

Catalysts of Cyber Threats on the Example of Visegrad Group Countries

MAREK GÓRKA



Politics in Central Europe (ISSN 1801-3422)

Vol. 18, No. 3

DOI: 10.2478/pce-2022-0014

Abstract: *The article deals with cyber incidents that were recorded in the area of the V4 countries. It is important for the discussed topic to extract certain factors and with their help to characterise the conducted cyberattacks in terms of political motivations. The analysis tries to prove the existence of politically motivated cyberattacks. This, in turn, helps to determine the consequences of such cyber incidents. Moreover, the scale and magnitude of the cyberattack can be information to determine the strategic maturity and cyber capabilities of the adversary. Thus, the incidents that have occurred allow a cyberattack to be characterised in political terms and thus have value as information about ongoing conflicts in cyberspace that either reflect reality or foreshadow actions yet to come in the real world. Cyber operations can also be used as a tool to build a sphere of influence and exert political, economic and military pressure on a particular state.*

Key words: *cybersecurity policy; Visegrad Group; cyberattacks*

Modern times are often called in scientific literature ‘a digital era’, in which the range and level of interactions between countries, organisations and society are growing rapidly. Relationships between authorities and society are mostly based on digital communication, and therefore, policy is more susceptible to the threats coming from cyberspace (Lakomy 2010). There appears a question whether individual countries have a real reason for such worries, and if they are especially related to the Visegrad Group countries. When an answer to this question is positive, we should analyse the steps the countries’ governments have undertaken and investigate the dimensions of cybersecurity policy. The key

for the description of cybersecurity policy included in this chapter is a sequence of cyber incidents (Nye 2011) that have occurred in the V4 countries and at the international level.

Multiple research analyses on cyber conflicts and changing relations between countries indicate the importance of cyber technology development and emphasise its influence on the functioning of public space. Cyber activities undertaken by one country against another, or against a group of countries with the use of cyberspace, are currently thought to be a part of an acceptable competition and political cooperation (Carr 2016). In this context, the analysis investigates these processes with special reference to harmful activities performed by actors functioning in the competitive cyber environment (Trim – Upton 2016).

As a result of the widespread use of cyberspace, it has become a natural area for the functioning of many countries and, consequently, it has become more susceptible to intentional interferences that may paralyse the systems responsible for the everyday activities of public institutions. The growing presence of cyber technology in various fields of political, economic, social and cultural life has made the Internet an important communication tool, providing accessibility to a massive amount of information (Madej 2009). Continuous development and evolution of cyber technology have also changed the perception of threats.

Analysis of cybersecurity policy allows us to investigate existing processes and patterns of cyber conflicts that are mirrored in the data related to cyberattacks (Dunlap 2011). Therefore this article tries to respond to the question of whether a real scale and dynamics of occurrences of cyber incidents between political rivals corresponds to political divisions existing in the international space. Thus, assuming that cyberspace has become a natural field for political interactions, the author tries to verify the hypothesis that cyber incidents may reflect the international position of the V4 countries.

The article consists of two parts. The first one analyses incidents in relation to cybersecurity. On the basis of the data concerning the number and the most common types of incidents, the author provides the characteristics of cyber threats that have been reported in the V4 countries. There is also a signal that cybersecurity may be perceived as a challenge to all parties involved in public life. Because of that, in this part of the work special attention has been given to disinformation as a phenomenon that may constitute special threats, especially in the context of communication technologies enabling a quick exchange of information. These types of threats may bring unpredictable consequences to many participants of public life, and therefore they are an important part of the state security policy.

The second part of the article focuses on the impact of cyber events on activities undertaken within cybersecurity policy of the V4 countries and the description of political processes and phenomena consequent to the incidents in cyberspace. There is also an analysis of activities performed by the V4 coun-

tries that are aimed at obtaining management and more extensive control over cyberspace as well as an overview of the methods of exercising cybersecurity policy in response to the harmful acts existing in cyberspace and coming from hostile actors.

Cybersecurity and cyberthreats in the strategic perspective of V4 countries

‘Cybersecurity’ is a term widely used and overused, both in everyday language and in several fields of science (i.a. law, security sciences, computer science or management sciences). The semantic scope of this term has been defined differently both in a number of official documents and by individual scientists, hence a number of initiatives have been taken to analyse the term in several contexts and to develop an acceptable common understanding of it. There are a few texts devoted to this semantic problem, e.g. *The EU’s Cybersecurity Strategy for the Digital Decade* (European Commission 2020), *Definition of Cybersecurity – Gaps and overlaps in standardisation* (ENISA 2016) and official documents containing increasingly recognised definitions of cybersecurity, most notably *NIST Cybersecurity Framework* (NIST 2020) and *EU Cybersecurity Act i.e.: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013* (European Parliament 2019).

The concept of cybersecurity includes not only military aspects, but also political, economic and social aspects. Consequently, the EU as well as the member states (including V4) are gradually broadening the perception of threats. Therefore, it is important to analyse how certain governments perceive potential cyber incidents. Thus, countries leaning towards a military approach – due to their heavy reliance on information infrastructure – see the stable functioning of this area as a major condition of national security.

Any significant disruption of cyberspace, whether global or local, will have an impact on the security of economic transactions, the sense of security of citizens, the efficiency of public sector institutions, the course of production and service processes, and ultimately on national security in general (Poland 2019–2024: 3).

The topic of cyberthreats arises in the context of identifying the actions of other states’ services or the actions of non-state actors whose intent is to gain access to financial, energy or public safety systems in order to cause failure or other harmful consequences. Thus, in countries where military discourse prevails, the threat of cyberattack is seen as a top priority and is categorised as a military action that can pose a threat to the entire state. The V4 members cannot ignore the developments in the field of cybercrime, which is emphasised

in their strategies related to this area. Therefore, each national cyber security strategy also identifies cyberthreats among the phenomena that can affect the global security environment.

Cyberattacks are namely ideal tools for damaging political, business or other targets, and are also a strong tool for the attackers to enforce their own will. At the same time, it is often very difficult to identify the attacker, mainly in real time, which decreases the risk of a potential adequate response. These facts along with relative absence of geographic and similar limitations offer a great advantage to the attacker (Czech Republic 2018–2022: 3).

In civilian discourse, cybersecurity can be seen as protecting technology from criminal activity. In this case, cyberattacks are not seen as a national security threat, but as a shared risk among all institutions in the cyber sector. States representing this perspective see potential cyberthreats as a risk to a specific sector and emphasise the need to strengthen cyber defenses institutionally as well.

