The Cybersecurity Strategy of the Visegrad Group Countries

MAREK GÓRKA

DE GRUYTER
OPEN

Politics in Central Europe (ISSN: 1801-3422)
Vol. 14, No. 2
DOI: 10.2478/pce-2018-0010

Abstract: *The Visegrad Group is the most dynamic transnational group in the Central and Eastern European region, connecting the Czech Republic, Poland, Slovakia and Hungary. Together these countries have established a useful framework for engaging with and coordinating policy at a regional level. At the same time, they are implementing EU programmes by creating cooperating networks with neighbouring countries based on their common security needs and strategic culture. This article focuses on the cybersecurity policies of the Visegrad Group countries. My analysis aims to reveal similarities and differences among these states that may be crucial for their future cooperation on a joint Central and Eastern European cybersecurity strategy. A cybersecurity strategy is a basic document created in a governmental context that reflects the interests and security rules at work in cyberspace. This document establishes the framework for future legislation, policies/standards, guidelines and other security- and cybersecurity-related recommendations. This study is also an attempt to assess the development of cybersecurity policies; as such, it provides an opportunity to hypothesise about the future of cybertechnology in the Visegrad Group region.*

Keywords: ***Visegard Group, Central and Eastern Europe, cybersecurity, cybertechnology***

Introduction: Analytic framework and research approach

Since the beginning of the 1990s, the countries of the Visegrad Group (the V4), i.e. Poland, the Czech Republic, Slovakia and Hungary, have been seen as models of transformation in Central and Eastern Europe, recording progress across

the political, economic and social spheres. These changes have occurred at the same time that technology has assumed growing importance. The modernisation of many areas of these countries was one of the conditions of their accession to the Western structures of the European Union (EU) and the North Atlantic Treaty Organization (NATO). However, changes in the use of cybertechnology only began to gain momentum in the first decade of the 21st century when these tools became widespread in the public domain. As such, the evolution of cybertechnology has been simultaneous with the process of Europeanisation and synonymous with changes to state management.

European integration, when considered in all its political, economic and cultural as well as technological and cybernetic dimensions, is a relatively long and complex process. This is especially clear if we take into account the evolution of social attitudes to democratic processes.

The first part of this article explores theoretical considerations, tracing the history of the Visegrad Group's cooperation and the main factors shaping security policies in the Central and Eastern European region. In the second part, I turn to the cyberstrategies of individual countries based on an analysis of published documents.

By analysing individual state cybersecurity policies, I aim to determine whether these strategies might pave the way for a new kind of cooperation within the V4 framework. Along the same lines, I ask whether neighbouring countries with similar historical traditions could jointly pursue solutions to the current problems in Europe.

Analysing the cybersecurity strategies of particular V4 states allows us to ascertain the extent to which governments are focusing on military and civil tasks. In this way, this study should help establish how individual governments define cybersecurity policy and whether this conflicts at all with democratic principles. The topic of cybersecurity itself leads us to ask whether digital transformation is a stage in the democratisation process that took place in Central and Eastern Europe in the '90s or it represents a separate and independent process that has different origins and is unfolding in another time scheme.

This study, thus, suggests how political factors can shape state cybersecurity. At the same time, it highlights similarities and differences in the cybersecurity strategies of the V4 countries.

My hypotheses hold that 1) cybersecurity policies reflect current processes taking place in the European political space and 2) the attitudes of individual states to security policy could affect the future of the V4's cooperation.

The starting point for this discussion is the concept of security policy, which aims to ensure the security of the state as the basic form of societal organisation. Such a policy also covers the state's involvement in creating international security as a way to prevent and counteract various types of threats (Gryz 2013: 46-47). Cyberspace has a fundamental role to play in this context and it adds

a dimension to state security policy. Cybersecurity, generally understood as part of politics, is, thus, crucial to this work. For our purposes, cyberspace is both a means of implementing state tasks and a virtual space where significant processes and phenomena take place from a state security perspective. Cybersecurity policy refers to the development of security policy that is specifically about cybertechnology.

The Visegrad Group

After the fall of Communism in 1989, the countries of Central and Eastern Europe began to adapt their political systems to liberal democracy. At the same time they had to define their main foreign policy goals. In 1991, Czechoslovakia, Hungary and Poland decided to create the Visegrad Triangle to enable their development and subsequent membership of NATO and the EU. After the dissolution of Czechoslovakia, this joint initiative became the Visegrad Group. For countries in this region, the most obvious and logical course for foreign policy was a new political and economic orientation towards the West.

By 2004, the Visegrad Group had achieved its most important political goals and the need arose for a new direction for cooperation. Many public policy issues, including transport infrastructure, the environment, tourism, migration, culture and education, had proven to be more effectively resolved at V4 level. Work on a common cybersecurity policy presented a chance for deeper cooperation among these countries.

On 13 May 2004, a new Visegrad declaration was adopted at the V4 summit in Kromeriz, replacing the document signed on the group's creation in 1991. The V4 representatives announced that the previous goals had been achieved and declared their readiness to foster their countries' cooperation as EU and NATO members. The Visegrad countries, thus, decided to work together on security policy-related issues, emphasising cross-border cooperation and the fight against terrorism and organised crime. Other matters raised included Schengen-based cooperation on illegal migration, critical infrastructure management and cooperation related to defence as well as the defence industry itself (Czyz 2007: 131–144).

In hindsight, it would seem, however, that the most important area of this cooperation was the sectoral dimension. In this regard, current V4 cross-border cooperation may focus on environmental protection, public transport or the development of regional infrastructure. The existence of reliable communication infrastructure remains critical, however, if there is to be effective communication among these states. Cybertechnology is, thus, key to the modernisation of this region, which hosts communication lines from Western Europe to the former Soviet republics. Something similar may be said of the building of energy and communication infrastructure between the North and the South,

which has served as the foundation for the Three Seas Initiative project (Törő – Butler – Grúber 2014: 364–393).

