with active use and support of digital technologies was emphasised. Strengthening of such activities would take place within the framework of Frontex activities. Many formulated declarations from the V4 countries on the challenges facing the European community were rich in content, speaking about the need for joint actions within the framework of security policy, as exemplified by, among others, the „Joint Declaration of Interior Ministers” on June 26, 2018, or the „Declaration of the Summit of the Visegrad Group and Austria on the Establishment of a Mechanism to Assist in the Protection of the Borders of the Western Balkan Countries” of June 21, 2018 (Visegrad Group, 2018g).

The spread of digital technologies and their application in everyday life was also reflected in the Declaration on the taxation of digital services of October 5, 2018 (Visegrad Group, 2018h).

There is a noticeable evolution of digital policy towards cyber applications, for example, in transport. The use of cybertechnology also occurs in the context of using EU funds for research and development, as indicated, among others, in the Joint Declaration of Ministers Responsible for Economic Development of 14 October 2018 (Visegrad Group, 2018i).

In the discourse on cybersecurity among the V4 countries, one can notice an increase in defensive activities in the context of NATO membership and the declaration of an increase in spending on the armed forces, which translates simultaneously into defensive cyber capabilities, which fits into the nature of deterrence. An illustration of this phenomenon is the decisions made in Banska Bistrica on December 5, 2018, which concerned commitments to increase defence spending to 2% of GDP and which also had an indirect effect on strengthening the capacity for cyber defence (Visegrad Group, 2018j).

In 2019, once again, the V4 countries emphasised cybertechnology as an active factor supporting regional cooperation that improves the functioning of public services in transport, energy security, utilities, and human mobility (Visegrad Group, 2019a).

Thus, the perception of digitalisation within the framework of non-military security as well as innovativeness and efficiency of state functioning is present. This goal is to be served by cooperation in building infrastructure and eGovernment services based on, among others: user identification, access to data from base registers, and exchange of information between government agencies. Attention was also drawn to cross-border electronic services, which, with the legislative and financial support of the EU, are to help eliminate the digital divide between European regions. In the view of the Visegrad Group policymakers, it is a way to connect users and public administration across national borders, reflecting the idea of European integration (Visegrad Group, 2019b).

There is still a strong element of deterrence aimed at potential aggressors by emphasising the V4 countries’ membership in an economic and defence community like the EU and NATO. However, there is a noticeable strong emphasis on non-military threats, which, as the V4 defence ministers emphasise, have a key impact on the region’s security, such as illegal migration and terrorism. It is also important to emphasise the challenges facing the Central European region from the east and the south (Visegrad Group, 2019c).

Declarations on cyber security have increasingly taken on a professionalised nature. They were formulated based on expert analyses and also had the potential to set the direction of future actions while pointing out areas requiring special attention, such as migration, police cooperation, the fight against cybercrime, and crisis management. An example of such a common political position is the „Declaration of the V4 Interior Ministers of 21 June 2019" (Visegrad Group, 2019d).

Worth noting is the statement entitled. „Long-term Vision for Defense Cooperation of the Visegrad Group Countries" of June 24, 2020, which by its nature is a security strategy for the four countries. In this document, the emphasis is placed on the presence of NATO and EU structures, which provides an opportunity for the armed forces of the V4 countries to use the technological potential of Western allies. The need for continuous adaptation and modernisation in security policy with digital innovations is also emphasised (Visegrad Group, 2020a).

The challenges posed by the COVID-19 pandemic, not only to health care but also to other areas of the state and society, have forced many policymakers to redefine public services under the new conditions. In this context, V4 governments have highlighted the importance of digital technology for existing tasks performed by private sector actors and public institutions (Visegrad Group, 2020b).

The following year (2021) brings, in terms of V4 cooperation, further declarations indicating the strengthening of national capabilities in cyber defence of the V4 countries with simultaneous coordination of actions by EU and NATO allies (Visegrad Group, 2021a). The official statements pointed to the need to develop cyber capabilities that reflect the nature of the dynamic changes in cyber security. Other findings and remarks echo earlier assumptions, which can be assumed that the established norms and directions for developing the V4 countries' cyber security policies continue to be implemented based on membership in international organisations (Visegrad Group, 2021b).