These efforts must be further fueled by closer cooperation among the NCOC, the private sector and the academic sphere. Cooperation in science and research activities will also be of crucial importance. Cooperation on the national level will also be backed up with appropriate strategic communications (Czech Republic 2018–2022: 13).

Governments that view cybersecurity policy from a civilian perspective define cyberthreats differently. An example of this is the interpretation of cyberattacks as activities whose primary purpose is to obtain financial gain or to steal sensitive information about specific institutions or individuals. This, in turn, shapes the state's top cyber priorities.

Just as security solutions evolve, the new techniques and methods of cyberattacks also develop. The opportunities for attackers and their tools are constantly evolving, and the response – appropriate security tools – may be late in many cases, or insufficient. Attackers respond in real time to emerging vulnerabilities in products and services, and are constantly improving in the use of social engineering methods. In addition, potential attackers have a time advantage. Preparing for an attack, preparing the tools, exploring the environment and phishing campaigns may potentially take a much longer time compared to the time available to defenders when responding to an ongoing attack. There is also a growing trend in the selling of attacks and attack tools (so-called Hacking as a Service), which allows less experienced attackers to perform sophisticated and devastating attack types (Slovakia 2021–2025: 9).

In this context, cybersecurity is viewed specifically by security risks only for a specific sector, such as finance, business, or science and research. The distinction between internal and external threats is also made in the Polish cyber security strategy. External threats listed in the doctrine include:

cyber crises and cyber conflicts involving state and non-state actors... cyber espionage, which involves actions carried out by foreign state services and non-state actors, including terrorist organizations, using specialized tools and aimed at gaining access to data that are critical to the functioning of state structures. The sources of threats in cyberspace are also extremist organizations, terrorist organizations, and organized transnational criminal groups... (Poland 2019–2024: 12).

In contrast, internal threats in the case of Poland include:

cybercrime, cyberviolence, cyberprotests or cyberdemonstrations of a destructive nature, disrupting vital public administration and private sector tasks (Poland 2019–2024: 10).

Meanwhile, both Slovakia and Hungary have a rather unclear and fragmented vision of the sources of cyberthreats. For example: Hungary focuses on technological vulnerabilities and their impact on the proper functioning of the country's economy without an in-depth analysis of their causes and the actors involved in the process. Hungary's National Cyber Security Strategy indicates that in addition to damage caused by external factors, inadequate regulation of ICT systems creates additional risks of harmful consequences.

In addition to the damage caused by external factors, the inadequate regulation of the operational security of the information and communication systems constituting cyberspace poses a further risk. Dynamic emerging new technologies, such as cloud computing or mobile Internet, lead to the continuous evolution of new security risks (Hungary 2013: 3).

The approach to the sources of cyberthreats is also relevant to the Czech Republic. Its security strategy identifies a wide range of cyber challenges, most of which, however, are criminal or technological in nature. These may include hacker activity aimed at causing technological failures or obtaining personal data or confidential information using botnets or DDoS / DoS attacks, etc.

As to the cyberdefence of the Czech Republic, the most important threat stems from the growth of offensive cyber capabilities in potentially hostile states. Other significant threats include a growing threat of cyberterrorism and the systematic strengthening of cybercrime structures as well as mutual interconnection of state and non-state attackers (Czech Republic 2018–2022: 3).

It is worth noting that almost all analysed states make a distinction between internal and external sources of cyberthreats in their strategic documents. However, the states from the civilian perspective do not further clarify this

distinction and focus mainly on the sources of threats that are most common in the security environment.

Cyberthreats as well as cybersecurity are constantly evolving. New targets and vectors of cyberattacks are constantly emerging, and are becoming more widespread, more frequent and more sophisticated. Some states and non-state actors resort more and more to pursuing their goals through unfair cyber activities. These can take several forms, including critical infrastructure attacks, cyberespionage, intellectual property theft, cybercrime and cyberattacks as part of hybrid threats. Cyberspace is increasingly becoming an area of strategic confrontation among states, reflecting a dynamic geopolitical environment and efforts to change the current international order. Technological innovations, including cybersecurity innovations, are becoming an instrument of confrontation and growing tensions in the political, economic and security fields (Slovakia 2021–2025: 5).

The potential sources of such threats are also fragmented and do not include only international actors from outside, but also internal phenomena resulting from malicious actions by hackers, hacktivists, criminal organisations, and also involve such accidental events as unintentional network disruptions. Civilian institutions in the Czech Republic, Slovakia and Hungary are responsible for monitoring cybersecurity threats and coordinating the response of state services to cyber incidents. The military approach is particularly emphasised in Polish documents, which tend to focus on foreign governments and hostile non-state actors as the main sources of threats.

The attackers may be criminal groups acting for profit, terrorist motives, as well as groups which may be backed by foreign states, and such actions serve the purpose of obtaining information, destabilising political or economic stability, or creating social discontent (Poland 2019–2024: 4).

The civilian approach is more prominent in the documents of the other V4 countries, which focus on harmful actions in the economic dimension, such as in Hungary, where it is indicated that:

Furthermore, it aims at protecting the activities and guaranteeing the security of 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 (Hungary 2013: 2).

Consequently, countries with a predominantly civilian approach are less likely to envision external cybersecurity threats. Incidents that may pose the greatest threats are defined in terms of economic or social fraud. Perceptions of the civilian or military context of cybersecurity are therefore closely related to how threats are interpreted.

An analysis of how individual states understand the sources of cyberthreats leads to the conclusion that cybersecurity is influenced by the actors carrying out harmful activities in cyberspace. Each of the V4 countries has gradually recognised the growing importance of the issue of cyberthreats and the urgent need to take a comprehensive approach to addressing the issue in order to protect the increasingly integrated critical infrastructure with cybertechnology.

When describing the studies examined, it is worth remembering that the content of the document does not always correspond to technological developments. Already at the outset, the strategies drawn up by the V4 countries can be seen to have this phenomenon. There are frequent cases of vague and very general formulations in such studies, thanks to which they cover a wide spectrum of phenomena occurring in cyberspace, including those that are not yet fully identified. Therefore, the following part of the article will attempt to identify cyberthreats occurring in the public space of the Visegrad Group countries.