Currently the V4 group is an active regional alliance that allows its four member countries to speak with a single voice both within the group and in their dealings with other states and political entities. This V4 cooperation is based on the assumption that geographic proximity leads to a common understanding of security among these states, which share boundaries and neighbourhoods and therefore have more reasons to act together.

There is, thus, great potential for the V4 countries to pursue common challenges whether this means modernising the Central and Eastern European region or applying a broad European security and defence policy to aspiring EU member states (Rosteková – Rouet 2014: 181–193).

Among the big challenges that lie ahead for the V4 group members is the expansion of their security-related cooperation to deal with energy diversification and cybersecurity. Located on the outskirts of the EU, the Visegrad countries have close relations with neighbouring Ukraine and Belarus – a fact that translates into a major security policy goal. This issue has also been important in establishing the V4 states' new political priorities, which have gradually come to influence the EU's Eastern policy.

Main determinants of the Visegrad Group's security policy

Implementing security policy projects is not an easy task. Undoubtedly there are factors that make joint activities impossible and in some cases even rule out their discussion. One of these factors is the great disparity in the security policy budgets of different countries. In particular, the defence expenditure of Hungary, the Czech Republic and Slovakia is different from the level in Poland, a situation whch frustrates the fulfilment of NATO policy commitments.

As a result of EU enlargement on 1 May 2004, the EU faced a completely new situation at its eastern borders: the former Soviet republics of Belarus, Ukraine and Kaliningrad Oblast (part of the Russian Federation) became the Union's neighbours, and the same was also true of Moldova after Romania's accession in 2007. Meanwhile within the Visegrad Group, the eastern borders of Hungary, Poland and Slovakia became the EU's eastern border and, thus, the most important dividing line in Europe.

Central and Eastern European security policy has unquestionably been influenced by the many decades that these states experienced within the Soviet bloc. Another key factor is the belief of modern Kremlin authorities that the former Soviet countries belong to Russia's exclusive sphere of interest (Gerasymchuk 2014: 42–54). The V4 countries have strong economic connections with their eastern neighbours, especially Russia. In Central Europe, Russian enterprises continue to dominate the energy sector, which remains particularly attractive

to Russian investors given the use of key (road and rail) transport corridors and the supply of oil and gas.

The Visegrad Group has put great emphasis on various forms of energy security, which it sees as a safeguard for economic competition and a defence against Russian use of gas and oil supplies as a political tool. The V4's common strategic goals for security policy include the diversification of energy transmission routes, cooperation around security and environmental protection and providing transformation assistance to Ukraine. Cyberspace has emerged as another important issue that is beginning to shape V4 security policy (Marušiak 2015: 28–46).

Russia continues to be one of the main players on the global energy market. At the beginning of 2006, members of the European Union acknowledged the importance of this situation. Since then, the Russian–Ukrainian conflict has led to a reduction of gas supplies to the V4 countries. The former Soviet bloc countries are also struggling with the dependence of much of their military (army) equipment on Soviet era technologies (Sarvas 1999: 99–118). Turning to the main theme of the current study, Russian authorities have started to pursue a policy of confrontation through non-governmental organisations and separatist and national movements in neighbouring countries. These groups use cybertechnology to try to influence the political and economic situation in selected countries.

The Visegrad Group governments have repeatedly stressed their commitment to Ukraine's European integration. In order to strengthen the financial support from the Eastern Partnership, they introduced the Eastern Partnership Visegrad Programme, which aims to enhance Central and Eastern Europe regional cooperation through the International Visegrad Fund (Nováky 2015: 244–266). The V4's clear political objective is to promote a pro-European stance in Ukraine, which could work as a kind of safety belt and foster stability. This could result in further enlargements that would shift European borders to the east and distance Central European countries from the risky border area. At the same time, the V4 security policy threatens to create tension with Russia, which has invested substantially in keeping control of Belarus and Ukraine.

The Visegrad Group countries have rarely taken a common stand on the Russian Federation given their different interpretations of the threats posed and the significant variation in their perceptions of their national interests (Marušiak 2015). In contrast to Poland, the Czech Republic, Slovakia and Hungary have all been reluctant to treat Russia as an existential threat. The reasons for this are probably twofold. First of all, there are geopolitical factors at work since apart from Poland, none of the V4 countries has a direct border with Russia. Secondly, there is the existing protection available based on the principle of common defence in Article 5 of the NATO charter. This is seen as

a highly credible deterrent and guarantee of security against potential threats (Törő – Butler – Grúber 2014).

A final political issue worth returning to is the differences within the V4 on the question of increased military spending. With the exception of Poland, all of the V4 countries fall well below the NATO threshold that requires two percent of GDP to be dedicated to defence spending (Kuzel 2017). Central and Eastern European states' different assessments of events and threats may also reflect their perceptions of their own national interests, which are, in turn, affected by policies in Brussels and Moscow.

Selected "cyber incidents" in East-Central Europe

Widespread access to cybertechnology, which has almost unlimited applications across many areas of life, has increased the pressure to use it in the political sphere. The transformation of public space with the help of cybertechnology, which took place after 2000, ran almost parallel with the European integration of the V4 countries. It remains unclear whether the V4 countries, which were less economically and technologically developed than existing EU members, had greater difficulty in adopting and applying cybertechnology. And while this question cannot be resolved by this study, it is certainly one worth posing. In any case, we can assume that the implementation of cybertechnology has been affected by the organisational culture of public institutions and ongoing upgrades to economic infrastructure. On joining a more advanced community, the V4 countries had to accelerate their own development to keep pace with more advanced economies and those with more experience of the liberal marketplace.

At the outset, we may also presume that current threats resulting from the popularity of cybertechnology have been influential in reviving the debate about security policy. Moreover, this situation has had an impact on the attitudes and political decisions of the V4 states. The dynamics and effectiveness of the Visegrad cooperation have, thus, been affected by both internal and external factors. In this context, cyberspace does not fit easily into any existing categories.