Confirmation of the use of cyber technology as a common policy area of the V4 countries is the „Final Document of the Agenda 2030 V4+ Forum" of June 2, 2021. In the adopted tasks, in addition to such fixed issues as enhancing digital capabilities, strengthening digital transformation and accelerating the adoption of key digital technologies by V4 countries, attention was paid to the importance of public-private partnerships, which, according to the signatories, is the foundation of cyber security (Visegrad Group, 2021c).

The beginning of 2022 saw a series of meetings at the diplomatic level between representatives of the Central European region and other EU and NATO leaders over the growing military threat against Ukraine from the Russian Federation until the war finally broke out. Russia’s invasion of Ukraine on February 24, 2020 caused the military perspective on the perception of cyber security to dominate the public discourse in international politics. In addition, the V4 countries have attempted to expand cooperation with the United Kingdom under the V4+ formula in the area of, among other things, cyber security. An important concept in this statement is cyber resilience, which is seen as the ability to manage cyber and respond to malicious cyber activities, including the spread of disinformation (Visegrad Group, 2022).

As one can see from the quoted declarations, the big challenge before the V4 is to maintain harmonious cooperation and to hold a common vision of Central European security policy. Different perspectives and the lack of a common stance among the V4 governments on Russia’s aggression against Ukraine make one wonder about the political future of the Visegrad Group. As far as 2021 is concerned, the attitude of the V4 policymakers is a balance between military and non-military perspectives when interpreting cybertechnology.

While it is characteristic that many security meetings have dealt with threats and institutional and legal challenges in the EU-NATO cooperation space, there have been fewer meetings devoted to cyber-technology application in international security in recent years. Nevertheless, cyber threat issues were present in the political discourse among the V4 countries, but they were only a detailed aspect accompanying other topics. It is perhaps indicative that cybertechnology has already been accepted as a natural entry tool in international political discourse.

Conclusion

Considering the ongoing international debates on cybersecurity, we may say that there is nothing new in the subjects discussed by the Visegrad countries. However, their political declarations create a new quality in the cooperation in the region. The content of their declarations, consequent to the meetings of the prime ministers, the ministers of foreign affairs or the national defence ministers, corresponds to the programs launched for subsequent presidencies. Similarly, it can be seen from the joint statements and information officially released by the V4 policy makers and from the presidency reports that the countries paid more attention to cybersecurity matters with the flow of time. The joint statements of the ministers and the declarations made by the countries who have taken over the annual rotating presidency are the continuation of the previous political solutions and correspond to the priorities accepted for the cybersecurity strategies of the V4 countries.

There is also a discernible trend toward greater attention to the issue of cyber security, especially as hybrid threats intensify. However, it is worth noting that many statements and declarations are enigmatic, which is not a disadvantage when we consider, for example, the role of an individual presidency of a member state in creating a program that does not raise any controversies or tensions between the countries. Moreover, the broad concept of the covered topics facilitates obtaining a mutually held opinion. As a result, all member states may be involved in implementing specific projects, in contrast to the clearly defined roles and rules, making negotiation processes or opinions harder to change, which may raise conflicts and tension between the V4 countries.

The frequent official declarations and statements issued in the Visegrad Group’s international forum confirm their readiness to undertake the tasks prescribed by the EU and NATO directives and strategies about cybersecurity.

Therefore, in this context, balancing military and non-military dimensions in the perception of cyber security policy among Central European governments is understandable.

One characteristic aspect is that the meaning of cooperation is emphasised in many declarations or announcements made at the time of taking over the presidency of the V4, which may be seen as a standard behaviour in politics or as a base for the security policy of these countries.

Bibliogrphy

Berzsenyi D. (2015), *New dimension in V4 defense cooperation. A comparative analysis of the cybersecurity strategies of CECSP countries*, http://visegradplus.org/analyse/new-dimension-v4-defense-cooperation-comparative-analysis-cybersecurity-strategies-cecsp-countries, 12.10.2021.

Botond F. (2017), *Parallel Competences: The State of Cyber Security in V4*, https://visegradinsight.eu/parallel-competences-the-state-of-cyber-security-in-the-v4, 18.01.2022.

Christou G. (2018), *The challenges of cybercrime governance in the European Union*, „European Politics and Society”, vol. 19/3.

Czyż A., Kubas S. (2014), *Państwa Grupy Wyszehradzkiej: pomiędzy przeszłością a teraźniejszością. Wybrane aspekty polityki wewnętrznej i zagranicznej*, Katowice.