Cyberattacks in Political Space

Cyberattacks have become an increasingly common tool of pressure used by both countries and private actors since the events of 2007 in Estonia. Cyberattacks may have an indirect impact on the opponent by harmful acts aimed at the economy or critical infrastructure. These cyberattacks which go with other physical operations or are independent, force the chosen actors to change their existing behaviour by putting pressure, blackmailing or other forms of leverage. In this context, a cyberconflict may be defined as a method of using digital technologies for the destruction of the chosen areas as well as a tool for changing political relationships between actors (Egloff 2017).

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

However, the competition in cyberspace differs from the traditional one and adopts various forms. It shows a great deal of uncertainty in respect of its range of consequences and sizes that may apply to a wider area of national security and contribute to crossing the traditional borders of conflicts. Most cyber activities may also be of symmetric nature. In this situation, actors weaker than their opponents reach disproportionately bigger profits than it might be expected when we consider their resources (Schmitt – Watts 2016).

Contrary to conventional operations, the use of cyber potential for carrying out an attack is relatively inexpensive, since there is no need to use such financial

means which are indispensable in the event of using physical tools. The actors launching cyberattacks cannot take over any territories, but they can interfere with critical infrastructure, paralyse the decision-making processes and gather intelligence information on conventional military powers (Procner 2015).

The relative easiness of carrying out cyberattacks and the lack of direct contact may enforce the position of non-governmental actors in relation to the stronger state actors. For understanding the methods of functioning of different organisations, it is necessary to measure the whole spectrum of possible threats. It shall be noted that despite a great number of hacker groups supported by the state, there are also groups presenting ideological motives such as hacktivists who challenge the state bodies in cyberspace (Jordan – Taylor 2014).

The previous cyber incidents did not lead to an open military conflict but only showed the competition in the international policy between the countries representing opposite political attitudes. However, cyber activities are getting more intense and raise their importance in the political space. The forms of acts in cyberspace directed by one country towards another become more common and natural method of pursuing policy. It may be presumed that when a specific actor is capable of interfering with the cyber systems of their opponent, they will do it.

The development of cyberspace has caused a revolution in security politics, which significantly affected interactions between states and other actors. Due to the power of cyber technology, the potential of cyberspace leads to the change in the existing international balance, including the political, economic and military position of a given country (Hoath – Mulhall 1998). Certainly, the growing number of cyberattacks aimed at the destabilisation of a state raises the need for continuous investments in security mechanisms.

Cyberspace is treated as a place of interactions between political actors as well as an area of establishing various organisations which pursue their objectives and shape political reality (Aleksandrowicz – Liedel 2014). However, it is difficult to decide whether cyberspace affects international relationships, or if it is only an additional space for political competition. In this context, investigations on the impact of cyber technologies on international relationships are of a complex and multi-dimensional nature.

The Sources of Information on Cyberthreats

Much information on cyberthreats that leaks to the public is residual and not complete, and therefore it is difficult to treat it as material giving a real image of the situation. Moreover, the reliability of these data may raise doubt due to the lack of transparent sources, so the analysis of cyberthreats is a significant challenge for their researchers. Information obtained from non-governmental organisations may be a great help.

One of the useful sources of information on this subject is the set of data that has been collected since 2006 by CSIS – the Center for Strategic & International Studies – that provides not only quantitative data but also information on characteristics of cyber incidents, such as targets, means and potential damages caused by harmful acts (CSIC 2020). Another source of information on cyberthreats is a set of data created by the non-governmental organisation CFR – the Council on Foreign Relations. The classification of cyber incidents included in their reports focuses mainly on the operations sponsored by states (CFR 2020).

The knowledge on the scope of cybercrimes and other acts of a political nature occurring in cyberspace, especially in the area of the Visegrad Group countries, is the information obtained from the interviewed personnel of the institutions working for the cybersecurity sector.¹ Another opportunity for collecting data on cyberattacks and their sources was an interview conducted with the staff of the European Union Agency for Network and Information Security (ENISA) during the international conference ‘Medea 2017’, which took place on 1st–8th September 2017 at the University of Crete in Heraklion, Greece (MEDEA 2017). The gathered data may also be a method of verifying the knowledge based on information given directly by institutions responsible for cybersecurity.

The research analysis and evaluation of incidents connected with information security in the V4 countries have been conducted on the basis of the reports and statistics provided by governmental teams responsible for the coordination of procedures applied in the case of cyber incidents. The study of the investigations included in this chapter focuses on cyberattacks reported and registered in 2013–2017.

Research Barriers to Cyberthreats Analysis

Research in the literature on the subject focuses mostly on cyber incidents directed against the states (or other actors) of Western Europe, and therefore the image of cyberthreats concerning Central and Eastern Europe is rather restricted (Sparks 2003). Moreover, there is a need to classify the cyber incidents reported in the V4 region if we want to obtain a more accurate description of their nature.

Another factor for the analysis is the fact that this problem usually appears at the time of their occurrence, and then it is described and popularised, but mostly at the level of opinion journalism. Consequently, many studies focus on the official information spread by state institutions or mass media, which often creates an inaccurate or false image of the attacks directed against a specific

1 The source of these data has been described in the first chapter of the work devoted to the budget expenditure related to cybersecurity. The undertaken investigation was carried out in 2015–2017, within the international project ‘Visegrad Group and the Central European Cooperation’ (No. 61450025), financed by the International Visegrad Fund.

country (Farwell – Rohozinski 2011). Besides, the cyberattacks of wider range are more likely to attract public attention, which may result in ignoring less significant ones. Therefore, this chapter tries to define the scope of harmful acts that have happened in the cyberspace of the V4 countries.

Official information and reports obtained from the state institutions have provided additional data on the subject. However, no matter how much effort is put into demonstrating the knowledge on the reported cyberattacks and into creating a corresponding complex data set on the subject, there is a risk that some incidents may pass unnoticed. Moreover, due to their confidential nature, most of them may never be revealed to the public. Both the attackers and their victims may have their reasons to keep such events secret. While the attackers maintain confidence in their offensive capability, the victims may be concerned about protecting such information from leaking. They may act in this way for fear of losing their reputation, as is usual with banking institutions.

In situations when the government and its services remain silent, the actors responsible for cybersecurity, as well as the mass media, do not inform about such incidents, a researcher is not able to note the threats on his own. This is especially true with regard to intelligence services involved in cybersecurity, as they act beyond public knowledge by their nature and do not usually reveal the offensive acts directed against the chosen targets. Exceptions have been the events which are difficult to be kept secret, i.e. blackout. Thus, to provide a realistic image of the incidents that have happened in the cyberspace of the V4 countries, the author interviewed the personnel responsible for monitoring the phenomena occurring in it. The confidential data collected on this subject allow us to understand the processes which are hidden from the public but determine cyber policy guidelines in the V4.