Seen more broadly, cybersecurity policy is the result of cumulative factors, including economic and technological considerations, internal political ambitions and the geostrategic imperatives that shape the security policy of individual Visegrad states. It is therefore questionable whether the issue of cyberspace is actually bringing these countries any closer together. There are also questions about whether the V4 countries can adapt to new threats from cybertechnology, how they perceive cybersecurity and whether the documents of individual governments – that is, their cyberstrategies – can serve as the basis for a joint security policy.

In 2017, allegations were made about Russia's participation in the US general election, with some expressing suspicions that Russian hackers had infiltrated

the electronic component of the American electoral system. These events produced anxiety in EU member states that were planning their own elections and were, thus, similarly exposed to the risk of cyber attacks (Sussex 2017).

Each of the V4 countries has a relatively well-developed nationwide IT sector. However, the popularity of the Internet, and hence the large number of users, increases states' vulnerability to cyber-threats. Cybercrime is on the rise in V4 countries in line with trends elsewhere in Europe and around the world.

Between 2015 and 2017, the Visegrad Group countries did not experience serious cybercrime on the scale seen in states like Estonia. In this regard, Estonian state infrastructure, which is based on cybertechnology, was the target of a distributed denial of service (DDoS) campaign as early as 2007. That attack came in response to the government's decision to remove a Soviet statue in Tallinn (Haataja 2017). In contrast, in 2017, the global "WannaCry" attack revealed a significant weakness in the cybernetic security of EU countries, and thus, of V4 members (e Silva 2018). In this context, several incidents in Central and Eastern Europe should be mentioned.

The Czech Republic has in fact been the target of several notable cyber attacks in recent years. These have included DDoS attacks on media websites and the most popular search engine in the country (seznam.cz) as well as Prague Stock Exchange, the Czech National Bank and the two largest Czech mobile telephone networks (Kostyuk 2014). In September 2016, Czech intelligence services noted disinformation and cyber-espionage activities which, they alleged, were being carried out by Russians. In February 2017, a similar case was reported, and the head of the Czech diplomatic service, Lubomír Zaorálek, told reporters that Czech Foreign Ministry email accounts belonging to the minister and deputy ministers among others had been hacked. Zaorálek also observed that a foreign state was probably behind the attacks (Tait 2017).

In 2014, the Hungarian government was also the target of an extended campaign launched by a group of Russian hackers called "ATP28" who were indirectly linked to Russian intelligence. This group also directed its activities at Poland, Georgia and NATO (Jones 2014). In April 2016, Hungary again experienced several large-scale cyber attacks that paralysed the government's official website. These concentrated attacks revealed deficiencies in the state's cybernetic defences including an inability to protect fully against cyber-threats. While government websites were the chief target, these events exposed the huge risks facing private companies that might be exposed to similar attacks. As such, they brought home the need to take action to protect data (Cyber attack temporarily shuts Hungarian government website 2018).

Given the tense relations between Poland and Russia, it is safe to assume that Russia has been the main source of cyber attacks on the Polish IT system. In mid-September 2009, soon after Prime Minister Putin's visit to Westerplatte and just before the Sejm resolution of 17 September and the Katyń massacre, an

organised attack took place on the servers of Polish state institutions. According to the Polish media, these attacks recur quite often but thanks to the systems and protocols of the Governmental Response Team for Computer Incidents (CERT.GOV.PL), the security of government networks and websites has been ensured so far. Nevertheless, Poland's infrastructure is vulnerable to cyber attacks, as seen by a number of assaults on government systems in 2012. The scale of the cyber-threats was made clear by an attack on the ground-based IT systems at Warsaw Chopin Airport, which led to the cancellation of a dozen or so Polish Airlines flights, leaving around 1,400 passengers stranded (Babinski 2015).

Based on these examples, we may conclude that the V4 states are a vulnerable zone on the geopolitical and cybernetic map in the 21st century. Central and Eastern European countries are connected not only by roads and gas pipelines but also by a digital highway. The region is also highly important to organisations whose activities focus on cyberspace.

Cybersecurity strategies of the Visegrad Group countries[1]

A security strategy is a basic and starting document used for the formulation of regulations, standards, methodologies, rules, (security) policies and other tools needed to ensure cybersecurity. Because national strategies are an effect of the political environment, we may assume that this strategy reflects the unique political culture of the given state. A state's security system is not stable and to a large extent depends on processes taking place in the political, social and technological environment. Cybertechnology tends to develop rapidly so we should consider whether policy documents address dynamically changing conditions and provide ways for citizens and public institutions to adapt to cyberspace. The documents analysed in this section contain guidelines that may steer the next stages of security policy implementation from both legal and practical perspectives. They should also help us determine the powers and competences of the various institutions involved in basic state operations.

Arguably the future development of Visegrad Group is closely tied to the use of cybertechnology both in general political life and at the level of specific projects. To understand the factors shaping this cooperation framework, however, we need to turn to the cybersecurity policy positions of individual states. The sources of this analysis are documents developed by these countries and presented as their cybersecurity strategy. These documents set out the political plans of individual governments, thus allowing us to map out their present and future actions.

1 This analysis of the cybersecurity strategies of the Visegrad countries is based on the documents available at: https://ccdcoe.org/cyber-security-strategy-documents.html (12 March 2018).

The Czech national cybersecurity strategy[2]

According to the Czech Republic's cybersecurity strategy, modern cybertechnology presents a key challenge for the state, with particular consequences for any public and private entities that depend on information and communication tools. In contrast with the strategies of the other V4 states, the Czech document emphasises the critical role of information security, the loss of which, we are told, could have unpredictable consequences for society:

> The public and private sectors' dependence on information and communication technologies becomes ever more obvious. Information sharing and protection are crucial for the protection of security and [the] economic interests of the state and its citizens. Whilst the general public is mostly concerned about their personal data abuse or afraid of losing money and data, cyber security as such encompasses much more. Major risks include cyber espionage (industrial, military, political, or other), ever more often carried out directly by governments or their security agencies, organized crime in cyberspace, hacktivism, intentional disinformation campaigns with political or military objectives, and even – in the future – cyber terrorism. (p. 5).