Foreign & Commonwealth Office (2012), *Hungarian leaders open cyber space conference in Budapest*, http://www.visegradgroup.eu/news/hungarian-leaders-open, 8.01.2021.

Kacała T. (2016), *Pojęcie bezpieczeństwa w dokumentach NATO i Grupy Wyszehradzkiej*, in: *Kategoria bezpieczeństwa w regulacjach konstytucyjnych i praktyce ustrojowej państw Grupy Wyszehradzkiej*, eds. A.Bień-Kacała, J. Jirásek, Ľ. Cibulka, T. Drinóczi, Toruń.

Kříž Z., Brajerčíková S., Urbanovská J. (2018), *Defense Co-Operation Between Germany and the Visegrad Countries*, „The Journal of Slavic Military Studies”, vol. 31/3.

Ministry of Foreign Affairs and Trade of Hungary (2017), *Joint Statement of the Ministers of Foreign Affairs of the Visegrad Group, Austria, Croatia and Slovenia*, http://www.visegradgroup.eu/calendar/selected-events-in-2017-170203/joint-statement-of-the-170710, 8.01.2021.

Ministry of Foreign Affairs and Trade of Hungary (2017), *Programme of the Hungarian presidency of the Visegrad Group 2017/2018*, http://v4.gov.hu/about-the-presidency, 20.01.2022.

Ministry of Foreign Affairs and Trade of Hungary (2021), *Hungarian Presidency 2021/22 of the Visegrad Group*, https://www.visegradgroup.eu/download.php?docID=470, 8.12.2021.

Ministry of Foreign Affairs of the Czech Republic (2014), *V4 Trust – Program for the Czech Presidency of the Visegrad Group (July 2015–June 2016)*, http://www.visegradgroup.eu/documents/presidency-programs/20152016-czech, 16.01.2022.

Ministry of Foreign Affairs Republic of Poland (2012), *Program Polskiej Prezydencji w Grupie Wyszehradzkiej lipiec 2012–czerwiec 2013*, http://www.visegradgroup.eu/documents/presidency-program, 15.01.2022.

Ministry of Foreign Affairs Republic of Poland (2017), *Raport Polskiego Przewodnictwa w Grupie Wyszehradzkiej (lipiec 2016–czerwiec 2017)*, https://msz.gov.pl/pl/polityka_zagraniczna/europa/grupa_wyszehradzka/polska_prezydencja_w_grupie_wyszehradzkiej_2016_2017, 8.11.2021.

Ministry of Foreign Affairs Republic of Poland (2020), *Polish Presidency of the Visegrad Group July 2020–June 2021*, https://www.visegradgroup.eu/download.php?docID=451, 8.12.2021.

Ministry of Foreign and European Affairs of the Slovak Republic (2014), *Dynamic Visegrad for Europe and Beyond – Program of the Slovak Presidency in the Visegrad Group (July 2014–June 2015)*, http://www.visegradgroup.eu/documents/presidency-programs/20142015-slovak#_4.%20DEFENCE%20AND%20SECURITY,%20JU-STICE%20AND%20HOME%20AFFAIRS, 8.11.2021.

Ministry of Foreign and European Affairs of the Slovak Republic (2018), *Slovak Republic 2018/2019 of the Visegrad Group*, https://www.visegradgroup.eu/download.php?docID=363, 8.10.2021.

Ministry of Foreign and European Affairs of the Slovak Republic (2015), *Bratislava Declaration of the Visegrad Group Heads of Government for a Stronger CSDP*, http://www.visegradgroup.eu/calendar/2015/bratislava-declaration, 8.11.2021.

Office of the Government of the Czech Republic (2016), *Joint Declaration of the Visegrad Group Prime Ministers*, http://www.visegradgroup.eu/documents/official-statements/joint-declaration-of-the-160609, 28.10.2021.

Office of the Government of the Czech Republic (2016), *Joint Statement of the Heads of Governments of the V4 Countries*, http://www.-visegradgroup.eu/calendar/2016/joint-statement-of-the-160919, 28.10.2022.

Olszewski B. (2016), *Perspektywy regionalizacji cyberbezpieczeństwa w ramach Grupy Wyszehradzkiej*, in: *Europa Środkowo-Wschodnia w procesie transformacji i integracji*, eds. H. Chałupczak, M. Pietraś, J. Misiągiewicz, Zamość.