The created data set contributes to a wider understanding of cyber politics. Another important objective of this work is to provide characteristics of the acts undertaken in relation to cyberthreats by individual governments of the V4 countries. This chapter focuses on the description of the methods applied by the countries to create their approach to the more and more frequent cases of cyberthreats.

The major difficulty encountered in this analysis of cyberthreats is the fact that most cyber incidents occur without an evident reaction from the affected countries, which may influence research analyses undertaken in this area. Much information about the incidents that have happened in cyberspace does not leak to the public and the knowledge about their range is rather restricted. Amid multiple types of harmful acts in cyberspace there are also such digital interventions that have an insignificant impact on the functioning of state institutions but may be burdensome for cybersecurity systems. Due to this fact, they are not reported in official registers. Moreover, many state institutions are not aware of the threats or violation of their cyberspace and it is rather difficult to attribute

such acts to specific actors. It appears that there may be countries behind cyber incidents; however, they act indirectly, through intermediate bodies, to avoid possible accusations or their political liability (Kulesza 2009).

The problem with attributing cyberattacks to a specific author may result from the fact that computer networks are beyond jurisdiction of a given country (Rid – Buchanan 2015). Another thing is that cyber harassment may pass unnoticed even for a long time and before such attacks occur. Even when the harmful software is activated, their presence is difficult to determine. Therefore, many countries are not likely to admit their problems with identifying cyber offenders, since it might be seen as a manifestation of their helplessness. In other words, it may be presumed that some operations that occur in cyberspace are hidden because they reveal a weakness of a country or might be viewed as a disgraceful remnant of its existing policy. Furthermore, when such events are revealed, some confidential data may be unintentionally disclosed. Thus, many countries, no matter if they are attackers or victims of cyberattacks, try to hide them to evade liability. The consequent damages and their intensity might be limited and focused mainly on low-risk operations (Nye – Nye 2011). Another reason for keeping cyberattacks secret are efforts made by governments to hold back from reactions that might result in an escalation of cyberconflicts and bring more negative consequences.

With respect to cyberattack analysis, it is difficult to find whether an incident is a single event or it is included in a planned campaign. In addition, cyber operations may be a response to the acts that have not been disclosed in public or a reaction to the previous actions. When it is difficult to classify a cyber incident as a political problem, it shall not be excluded that it may indicate a new, unknown political competition.

A research challenge does not mean only registering cyber incidents, but first of all, attributing them to specific political conflicts. Any difficulties that are likely to appear may be resolved by relating them to the political tensions existing in the real world. Moreover, the analysis of technical advancement may help to identify a cybercrime perpetrator due to the fact that actions at a high technological level are most frequently performed by intelligence services of a specific country. Consequently, technological and political factors shall be considered in the process of attributing cyberattacks to a specific body.

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

Reaction to a Cyberattack as a Political Problem

The nature of cyberspace causes problems with analysing cyberattacks in relation to both scientific research and political acts. When specific incidents are concerned, there may be some doubt whether the victims can be certain about the source of the attack, and this knowledge is indispensable for retaliation. Another question is which types of cyberattacks can justify using military force within the right to self-defense.

Even if there is not enough evidence to support suspicions of a cyberattack, a formal report on such an event shall be given by the government (Sanger 2017). In this way the authorities determine their approach and respond to the inquiries coming from inside as well as outside the country.

A report published in this way is a publicly pronounced declaration that the government will implement previously accepted tasks. Such acts correspond to internal laws which impose obligations on the government in relation to security of the state and its cyberspace as well as to international regulations (under Art. 51 of the United Nations Charter) specifying that any acts of self-defense must be legitimised by recognising an attack and warning the opponents. They shall be aware that any further attacks may encounter retaliation and the incurred costs are likely to exceed the expected benefits (Nye 2017).

Policy-makers face the challenge when deciding about the methods of reactions to incidents in cyberspace. There appear some political dilemmas of whether a reaction shall involve physical, conventional or diplomatic tools, or cybertechnologies. Despite the question about the character of a retaliation, there is another one about the nature of a political cyber incident, i.e., motivation and context in which cyber operations are carried out. It often happens that even successful attacks cause only interim disruptions and system administrators can repair damages quickly and safely (Axelrod – Iliev 2014). However, in such cases, we may presume that the main objective of harmful acts is not unfavourable consequences but, first of all, testing cyber capabilities of the enemy in relation to resolving the problems caused by a cyberattack. The selection and usage of retaliatory measures depend on who has perpetrated the attack, whether it has been a politically motivated individual, a state or a group of people ordered and/or controlled by a state (Mačák 2016). It is also questionable if a state is likely to attack and completely damage an energy network, critical infrastructure objects, public facilities or state organisations of their opponent. For the fear of retaliation to an attack, an actor considering such an action may finally give up their plans.

The analysis of possible reactions to cyberthreats indicates an important role of social approaches that significantly affect decisions made by state authorities in relation to cybersecurity. Cyber incidents whose consequences are difficult or even impossible to be hidden from the public may trigger a reaction from

the party they have been directed to. Therefore, cyberattacks may not only be a means of pressure but also a factor increasing negative emotions and radicalising the political attitudes of their victims. Cyberattacks aimed at changing a state's policy may lead to the escalation of a conflict and growing radicalisation of previously manifested attitudes and opinions. Moreover, contrary to their intentions, they may contribute to the rising intensity of cybersecurity.

The key issues for cybersecurity policy are circumstances in which social moods may be in favour of using force in response to a cyberattack. In some circumstances, public opinion may play an important role in political reflections and discussions. First, the social emotions and attitude form the base for democratic leaders to take up decisions in response to current affairs. The use of force may be a consequence of social pressure. Second, the process of estimation and identification of an attack, which would help to find a responsible actor, may take a lot of time, often indispensable for making proper decisions by authorities acting under social pressure. Third, the lack of political agreement on reactions to cyberattacks may open new opportunities for the actors that have been on the margin of political life (Fontana 2017). Mass media also play an important role in the politicisation of cyber incidents, but they often deliberately overstate the meaning of a given subject in public debate (de Wilde – Leupold – Schmidtke 2016). Thus, threats and security are not objective factors and may constitute a tool for political confrontation.