The document stresses that upholding basic cybersecurity principles will require a proactive approach from not only the state but also its citizens. As such, achieving a culture of security is said to require awareness-raising among the general public as well as the private sector. Czech cybersecurity is, thus, tied to the ongoing development of not just durable information infrastructure but also an alert and educated society:

> Due to the open and publicly accessible nature of the Internet characterized by [the] absence of geographical borders, [the] security and protection of cyberspace demand a proactive approach not only from the state, but also from its citizens. (p. 6). The Czech Republic shall encourage [the] development of an information society culture through awareness raising among its citizens and private sector subjects. They shall have free access to information society services and to information on responsible behaviour and use of information technologies. (p. 8).[We need t]o train experts specialised in [...] active counter-measures in cyber security and cyber defence and in [an] offensive approach to cyber security in general. (p. 18).

2 National Cyber Security Strategy of the Czech Republic: available at https://ccdcoe.org/cyber-security-strategy-documents.html (10 March 2018).

The strategy notes that cybersecurity must go together with the protection of basic human rights and freedoms and the principles of a democratic state. In this regard, the open and neutral nature of the Internet, freedom of expression and privacy laws are said to guarantee the protection of civil liberties in cyberspace:

> In ensuring cyber security, the Czech Republic abides by fundamental human rights, democratic principles and values. It respects the Internet's open and neutral character, safeguards the freedom of expression, personal data protection and [...] privacy rights. It therefore strives for [...] maximal openness in access to information and for [...] minimal interference in individuals' and private entities' rights. (p. 9).

Another important element of the strategy is its classification of the threats arising through cyberspace. These threats include cybernetic espionage (divided into industrial, military, political and other kinds), cybercrime, hacktivism, disinformation and cyberterrorism.

The Czech strategy has four main parts: the first offers a vision of state cybersecurity with goals extending beyond the designated time period of 2015–2020. The second part sets out the basic principles that should shape cybersecurity policy. The third identifies specific cybersecurity challenges for the state and international organisations while the fourth describes the strategic goals whose achievement is crucial for Czech cybersecurity policy in this period. The document also stresses the state's obligations resulting from its role in international organisations and NATO's collective defence structures:

> The Czech Republic shall actively support its international partners in preventing and solving cyber attacks, fulfil its commitments arising from the membership in international organizations and from the collective defence within the NATO, and promote security in other states. (p. 7). The Strategy follows the principle of indivisible security; the Czech Republic's cyber security is thus indivisible from global, namely Euro-Atlantic cyber security. (p. 9).

Other sections highlight the need for state cooperation with the private and academic sectors on research and development concerning secure information and communication technologies. At the same time, the state confirms its support for the production, research, development and use of advanced technologies:

> To cooperate with [the] private sector and academia on research projects (including primary and experimental research) and on activities in technical disciplines and social sciences, at the national, as well as European and international, transatlantic levels. (p. 19).

The Czech Republic addresses cybernetic security comprehensively and so the document rightly observes that cyberspace is a global phenomenon transcending geopolitical boundaries. The authors note that the state and its agencies cannot be solely responsible for cybersecurity. Instead the active cooperation of the Czech public, private entities and entrepreneurs is required:

> The state and its agencies cannot bear the sole responsibility for cyber security; [...] active cooperation of the Czech Republic's citizens, private legal persons and individual entrepreneurs is needed. (p. 10).To ensure, in cooperation with [the] private sector, a cyberspace offering a reliable environment for information sharing, research and development and provide a secure information infrastructure stimulating entrepreneurship in order to support the competitiveness of all Czech companies and protect their investments. To provide education and raise the private sector's awareness of cyber security. Provide the private sector with guidance on how to behave in crisis situations, particularly during cyber incidents but also in their day-to-day activities. (p. 18).

As such, this area of security policy is said to require various forms of cooperation across the public and private sectors, civil society and the academy.

The Hungarian national cybersecurity strategy[3]

The Hungarian cybersecurity strategy focuses largely on the enforcement of national interests within the context of the state itself. Reading the document, we come away with a strong sense of its highly national concerns. Established targets of security policy (for example, guaranteeing economic security, adapting to technological innovation and ensuring international cybersecurity cooperation) must all be compatible with Hungarian state interests:

> The purpose of this Strategy is to determine national objectives and strategic directions, tasks and comprehensive government tools which enable Hungary to enforce its national interests in the Hungarian cyberspace, within the context of [...] global cyberspace. The strategy aims at developing a free and secure cyberspace and protecting national sovereignty in the national and international context [...] Furthermore, it aims at protecting the activities and guaranteeing the security of [the] national economy and society, securely adapting technological innovations to facilitate economic growth, and establishing international cooperation in this regard in line with Hungary's national interests. (p. 2).

3 National Cyber Security Strategy of Hungary: available at https://ccdcoe.org/cyber-security-strategy-documents.html (10 March 2018).

The document also lists tools for maintaining and improving the level of cybersecurity. The safe use of cyberspace, according to these authors, depends on the clear and effective coordination of government activities. This cooperation should be strengthened:

> However, due to the complexity of this area, these responsibilities can only meet the Government's objective regarding [the] free and secure use of cyberspace through [...] clear and efficient government coordination. Therefore, [...] central government coordination through the Prime Minister's Office shall be strengthened, a mandatory step for the coordinated and concentrated use of government and sectoral resources. (p. 4).

The introduction to the document sets out two specific goals for the cyberstrategy: it should manage threats and risks arising in cyberspace (understood here as both a location and the source of harmful processes) and it should enhance government coordination and resources. There are also references to values such as freedom, security and the rule of law and the need for international and European cooperation. In this way, the Hungarian strategy highlights the international materials that have served as signposts for the national document. Those sources include recommendations from European Parliament, documents from the European Commission and the High Representative for EU Common Foreign and Security Policy and the main tenets of the NATO strategy:

> At the same time, the Strategy is in conformity with the recommendations of the European Parliament for the Member States included in Decision No. 2012/2096(INI) on cyber security and defence, adopted on 22 November 2012, and with the joint communication published by the European Commission and the High Representative of the Common Foreign and Security Policy of the European Union on 7 February 2013 under the title "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Furthermore, the Strategy is in line with the Strategic Concept of NATO accepted in November 2010, the Cyber Security Policy of the Organisation adopted in June 2011 and its implementation plan, as well as with the cyber protection principles and objectives set forth in the documents of the NATO summits held on 19-20 November 2010 in Lisbon and on 20-21 May 2012 in Chicago. (p. 2).