Samoilenko S., Osei-Bryson K.-M. (2015), *Before and After Joining the European Union: The Impact of Investments in Telecoms on the Visegrád Group of Countries and Baltic States*, „Journal of Global Information Technology Management", vol. 18/2.

Senate of the Republic of Poland (2012), *Informacja na temat Grupy Wyszehradzkiej*, https://www.senat.gov.pl › plik › inf_wyszegrad, 18.01.2022.

UaPosition (2016), *Uncanny under-performer: fixing V4 digital gap*, http://www.visegradgroup.eu/uncanny-under-performer, 28.10.2022.

Urbański M., Dołęga K. (2016), *Regionalny wymiar bezpieczeństwa na przykładzie Grupy Wyszehradzkiej w kontekście przynależności do Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Sztuki Wojennej", vol. 1/17.

Valášek T. (2012), *General principles*, in: *Towards a smarter V4: How to improve defence collaboration among the Czech Republic, Hungary, Poland and Slovakia*, ed. T. Valášek, Bratislava.

Visegrad Group (1991), *Declaration on Cooperation between the Czech and Slovak Federal Republic, the Republic of Poland and the Republic of Hungary in Striving for European Integration*, https://www.cvce.eu/content/publication/2004/2/9/6e592602-5431-42fd-8e65-2274e294ad89/publishable_pl.pdf, 18.01.2022.

Visegrad Group (2012), *Joint Communiqué of the Ministers of Defence of the Visegrad Group*, http://www.visegradgroup.eu/calendar/2012/joint-communique-of-the, 8.11.2021.

Visegrad Group (2013a), *Martonyi welcomes success of cyber conference, urges further dialogue*, http://www.visegradgroup.eu/news/martonyi-welcomes, 8.11.2022.

Visegrad Group (2013b), *Joint statement of the V4 ministers of defence*, http://www.visegradgroup.eu/documents/official-statements/joint-statement-of-the, 8.11.2021.

Visegrad Group (2016), *Joint Statement of the Heads of Governments of the V4 Countries*, http://www.visegradgroup.eu/documents/official-statements/joint-statement-of-the-161215-1, 8.01.2022.

Visegrad Group (2017), *Joint Declaration of Intent of Prime Ministers of the Visegrad Group on Mutual Co-operation in Innovation and Digital Affairs*, http://www.visegradgroup.eu/calendar/selected-events-in-2017-170203/joint-declaration-of, 8.01.2021.

Visegrad Group (2018a), *Joint Communiqué of the Visegrad Group Ministers of Defence*, http://www.visegradgroup.eu/calendar/2018/joint-communique-of-the-180329, 8.09.2021.

Visegrad Group (2018b), *V4 Statement on the Future of Europe (V4 Heads of Government)*, https://www.visegradgroup.eu/calendar/2018/v4-statement-on-the, 12.11.2021.

Visegrad Group (2018c), *Joint Statement from the Official Meeting of the Speakers/ Presidents of the Visegrad Group Parliaments*, https://www.visegradgroup.eu/download.php?docID=343, 12.11.2021.

Visegrad Group (2018d), *Joint Communiqué of the V4 Defence Ministers*, https://www.visegradgroup.eu/calendar/2018/joint-communique-of-the-180329, 12.11.2021.

Visegrad Group (2018e), *Joint Declaration of the Ministers of Economic Affairs of the Visegrad Group Countries on the Future of Economic Cooperation*, https://www.visegradgroup.eu/download.php?docID=351, 12.11.2021.

Visegrad Group (2018f), *Stronger Together – Joint Statement of the Prime Ministers of the Visegrad Group*, https://www.visegradgroup.eu/download.php?docID=353, 12.11.2021.

Visegrad Group (2018g), *Visegrad Group and Austria Summit Declaration on “Setting up a mechanism for assistance in protecting the borders of the Western Balkan countries”*, https://www.visegradgroup.eu/download.php?docID=359, 12.11.2021.

Visegrad Group (2018h), *Joint Declaration of the Ministers of Finance on the Taxation of Digital Economy*, https://www.visegradgroup.eu/calendar/2018/joint-declaration-of-v4, 12.11.2021.

Visegrad Group (2018i), *Joint Declaration of Ministers Responsible for Transport*, Development and EU Funds, https://www.visegradgroup.eu/calendar/2018/joint-declaration-of-181213, 12.11.2021.

Visegrad Group (2018j), *Joint Statement from the North Atlantic Council Simulation*, https://www.visegradgroup.eu/download.php?docID=439, 12.11.2021.