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

Most cyber incidents are of low intensity and do not lead to escalation of the conflict both in cyberspace and the real world, which means that policymakers have adopted an attitude of restraint (by now). This thesis corresponds to the opinions based on the observations of western researchers who have analysed cyber incidents that occurred in the international space (Valeriano – Maness 2014). It shall be noted that no cyber incident has caused a conflict in the real world so far.

Another group of researchers is against this stance as they believe that modern societies, including the military forces of many countries, depend on communication and information networks and a destructive attack on the key systems may lead to military conflicts or to the decisive acts giving one of the involved parties a significant advantage over the other (Goldman – Warner, 2017).

On the basis of the interview with the staff of the services liable for cybersecurity in the V4 countries, it may be noted that there may be a third approach and

they are not mutually exclusive. It may be presumed that two opposite countries may tolerate cyber operations as far as they do not violate some boundaries or lead to unintended, damaging consequences. Further events may result in a situation of tolerance to cyberattacks unless they are accompanied by offensive and aggressive actions that destroy energy networks or infiltrate to take control over military units of the antagonists.

Another factor for restrictions imposed on cyber operations are the efforts made by an attacking party aimed at tightening the scope of actions to a chosen area or objects, which allows the attackers to foresee the consequences. This is intended to limit a possible escalation of the conflict, especially since the infrastructure of many countries is based on complex and interdependent networks directly affecting civilian population. Due to the threat of retaliation and potential harm to the civilians, cyber acts that have happened by now were of a selective nature.

The Consequences of Cyberattacks in the Area of Visegrad Group Countries

Cyberattacks are mostly intended to interfere with activities of critical infrastructure responsible for the proper functioning of institutions working in the public space. A good example of it is an e-banking system failure when thousands of clients cannot perform any operations online. Such a situation happened in 2015 when the Polish banking system was hacked and the hackers stole sensitive data of a few hundred clients, including account histories (cyberdefence24 2015).

A similar and equally harmful situation may happen when a state institution becomes the target of a cyberattack. In such circumstances, nationals may have a limited access to services provided by the state, as it happened in 2016 in the Czech Republic, when hackers infected a computer of a state official and sent false messages to EU institutions. Those messages contained a code which was later identified as spy malicious software. Such attacks are usually carried out with the use of botnets or zombies, i.e., computer networks controlled and directed by a hacker (Chamonikolas 2017).

Cyberattacks usually have a negative impact on the public sphere. In the event they occur between countries, they may mirror the existing political relations and affect further political actions. This was the case with Hungary in 2014, when the Hungarian government became the target of a long-term campaign started in cyberspace by the Russian organisation called ATP28, which also acted against the Polish and Georgian governments, as well as NATO, the European Council, OSCE, the diplomats and representatives of the US, British, Canadian and Norwegian military forces. Moreover, the Hungarians, in the result of an extensive cyberattack in April 2016, had to close the government's computer networks. The range of its consequences showed cybersecurity deficiencies and

the inability of the state to provide complete protection against cyberthreats. At such events, the authority of a political power and democratic legitimisation may be undermined (Paganini 2016).

Some incidents in cyberspace are of a specific psychological nature and their consequences are likely to greatly affect social opinions and emotions that have a decisive influence on the choices of political powers in democratic countries. In keeping with this, cyber incidents may force the state of destination to change the policy or the behaviour of its political elites. It seems that such incidents happen when both parties are in conflict or when one of them admits that existing diplomatic actions do not pursue accepted objectives.

As digitalisation becomes more and more common and related to everyday life, the increasing number of cyber incidents proves that cyber phenomena and processes become more political. This is shown by other examples illustrating the role of cyber incidents in politics. One of them may be hackery into energy systems of the EU countries (including Poland and the Czech Republic) in July 2014. It is thought that hackers from Eastern Europe are responsible for it. An analogical situation happened in December 2015 in Slovakia and Ukraine, where energy networks were closed due to cyberattacks from Russia. Although Slovakia's cybersecurity potential is higher than Ukraine's, the fact that Slovakia is a member of the EU as well as NATO makes it prone to the consequences of attacks coming from behind the eastern border.

The threats and capabilities of cyberspace are best illustrated by the example of the Prime Minister of the Czech Republic, whose email account and profile on Twitter were blocked by right-wing extremists in January 2016. Another significant event happened in September 2017 when Russian services hacked into systems of the private telephones of the NATO soldiers who stationed in Poland and the Baltic states.

If we take a closer look at the above cyber events, it is difficult to find sufficient evidence undermining the opinion that the contemporary policy in cyberspace is far from international interactions. The incidents that have happened imply that cyber operations can change the mindset of politicians as well as their nationals, which affects the way of interpreting policy in many areas. All in all, it may be thought that cyberspace can influence both the state's economic and political situation and affect the existing international relations. Harmful actions carried out with the use of cybertechnologies are the main reason for creating emotions and political unrest and may be a strategic issue for the state stability.

Factors Defining a Cyberattack as a Political Phenomenon for the V4 Countries

When analysing the examples of cyberthreats, we should bear in mind that not each incident is of a political nature. Thus, a research task is to distinguish

cyber incidents of a political nature from the others that may have an economic or social character. Therefore, we should consider five factors that enable us to assign the actual cyber incidents to the set of political actions. The analysis of these factors in the context of the attacks carried out by a states or private actors fills the existing empirical gap and facilitates a more detailed description of the phenomena occurring in cybersecurity policy (see: Table).

The first factor is information on the source of an attack. The key issue is whether the attack has come from the inside of the country or from beyond its borders. The intervention of a strange actor in cyberspace may be a political act. The set of data listed in the table illustrates the range of unauthorised and harmful incidents coming from outside of the attacked country. Defining a location of such an attack helps in finding the alleged perpetrator and estimate its range in the international context. Thus, the core of a reported incident may be seen in the perspective of the ongoing political conflict. Moreover, the analysis of its consequences responds to the question about the range and dynamics of political debates and the replacement of kinetic actions by cyberattacks.

The collected data indicate that amid the V4 countries, in the period from 2013 to 2017 Poland was the most vulnerable to cyberattacks from outside of its territory. The year 2014 marked a turning point in cyberthreats for all members of the V4 countries, as since then the increasing number of cyberattacks has been noted. Most of them comprised hacking into governmental resources, stealing confidential information or infiltrating data bases. It may be assumed that the above acts, as well as the growing activity of hacking groups, were consequent to the protests of the EU countries against the Russian aggression in Eastern Ukraine.