Hungary's strategy also introduces and defines a concept of "Hungarian cyberspace," which includes both electronic information systems located within state territory and social and financial processes occurring within and through cyberspace. Those processes may result in data and information found in the Hungarian public domain or outside state borders but affecting the level of Hungarian security.

Significantly, the drafters understand the concept of cybersecurity in a military context. The idea of an "information war" is invoked, with cyberspace described as one of the most important theatres of modern warfare. Turning to the security standards of international organisations, the cyberstrategy appeals to a notion of community defence based on the common defence principle under Article 5 of the NATO charter. Hungary, thus, recognises the cooperation with NATO as key to cybersecurity:

> Hungary considers it highly important that cybersecurity has become an issue for collective defence under Article 5 of the founding treaty of NATO. (p. 3).

The strategy also notes the dynamic way that new technologies such as cloud computing and the mobile Internet develop leading to the continuous appearance of new security threats. Subsequent sections, thus, define cybersecurity as an ongoing and planned process of cyber-threat minimisation through political, legal, economic, educational and technical means. There is an emphasis on scientific development and relations with the scientific community. The unique role of this cooperation and its significance for security policy are made clear by the use of the word "strategic."

The Hungarian text also refers to civil liberties and human rights. These values are said to coexist with another important and often irreconcilable value: the right to security. This is apparent, for example, in the following statements about ensuring freedom from fear while also guaranteeing the protection of personal data and the free and safe use of cyberspace:

> This Strategy reflects the basic values enshrined in the Fundamental Law of Hungary, specifically freedom, security, [the] rule of law, international and European cooperation, in a separate field within security and economic policy. (p. 2). The protection of Hungary's sovereignty in [...] Hungarian cyberspace is a national interest, too; free, democratic and secure functioning of the Hungarian cyberspace based on the rule of law is regarded as a fundamental value and interest. In Hungary, the freedom and security of cyberspace is ensured through the close cooperation and coordinated activities between Government, academia, business sector and civil society based on their shared responsibility. (p. 3).

The authors highlight potential threats to the state that may arise from an information leak, maintaining that this is why the protection of state data is so essential. In this context, they also draw attention to the security of key cyberspace infrastructure. Another important issue, more marginal in other V4 countries' strategies, is the need to provide a safe online space for children and young people:

> Child protection. Hungary regards the creation and maintenance of an environment allowing the healthy development of children as a basic element of cybersecurity, and treats it as a priority in all affected areas, achieving, at the same time, the objectives of the European Strategy for a Better Internet for Children. Particular emphasis is laid on encouraging the creation of quality online content for young people, supporting awareness-raising and preparatory measures, the prevention of the harassment and exploitation of children, and the establishment of a secure online environment. For this purpose, Hungarian non-governmental organisations with a proven record in online child protection are regarded as key partners. (p. 6).

The document focuses on cooperation and the effective exchange of information. To this end, it calls for the creation of forums for effective cooperation including economic and scientific experts who should prepare and present recommendations and opinions on cybersecurity activities.

The strategy also underlines the importance of specialist security policy institutions. Implementation, it notes, should be entrusted to organisations with specific skills and powers. Those organisations should cooperate not just with one another, but also with other authorities responsible for data protection and classified information:

> These tasks affect organisations responsible for national security, defence, law enforcement, disaster management and critical infrastructure protection, as well as authorities responsible for electronic information security. (p. 5).

It is worth noting that the organisations responsible for cybersecurity policy are not clearly indicated in the document, and in practice, this provision may result in many controversial actions. The drafters stress the aim of expanding Hungary's role in EU and NATO cybernetic protection initiatives and cooperation as well as in UN and OSCE cybersecurity cooperation projects. Finally they announce the continuation and expansion of cooperation in the Central and Eastern Europe region.

The Polish cybersecurity doctrine[4]

The starting points for the Polish security strategy are provisions of EU documents. Like the other V4 countries, Poland sees the chance to strengthen its cybersecurity as a potential benefit of its membership of NATO and EU allied defence and cybernetic defence structures. The document, thus, emphasises

4 Cybersecurity Doctrine of the Republic of Poland: available at https://ccdcoe.org/cyber-security-strategy-documents.html (10 March 2018).

that any Polish provisions should be compatible with the strategies of allied states and international organisations like the EU and NATO:

> It is important that the evolution of security in Europe favours coherence and solidarity, as well as [the] development of defence capabilities of NATO and the EU, and not a decrease in Member States' ambitions related to this domain [...] [Objectives include] developing the defence and protection capabilities that would be adequate to the needs and capacities of the state, as well as increasing their interoperability within NATO and the EU [...] reinforcing NATO's readiness and ability to provide collective defence, as well as the coherence of EU's actions in the field of security; building a strong position of Poland in the two organizations. (p. 17).

Like its Slovak counterpart (see the discussion below), the Polish strategy assumes the need to establish a defining framework for processes and phenomena at the very outset. The document, thus, contains an explanation of the basic concepts that it uses when discussing the cybersecurity problem. The strategy's main goal is to ensure Poland's safety in cyberspace. In this context, however, cybersecurity is understood mainly in terms of the efficient functioning of key state and private sector infrastructure, particularly as this affects the financial, energy and health sectors. In other words, the focus is on the structure of the state and its economic environment, including the private sector, which directly determines security policy:

> Particular importance is attributed to: cooperation and coordination of protective actions with entities from the private sector – in particular the finance, energy, transport, telecommunications and health care sectors; conduct of preventive and prophylactic activities with regard to threats in [...] cyberspace; elaboration and use of appropriate procedures for social communication in this field; recognition of offenses committed in cyberspace, their prevention and prosecution of their perpetrators; conduct of information struggle in the cyberspace; Allied cooperation, also at the level of operational activities aimed to actively combat cyber offences, including the exchange of experience and good practice in order to increase the efficiency and effectiveness of domestic measures. (p. 21).