Visegrad Group (2019a), *Conclusions of the Meeting of the Foreign Affairs Committees of the Parliaments of the Visegrad Group countries*, https://www.visegradgroup.eu/download.php?docID=383, 16.10.2021.

Visegrad Group (2019b), *Ministerial Declaration on the Mutual eGovernment Cooperation*, https://www.visegradgroup.eu/download.php?docID=427, 16.10.2021.

Visegrad Group (2019c), *Joint Communiqué of the V4 Defence Ministers*, https://www.visegradgroup.eu/download.php?docID=419, 16.10.2021.

Visegrad Group (2019d), *Joint Declaration of the V4 Ministers of Interior*, https://www.visegradgroup.eu/documents/official-statements, 15.10.2021.

Visegrad Group (2020a), *The Long Term Vision of the Visegrad Group Countries on Their Defence Cooperation*, https://www.visegradgroup.eu/download.php?docID=454, 15.10.2021.

Visegrad Group (2020b), *On-line meeting of Economic Affairs Ministers of the Visegrad Group during the Impact’20 Connected Edition*, https://www.visegradgroup.eu/calendar/events-in-2020/joint-communique-of-the, 15.10.2021.

Visegrad Group (2021a), *Summit of the V4 Prime Ministers with the President of the French Republic*, https://www.visegradgroup.eu/calendar, 11.01.2022.

Visegrad Group (2021b), *V4 meeting of Chiefs of Defence in Cracow*, https://www.visegradgroup.eu/download.php?docID=460, 15.12.2021.

Visegrad Group (2021c), *The 2030 Agenda Forum on-line conference of development/economy ministers organised in the V4+ Bulgaria and Romania format (with the participation of experts and business)*, https://www.visegradgroup.eu/download.php?docID=466, 15.12.2021.

Visegrad Group (2022), *Meeting of V4 Prime Ministers with the Prime Minister of the United Kingdom*, https://www.visegradgroup.eu/calendar, 16.03.2022.

Wierzbicki S. (2015), *Wojny cybernetyczne jako element niekonwencjonalnej konfrontacji międzypaństwowej. Pragmatyczna rzeczywistość, nieunikniona przyszłość*, „De Securitate et Defensione. O Bezpieczeństwie i Obronności*”*, vol. 2/1.

Dyskurs na temat cyberbezpieczeństwa w polityce państw Grupy Wyszehradzkiej 2011–2022

Strzeszczenie

Grupa Wyszehradzka (V4) jest jednym z najbardziej intrygujących przykładów współpracy państw w Europie Środkowej. Skupia ona Czechy, Węgry, Polskę i Słowację. Państwa te tworzą razem użyteczne ramy, które ułatwiają koordynację polityki na poziomie regionalnym. Wdrażają one również programy UE poprzez tworzenie sieci współpracy z państwami sąsiadującymi. Sieci te opierają się na wzajemnej geografii bezpieczeństwa i wspólnej kulturze strategicznej. Gdy w 2014 roku najważniejsze cele polityczne zostały osiągnięte, pojawiła się potrzeba wyznaczenia nowego kierunku wzajemnej współpracy. Okazało się, że wiele kwestii z zakresu polityki publicznej, takich jak infrastruktura transportowa, środowisko naturalne, turystyka, migracje, kultura czy edukacja, mogą być skutecznie realizowane na poziomie V4. Ponadto współpraca w dziedzinie wspólnej polityki bezpieczeństwa cybernetycznego jest obecnie szansą na pogłębienie współpracy między czterema krajami. Jednak zmiany w wykorzystaniu i rozpowszechnianiu cybertechnologii w przestrzeni publicznej zaczęły nabierać tempa dopiero w pierwszej dekadzie XXI wieku. Tym samym proces cyberrewolucji był zwiastunem zmian w zarządzaniu państwem. Niniejsze opracowanie zawiera analizę polityki cyberbezpieczeństwa państw Grupy Wyszehradzkiej w latach 2011–2022 zarówno w aspekcie militarnym, jak i pozamilitarnym.

Słowa kluczowe: Grupa Wyszehradzka, polityka cyberbezpieczeństwa, polityka pozamilitarna, polityka cyfrowa, innowacyjność technologiczna, rozwój cyfrowy

Article submitted: 12.04.2022; article accepted: 17.05.2022.