When identifying a cyberattack of a political nature, we should keep in mind that it is only a part of the interaction occurring between the actors in a conflict. This form of rivalry may be a continuation or reflection on competition between political actors.² The conflict of interests existing between at least two actors appears in different forms of tension in the international relations, including cyberattacks aimed at the competing parties. Although there is a little knowledge on an attacking actor and the liability for harmful actions cannot be clearly assigned, there are also some hints raising suspicions in relation to the role of specific actors behind the incidents occurred in cyber space.

The second factor is based on the presumption that the political significance may be attached to attacks only when a specific state or an actor liable for such incidents is believed to have been contracted by the present government. In this case, cyberattacks also have been noted more frequently in Poland than in other the V4 countries. It may be said that harmful cyberattacks clearly targeted

2 The data are listed in the appendix, in the table. 'The indicators of the cyber incidents of political nature in the V4 countries 2015–2020'.

towards a chosen country and their nature itself, which enables identification of an attacking country, have mostly a provocative character.

The third factor comprises acts performed by non-state actors involved in political issues. This type of actor is often used by the perpetrator to maintain credibility on the international stage and not to be related with cyber incidents. Moreover, some weaker states or non-state actors that have been passive in cyberspace by now, may also start using cybertechnologies for carrying out actions in line with their own political interests. This category of cyberthreats is pretty complex and demands a proper reading of data. It appears that in the case of Poland, despite the greatest number of reported cyber incidents of this category, which is 16,66%, this level is not dominant if we compare them to the other cyberthreats targeted at this country. This type of cyberattack carried out by the actors of political aspirations occur more frequently in countries such as Hungary (25 %), Slovakia (17,05 %) and the Czech Republic (19,98 %) than in Poland. This means that the members of the V4 may differently perceive the phenomena related to cyberthreats, even if they have a provocative character. These differences determine their consistency in creating and shaping cyber-security policy in the region.

The fourth factor comprises a set of political incidents targeted at the objects classified as state institutions or actors of critical infrastructure such as ministries, national legislatures, courts, civil administration, military and police facilities (Maness and Valeriano, 2016). In this category the greatest number of cyber incidents have been noted in Poland (58,70 %), and correspondingly in Slovakia (36,76 %), the Czech Republic (38,40 %) and Hungary (42,56 %). These differences are consequent to the unequal level of infrastructure security in the V4 countries. It can be deduced that as in the case of Slovakia, the Czech Republic and Hungary, the wider range of cyberattacks targeted at public institutions is not only evidence of the special activeness of strange actors, but also a consequence of the gaps existing in the critical infrastructure system which may be easily used by hostile organisations. Another symptom of the weakness of a state may be the inefficient monitoring of cyberspace and insufficient reactions of law enforcement authorities to minimise potential cyberthreats.

The fifth symptom is the relation of cyber incidents to historical reality, which results in an increasing intensity of cyberattacks in the public space. It follows that political and social emotions consequent to historical experiences of a nation become active as a result of cyber incidents and determine the perception of threats. In other words, the emotions existing in a social group may assign a specific political meaning to such events. Moreover, social tensions following stereotypes and political prejudices may expand the destructive effect of harmful phenomena occurring in cyberspace. The tragic experiences of the nations living in the Eastern part of Central Europe, and especially the historical events of the 20th century, make them particularly sensitive to facts from

the past. The case of Poland is exceptional as cyber incidents targeted at this country use social tensions, and the indicator of cyberthreats is the highest of all, 36,71 %. The other V4 countries have also noted similar, but less frequent acts, as is in the case with the Czech Republic 24,98 %, Slovakia (20 %) and Hungary (19,93 %).

Cybersecurity policy is a multidimensional phenomenon that comprises processes and factors creating the frames of political culture, starting from an individual computer user to cyber security specialists, computer programmers, consultants, bodies and organisations, most of whom transfer their activities to cyberspace.

Cybertechnology has changed relations between countries as well as the methods of political competition. Countries do not want or are not able to wage a war, so their activities are limited to the virtual space. The international cyber interactions depend on political factors and, therefore, the phenomena occurring in cyberspace may follow or mirror the actual political actions. Cyberspace may be treated as an instrument for conducting diplomacy and shaping international relations and other forms of the political pressure imposed by the government. Cyber instruments allow us to harass the opponent, to demonstrate our capabilities or force. It may be expected that ongoing conflicts and debates in cyberspace will become more intense in the future, and as a result, they will develop into one of the main determinants of security policy.

When cyberattacks become widely visible and noticeable, the government of an attacked state is forced to take a stance on the issue and take decisive reactions. The case of the V4 countries is a bit different if we compare them with the events of 2007 in Estonia. They have not experienced any cyberattacks that would be as harmful as those that happened in Tallin. Therefore, the intensity of their initiatives related to cybersecurity policy is at another level of advancement, as is shown in the results of the research illustrating the level of ICT development.

There is a problem of the attribution of task in cyberspace and, as it was noted during the presidential campaign in the US in 2016, we are still uncertain whether a cyberattack that neither causes any physical damage to society nor destroys critical infrastructure shall be recognised as an act of aggression justifying retaliation. It seems that reaction to harmful events, or even preventing them, is much more difficult in cyberspace than in the physical world.

Types of Cyber Incidents Reported in The Visegrad Group Countries

A part of this chapter comprises some examples of the incidents classified to a set of the harmful cyber incidents reported in the V4 Group. The aim of this research is comparison and assessment of incidents related to cybersecurity. The

analysis has been based on the reports of the Government Computer Emergency Response Team (GovCERT.CZ), the Government Computer Security Incident Response Team (CERT.GOV.PL) and the Computer Security Incident Response Team in Slovakia (CSIRT.SK). The source for this analysis of cyberthreats reported in the Visegrad Group was the data collected by the National Computer Security Incident Response Team in the Czech Republic (CSIRT.CZ), CERT Poland (ICERT.PL), the National Computer Emergency Response Team in Slovakia (SK.CERT.SK) and the Government Computer Emergency Response Team in Hungary (GovCERT-Hungary).