The strategy next highlights the co-existence of public and private entities in cyberspace. Entities in the financial, energy, transport, public health and advanced technology sectors are seen to be at particular risk, especially when it comes to data theft and attacks on their integrity or breaches of confidentiality related to the scope of their activities and availability ofservices. One of the few references to the social risks of cybertechnology appears in the discussion of

public administrative and financial services. In these realms, data and identity theft and the loss of control of private computers are all seen as serious threats:

> [The] improving position of Poland in the international arena, as well as its membership [of] NATO and the EU, result in an increased interest of foreign secret services in our country. Possible unauthorised disclosure or theft of classified information and other data protected by law may cause damage to the national security and interests of the Republic of Poland. (p. 10).

If cybersecurity policy is to be effective, the document notes that appropriate standards and good practices must be established to support private and non-public organisations (NGOs and scientific and research institutions) with cybersecurity risk management. There is also a need for preventative education and information to protect citizens from potential cyber- threats:

> Education for security comprises activities thanks to which citizens gain knowledge and skills related to security. It is provided within the framework of general and higher education, by central and local state institutions, as well as associations and non-governmental institutions. It is [a] priority [...] to increase social awareness in terms of the understanding of threats to [...] security and to shape competences [...] to respond to such threats in a deliberate and rational manner. (p. 21).

The Polish authors detect a high risk to national security coming from private operators and ICT service providers (especially transnational entities with decision-making centres abroad) given the limited state influence on their operations. Unregulated or improperly regulated relations between these entities are, thus, an important challenge for Polish cybersecurity policy. At the same time, the text notes a potential threat to democracy arising from efforts to balance two sets of values, i.e. the protection of personal freedom and personal rights in the virtual world on the one hand, and the use of adequate security measures on the other. This tension may complicate the introduction of effective new cyberspace security systems:

> [...] ensuring that citizens freely enjoy freedoms and rights, without detriment to the safety of others and of the security of the state, as well as assuring national identity and cultural heritage. (p. 12).

As technology has advanced, the counterparts of all traditional security threats have arisen in cyberspace. Of particular importance are those threats affecting critical state infrastructure controlled by IT systems. The development of information technology has led to a range of new external threats including

cybercrimes and cyber-conflicts with state and non-state entities, which may, in turn, produce cyber-threats. Cyberspace operations are, thus, now am integral part of political and military conflicts.

One contemporary external threat that Poland identifies in cyberspace is cyber-espionage. This refers to operations by foreign state services and non--state entities, including terrorist organisations. These entities use special tools to gain access to sensitive data. Other sources of danger include extremist organisations, terrorist organisations and organised transnational criminal groups whose cyber attacks may have ideological, political, religious, financial or criminal motivations:

> Together with the occurrence of new information and communication technologies (ICT) and the development of the internet, new threats have appeared, such as cybercrime, cyberterrorism, cyber espionage and cyber conflicts, with the participation of non-state entities, and cyber war understood as [a] confrontation between countries in [...] cyberspace. Current trends in the development of threats in the cyberspace clearly indicate [the] increasing influence of the level of security of the cyber domain on the general security of the country. Considering [the] increasing dependence on ICT, conflicts in [...] cyberspace may seriously disrupt the functioning of societies and states. (p. 13).
>
> The strategy outlines some of the challenges that Poland continues to face.

The country's most important cybersecurity tasks include developing and adopting a systemic approach, which will have legal, organisational and technical dimensions. Like the strategic proposals of all the V4 countries, the Polish document notes that the expansion of cybersecurity brings with it the potential for significant scientific collaboration. There is, thus, a need to create a support system for cybersecurity and education research and development, including projects to be implemented with scientific and commercial enterprises.

Another key point reiterated by all of the V4 states is the importance of ongoing development of the armed forces. Here the Polish drafters pay particular attention to intelligence and counterintelligence services:

> The substance of defensive actions is [the] continuous maintenance of readiness to effectively respond to threats to the independence and territorial integrity of the Republic of Poland. Complementary actions include active seizing of opportunities and anticipatory reduction of risks in the field of security by, inter alia, [...] participati[ng] in international efforts aimed [at] the reduction of sources of threats, including international security operations. It is achieved by means of: diplomatic efforts for security, military actions, intelligence and counterintelligence in the domain of defence, as well as functioning of the scientific and industrial defence capabilities. (p. 20).

As can be seen, Poland calls for the expansion of intelligence services' powers and capacities in cyberspace since this will enable them to neutralise foreign intelligence activity and be an effective counterespionage tool. In this context, cybersecurity policy must introduce a safe system of oversight, that is, an independent communications network to manage national security (this could be done from within the government communications network, for example). It will also be important to ensure the national control of ICT systems.

The Slovak cybersecurity concept [5]

The drafters of the Slovak strategy emphasise that cyber-threats are a constant accompaniment of everyday life. As such, cooperation with NATO allies is essential under Article 5 of the North Atlantic Treaty, which concerns collective defence and response coordination in the event of an attack on an alliance member. Like the Czech strategy, the Slovak document stresses the need for ongoing planning by raising political, legal, economic, social and technical-organisational awareness:

> At a state level, it is a system of continuous and planned increasing of political, legal, economic, security, defence and educational awareness, also including the efficiency of adopted and applied risk control measures of a technical-organizational nature in cyber space in order to transform it into a trustworthy environment providing for the secure operation of social and economic processes at an acceptable level of risks in cyber space. (p. 6).

The document also notes the lack of any coherent, formal cybersecurity terminology. As such, it includes an appendix with basic explanations of all the key terms used. The authors emphasise that cybersecurity issues are neither isolated to the Slovak Republic nor limited to one or a few segments of the socio-political environment. Rather, due to its global nature, cybernetic security is a general social phenomenon. This interdisciplinary approach to cybersecurity is also clear from the assumption that implementing cybersecurity policy requires continued cooperation among a wide range of entities: the armed forces and civilians, the state and the private sector and national and international bodies:

> Due to its global nature, cyber security is a society-wide phenomenon. Cyber security must be based on a complex approach, requiring intense joint use of information and coordination of activities on both national and international

5 Cyber Security Concept of the Slovak Republic: available at https://ccdcoe.org/cyber-security-strategy-documents.html (10 March 2018).

> levels. When building cyber security, it is necessary to pursue collaboration between the civilian and security units of the state, [the] public and private sectors, as well as national and international institutions. (p. 6).

The Slovak strategy emphasises its compliance with the cybersecurity principles set out in EU and NATO documents. It is also supported by references to existing Slovak laws, including provisions on defence planning, crisis situation planning and coordination and intelligence services:

> Cyber security is perceived as a key component of state security. The basic components forming and implementing the security system of the Slovak Republic are, according to the law: foreign policy, defence planning, civil emergency planning and coordination and intelligence services. (p. 7).

Like the cyberstrategies of other V4 countries, the Slovak document highlights the need for cybersecurity education. However, the text points out certain shortcomings that may affect the general level of knowledge about cyber-threats. Education, it notes, does not take place at the level of specialised fields of study. Instead it is mainly handled in discrete courses offered by selected educational institutions based on selected needs:

> What is absent is a Centre of Excellence that would focus on questions related to cyber security. The collaboration of the public sector with the private sector, academic institutions and civil society has not developed in the necessary scope and a framework of systematic, coordinated and efficient collaboration, mostly at a strategic level, is lacking. (p. 8).

As a NATO and EU member, Slovakia is, like all the V4 states, involved in drafting international strategic documents which also cover cybersecurity. This implies an obligation toapply the adopted documents and transpose them into national law. In this respect, the Slovak government is cooperating closely with the NATO Cybernetic Defence Excellence Center in Tallinn as well as the European Network and Information Security Agency (ENISA) and the European Cybercrime Center (EC3), which was established in 2013.

Slovakia's cybersecurity strategy describes a cybersecurity culture made up of basic elements that are also noted by other countries. The cybersecurity policy consists of several key activities. The first of these is establishing an institutional framework for cybersecurity administration. The second is creating and adopting a legal framework for cybersecurity. The third is maintaining and applying basic systems for secure cybernetic space administration. The fourth is supporting, preparing and implementing a system of cybersecurity education. The fifth is introducing and applying a communication risk control

system among interested parties. The sixth is active international cooperation and the seventh and final activity is supporting cybersecurity-related science and research.

Prevention is the key to the strategy and it entails the use of protective tools that will avert cyber-threats. In this context, the focus is not only public education but also intelligence activities that collect and evaluate intelligence data in order to predict and prevent certain cyber-incidents:

> [T]his involves the activation of entities active when solving crisis situations and if necessary, an early warning for the public, taking measures aimed at stopping the escalation of the crisis situation and the creation of conditions for a return to a stabilized situation. Offensive activities aimed at weakening and/or eliminating the cyber and even physical capacities of the attacker and to discourage the attacker from continuing in the attacks. Intelligence activities aimed at supporting defensive and/or offensive activities (e.g. intelligence information about the cyber capacities of the attacker). (p. 16).

The strategy demonstrates the system for responding to existing or potential threats, i.e. the steps taken to respond effectively to specific events. At the same time, it highlights the repair mechanism that should reduce the damage caused by cyber-attacks and restore the status quo:

> Removal of the consequences of the crisis situation and return to a stabilized state. Organizational, personnel, technological and other specific measures to avoid the reoccurrence of the crisis situation and/or threat. The nature of the fight against cyber attacks implies the necessity to use all security mechanisms and tools with efficient cross-sectoral and international cooperation. (p. 17).

In a characteristic move for strategies of this type, the document calls for the creation of a formal cooperation platform at national level. This structure should ensure representatives of the business and academic communities are involved in preparing and drafting government decisions. In particular, these representatives should provide opinions on the development and ongoing improvement of the cybersecurity system.

Conclusion

There are still some serious obstacles to the Visegrad Group's cooperation. On top of the historical, cultural and political-economic difficulties that the V4 states encountered especially during the transition from communism to democracy and the adoption of a market economy after the Cold War, they must overcome some specific obstacles to formulate a security policy. Ensuring

cybersecurity is now one of the most important tasks facing not only the V4 group but all states and public institutions.

The IT revolution has meant that post-communist countries and those which have long operated within the liberal economy are now confronting the same problem regardless of their pasts. Analysing the cybersecurity strategies of the individual V4 states reveals various answers and solutions to specific problems. At the same time, it highlights the different political ambitions and limits that come into play when addressing current challenges for the EU.

In their strategies, the V4 states are unanimous about their plans to strive to increase national cyber-defence capabilities and expand the resources for counteracting cyber-attacks. Each of these countries also makes use of international cooperation to exchange cybersecurity intelligence and technical assistance. Membership of NATO since 1999 and the EU since 2004 has led to closer cooperation between the V4 countries and the most advanced economies in the world on the areas of policing, combating terrorism and military training.

The Visegrad Group countries are also involved in an international alliance against the sexual exploitation of children, an EU-US initiative established to combat this type of crime. The current cybersecurity policies also comply with their responsibilities as members of NATO and the EU. They have been part of the Central European Platform for Cyberspace Safety since 2013 and base their security policies on cooperation with Europol, the European Cybercrime Center (EC3) and the European Network and Information Security Agency (ENISA) (Bossong – Wagner 2017).

A special hotline has been set up in each V4 country to enable anonymous reporting of harmful and illegal cyber-content. Such content includes child abuse, explicit material, racism, extremism and items inciting hatred and violence. Furthermore, each V4 state's cyber-strategy underlines the need for state cooperation with the private sector and the academic community. The second pillar of cooperation often stressed in these documents is international relations, which should include exchanges of knowledge and experience as well as warnings against possible threats.