The above-named organisations have been created to provide security services such as development and research on cybersecurity, education, support for public institutions in protection against threats, registering and responding to incidents. These teams prepare yearly reports on the security of cyberspace, and according to the obtained results the number of incidents related to the security of information has rapidly increased and is expected to grow in the future. This work focuses on the incidents reported in 2013–2017. However, the comparative analysis of incidents is quite complex. The core problem in comparing cyberthreats reported in the V4 countries is the fact that the different teams (CERT or CSIRT) use different classifications for the same events (Aradau 2010). Moreover, as has been in the case with Slovakia, a different classification is used in relation to time periods within one country. Therefore, in the conducted research the data related to cyberthreats has been standardised, but the starting point was not a form of the used cyber instruments (such as botnet, crack, DoS/DdoS, Malware, Phishing, Spam, Trojan, Virus etc.), but the designation and target of the applied malware (see: table).

The first set reveals quite a high level of computer crimes in relation to the direct financial scams or stealing confidential information. Identity fraud or identity theft are also included in this set, since they are used for obtaining private information or stealing intellectual property. The greatest number of this type of crime was reported in Slovakia and Hungary – above 50% of all harmful incidents in cyberspace. Whereas Poland and the Czech Republic reported fewer number of such acts – above 40 %, although this number also seems to be quite significant.

The visible growth was also noted in relation to the offensive and illegal contents, especially during election campaigns led in all the V4 countries. Such behaviours may be considered hate speech targeted at politicians or other public individuals at a specific time. This was the case with Hungary in 2014, when they held a national election as well as to the European Parliament, and hate speech increased from 7,2 % to 9,9 % at that time.

A similar phenomenon was reported in the Czech Republic in 2013, during the election to the Chamber of Deputies when verbal aggressiveness reached as high as 10,3 % and in 2016 during the election to the Senate rising to 12,8 %.

In Slovakia in 2014, during the presidential election as well as the election to the European Parliament, the level of aggressive behaviour in cyberspace rose from 8,2 % to 9,7 %. That situation repeated itself in 2016, when during the parliamentary election the increase was from 10,1 % to 12,7 %.

These interdependences were also confirmed in the case of Poland in 2015, when election to Parliament and Senate took place at the same time as the presidential election, and the change in hate speech was significant and rose from 6,9 % to 12,2 %. All in all, political competition evokes much emotion which may be transferred to communication in cyberspace intensifying offensive and illegal contents.

The third classification concerns the damaging phenomena when there is a primarily unnoticeable, remote break into the area of activities conducted by a specific institution. Such attacks usually occur with the use of digital malware such as viruses, worms or logic bombs (Lisiak-Felicka 2017). They aim not only to paralyse the institution's activities, but also to infiltrate and steal confidential data, which may lead to the loss of confidence when such a situation is disclosed and to other serious problems in its functioning. The cases of the V4 countries show that in all four incidents neither the amount of malware detected in 2013–2017 nor the instruments used for cyberattacks changed, which may imply that only their targets differed.

Cybersecurity, at the most basic level, relies on protecting computer systems against cyberattacks, data breaches or their complete damage. The fourth and fifth set of data is related to these categories of breaches that illustrate the level of the state's resistance to cyberthreats. Some attacks targeted at paralysing communication and information networks working in transport, power providing, emergency services, health services, water management, food industry and farming, financial markets and public services have been reported since 2013 (Warner – Chapin – Matfess 2019).

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

The research has revealed a great deal of disinformation existing in cyberspace and undermining credibility of the government's policy or manipulating public opinions. The Internet users may (purposely or not) create and spread false information hiding their real intentions. The intensity of this phenomenon depends on a specific country, and as it may be noted in Poland in 2013–2017 this indicator almost doubled from 4,3 % to 8,5 %. The equally high level of

harmful acts was noted in Slovakia from 3,4 % to 5,3 %, in Hungary from 3,2 % to 5,9 % and the lowest level in the Czech Republic from 7,6 % to 9,4 %.

There was a change in the targets of cyberattacks that occurred in the V4 countries in the period from 2013 to 2017. The attackers were more interested in obtaining confidential information, taking control over critical infrastructure and manipulating public opinions by means of false data. These sorts of cyberthreats are a serious challenge to democratic countries and may be more dangerous to a country's stability than the failures of critical infrastructure caused by cyberattacks. It should be emphasised that disinformation and kinetic violence are not mutually exclusive and many acts in cyberspace aimed at breaching or paralysing the enemy's communication systems may affect public opinion.

Another important aspect are actions undertaken to protect computer networks against data loss or unauthorised acquisition of data by third parties (Minarik 2016). Cyber diversion also becomes a serious problem as it is usually consequent to data destruction or changes in digital values interfering or damaging network or functions of critical infrastructure.

Conclusion

The study shows that cybersecurity policies reflect real world phenomena and processes, which initiate actions that then find their place in cyberspace. The analysis also reveals a different way of interpreting cybersecurity (especially in the political and military dimensions), which leads to the conclusion that the activities carried out by the Czech Republic, Slovakia, Poland and Hungary in the field of cybersecurity are much more individual than communal in nature within the V4. Therefore, it can be suggested that there is a need for much more intensified activities that will create an integrated character of cybersecurity policy.

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

The increase in the number of cyber incidents is visible in all countries of the Visegrad Group, but most of them have been reported in Poland. The CERT or CSIRT teams in these countries report the growing number of incidents related to data transmission and the security of storage facilities. Cyber activities are more and more frequently aimed at affecting public opinion, which leads to undermining the enemy's credibility. They comprise such acts as leaking confidential information, critical and harmful publications on the Internet and creating special websites promoting ideology of political groups, often representing extremist views. Cyberthreats may be perceived as the use of technology for destructive actions influencing or modifying political processes (Lin 2012).

Table: The most frequent cyber incidents reported in 2013–2017³
(data given in %)

Country	Poland				
Time	2013	2014	2015	2016	2017
Computer crimes (social and economic)	42,6	42,4	40,8	43,7	44,3
Offensive and illegal content	7,5	6,9	12,2	7,8	8,6
malware	17,7	18,1	17,3	16,5	17,2
Breaking in attempts	7,5	6,9	7,2	7,7	8,1
Breakings	2	2,3	2,7	3,4	3,9
Disinformation	4,3	6,4	9,3	6,8	8,5
Attack on security of confidential data	5,9	6,5	8,1	7	7,4
Others	12,5	10,5	2,4	7,1	2
Total	3445	4390	5185	6240	7046

The consequences of attacks on communication systems determine political attitudes and emotions, especially in democratic systems (Hersh 2010).