At the same time, it is worth noting the differences and variations in some of the V4 states' approaches to cybersecurity. A characteristic feature of the Hungarian security system is the extensive scope it allows for the collection of telecommunications information without any judicial oversight. As such, the extent of state monitoring of cyberspace is unclear and this presents a threat to freedom of expression and the work of the mass media. Hungarian law permits the blocking or restriction of the Internet and other telecommunications services in the case of unexpected attacks, emergencies or national crises or for reasons of preventive protection. This could seriously disrupt business operations given the growing dependence on Internet communications networks. In

January 2016, the European Court of Human Rights ruled that these practices of telecommunications supervision violated the European Convention on Human Rights.

Similar allegations have been made about Poland's security system since Polish parliament adopted anti-terrorist legislation on 10 June 2016. One point of great controversy is the role of anti-terrorist operations, which use a variety of tools and techniques that may exceed the limits of ethics and the law. The disproportionate new law strengthens the powers of special services by restricting freedom of assembly, blocking Internet content, allowing discriminatory proceedings against foreigners and requiring the registration of prepaid cell phone cards (Górka 2016).

The reconciliation of the conflicting values of freedom and security appears to be impossible. Privacy and other civil liberties are often violated at times of crisis. When a situation threatens national security, the government often imposes restrictive laws and requires greater recognition and acceptance of secret services. It must also be said that the general wording in security strategies can leave great scope for their interpretation.

Cyber-attacks undeniably pose a major threat to state security. The growing problem of cybercrime may seriously reduce the efficiency of enterprises that rely largely on information technology. This is particularly important for the Central and Eastern European economy, which is still undergoing modernisation and is far more sensitive to cyber-incidents of various kinds. Cooperation on a security policy framework is therefore particularly important for the countries in this region. Decisive considerations will include the different interests, needs and motives of the individual states as well as their political ambitions to play a dominant role in the Visegrad Group.

References

Babinski A. (2015): State Activities in the Securing of Cyberspace. *Internal Security* 7 (2): 217–236.

Bossong, R – Wagner. B. (2017): A typology of cybersecurity and public-private partnerships in the context of the EU. *Crime, Law and Social Change* 67 (3): 265–288.

Cyber attack temporarily shuts Hungarian government website, „The Independent", 2 April 2018, available at https://www.independent.ie/world-news/europe/cyber-attack-temporarily-shuts-hungarian-government-website-34593756.html (20 April 2018).

Czyz, A (2007): What is the Future of the Visegrad Group as an Example of Regional Cooperation. *Studia Universitatis Babes-Bolyai. Studia Europaea* 52 (2): 131–144.

e Silva, K. K. (2018): Vigilantism and cooperative criminal justice: is there a place for cybersecurity vigilantes in cybercrime fighting? *International Review of Law, Computers & Technology* 32 (1): 21–36.

Gerasymchuk, S. (2014): Visegrad group's solidarity in 2004-2014 tested by Ukrainian crisis. *International Issues & Slovak Foreign Policy Affairs* 23 (1–2): 42–54.

Górka M. (2016): Freedom or Security? Contribution to the Discussion on the Example of the Law on Anti-terrorist Operations of 10 June 2016. *e-Politikon* 9, 49–79.

Gryz, J. (ed.) (2013). *Strategia Bezpieczeństwa Narodowego Polski.* Varšava: Wydawnictwo Naukowe PWN.

Haataja, S. (2017): The 2007 cyber attacks against Estonia and international law on the use of force: an informational approach. *Law, Innovation and Technology* 9 (2): 159–189.

Jones, S. (2014): Russian government behind cyber attacks, says security group. *The Financial Times*, 28. 10. 2014.

Kostyuk N. (2014): International and Domestic Challenges to Comprehensive National Cybersecurity: A Case Study of the Czech Republic. *Journal of Strategic Security* 7 (1): 68–82.

Kužel, M. (2017): The Investment Development Path: Evidence from Poland and Other Countries of the Visegrád Group. *Journal of East-West Business* 23 (1): 1–40.

Marušiak, J. (2015): Russia and the Visegrad Group – more than a foreign policy issue. *International Issues & Slovak Foreign Policy Affairs* 24 (1–2): 28–46.

Nováky, N. I. M. (2015): Why so Soft? The European Union in Ukraine. *Contemporary Security Policy* 36 (2): 244–266.

Rošteková, M. – Rouet, G. (2014): The Visegrád Group – a model to follow? *Politeja* 28 (11): 181–193.

Sarvas S. (1999): Professional soldiers and politics: A case of Central and Eastern Europe. *Armed Forces and Society* 26 (1): 99–118.

Sussex M. (2017): The triumph of Russian national security policy? Russia's rapid rebound. *Australian Journal of International Affairs* 71 (5): 499–515.

Tait, R. (2017): Czech cyber-attack: Russia suspected of hacking diplomats' emails. *The Guardian*, 31. 1. 2017.

Törő, C. – Butler, E. – Grúber, K. (2014): Visegrád: The Evolving Pattern of Coordination and Partnership After EU Enlargement. *Europe-Asia Studies* 66 (3): 364–393.

Marek Górka *graduated in Political Science at the the Nicolaus Copernicus University in Toruń/ Poland. He is Assistant Professor at the Faculty of Humanities, Koszalin University of Technology/Poland and author of works devoted to Israeli and Polish intelligence services, cyberbullying and cyberbullying among children and adolescents. His research interests include security policy, cyber security, terrorism, intelligence and counterintelligence services, internet sociology, electoral rivalry, charismatic leadership. He is author or co-author of more than one hunderd scholar publications. Among the most recent we can mention books: PO-PiS democracy. Competition between Civil Platform and Law and Justice in the years 2015-2017*

(2017), Global and local security policy problems (2017), Cyber security for children and youth (2017), Intelligence services as part of the Polish security policy (2016), Interview and counterintelligence in international politics at the turn of the 20th and 21st centuries (2016), Carnival and media as determinants of modern politics (2015), Mossad. Failures and successes of Israeli secret services (2015).
E-mail: marek_gorka@wp.pl