The characteristic features of cyberthreats are the pace of changes and innovations that is much faster than in the case of harmful phenomena reported in physical world, technology that is much more decentralised at present and may constitute an instrument of destabilisation in a country, and last but not least, many more actors involved in harmful acts in cyberspace than in a real conflict. Reacting to various cyberthreats or the attempts to marginalise them is not only a challenge for many governments but also will generate difficult problems.

All in all, the data collected by CERT or CSIRT teams are important from the scientific point of view as well as for the institutions liable for cybersecurity of the state. Considering the data related to the most frequent cases of cyber incidents, we may find appropriate preventive measures. However, the comparative analysis of data is quite complex due to the lack of both standardisation of reports and classification of incidents in the Visegrad Group countries.

³ The author's analysis based on the reports of CERT of the V4. The number of officially registered incidents (based on reports and statistics of govCERT.PL., CERT.GOV.PL, CSIRT.CZ, CERT.PL) <https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map>

Czech Republic					Slovakia					Hungary				
2013	2014	2015	2016	2017	2013	2014	2015	2016	2017	2013	2014	2015	2016	2017
44,2	44,1	43,5	42,4	42,7	50,3	50,1	51,4	51,7	52,6	48,3	48,9	50	51,5	52,3
10,3	10,7	10,2	12,8	9,6	8,2	9,7	10,1	12,7	9,5	7,2	9,9	9	9,2	9,5
14,3	14,7	13,9	13,8	15,1	9,7	10,6	11,9	11,4	10,7	13,2	13,4	13,9	14,1	13
6,7	5,9	6,3	6,8	7,6	6,3	6,4	7,4	6,3	7,3	5,8	6,2	6,6	6	7,1
1,5	1,9	2,2	2,3	2,5	3,5	4,7	5,4	5,8	5,6	3,9	4,5	4,8	4,8	5,2
7,6	8,9	7,7	7,4	9,4	3,4	4,1	4,5	5,1	5,3	3,2	4,4	4,8	5,5	5,9
6,8	7,4	6,4	6,8	7,8	4,1	5,3	6,4	5,3	6,1	2,4	3,5	3,9	4,2	4,8
8,6	6,4	9,8	7,7	1,7	14,5	9,1	2,9	1,7	2,9	16	9,2	7	4,7	2,2
1358	1701	2550	3815	5410	294	348	361	346	423	861	1097	1296	1560	1761

References

- Aleksandrowicz, T. R. – K. Liedel (2014): 'Społeczeństwo informacyjne – sieć – cyberprzestrzeń. Nowe zagrożenia', in K. Liedel, P. Piasecka and T.R. Aleksandrowicz (eds.), *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji*, Warsaw: Difin, 9–38.
- Aradau, C. (2010): Security That Matters: Critical Infrastructure and Objects of Protection. *Security Dialogue* 4(5): 491–514.
- Axelrod, R. – Iliev, R. (2014): Timing of cyber conflict. *PNAS* 111(4): 1298–1303.
- Carr, M. (2016): *US Power and the Internet in International Relations. The Irony of the Information Age*, London: Palgrave Macmillan.
- CFR (2020): Cyber Operations Tracker. Available at <https://www.cfr.org/interactive/cyber-operations> (June 212020).
- Chamonikolas, K. (2016): Czech Republic Says Russian Hackers Were 'Very Active' There in 2016. Available at <https://www.bloomberg.com/news/articles/2017-10-24/russian-fancy-bear-hackers-seen-very-active-in-prague-in-2016> (18 June 2020).
- Christou, G. (2015): *Cybersecurity in the European Union. Resilience and Adaptability in Governance Policy*, London: Palgrave Macmillan.
- CSIC (2020): Significant Cyber Incidents. Available at <https://www.csis.org/programs/cybersecurity-and-gov-ernance/technology-policy-program/other-projects-cybersecurity> (29 June 2020).

- cyberdefence24 (2015): Perpetrator of cyber attack on Plus Bank in hands of police. Available at <https://www.cyberdefence24.pl/sprawca-cyberataku-na-plus-bank-w-rekach-policji> (18 June 2020).
- Czech Republic 2018–2022 (2018): Cyber Defence Strategy of the Czech Republic 2018–2022. available at: <https://ccdcoe.org/library/strategy-and-governance> (12 April 2022).
- de Wilde, P. – Leupold, A. – Schmidtke, H. (2016): Introduction: The Differentiated Politicisation of European Governance. *West European Politics* 39(1): 3–22.
- Dunlap, C. (2011): Perspectives for cyber strategists on law for cyberwar. *Strategic Studies Quarterly* 5(1): 84.
- Egloff, F. (2017): Cybersecurity and the Age of Privateering. In: *Understanding Cyber Conflict. 14 Analogies*, edited by George Perkovich and Ariel E. Levite. Georgetown: Georgetown University Press, 231–247.
- ENISA (2016): Definition of Cybersecurity – Gaps and overlaps in standardisation: available at: <https://www.enisa.europa.eu/publications/definition-of-cybersecurity> (12 April 2022).
- European Commission (2020): The EU's Cybersecurity Strategy for the Digital Decade: available at: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> (8 April 2022).
- European Parliament (2019): EU Cybersecurity Act i.e.: Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013: available at: <https://eur-lex.europa.eu/eli/reg/2019/881/oj> (10 April 2022).
- Farwell, J.P. – Rohozinski, R. (2011): Stuxnet and the Future of Cyber War. *Survival* 53(1): 23–40.
- Fontana, I. (2017): Disentangling the cyber politics-cyber security nexus: the new challenge of global politics. *Global Affairs* 3(1): 2–4.
- Goldman, E. – Warner, M. (2017): Why a Digital Pearl Harbor Makes Sense and Is Possible. In: George Perkovich and Ariel E. Levite *Understanding Cyber Conflict. 14 Analogies* G. Georgetown, Georgetown University Press, 147–157.
- HershOctober, S.M. (2010): The Online Threat, Should we be worried about a cyber war? available at: <https://www.newyorker.com/magazine/2010/11/01/the-online-threat> (29 June 2020).
- Hoath, P. – Mulhall, T. (1998): 'Hacking: Motivation and Deterrence', *Computer Fraud and Security* 4: 16–19.
- Hungary 2013 (2013): National Cyber Security Strategy of Hungary 2013. available at: <https://ccdcoe.org/library/strategy-and-governance> (12 April 2022).
- Jordan, T. and P. A. Taylor (2014): *Hactivism and Cyberwars Rebels with a cause?*, London, New York: Routledge.
- Kulesza, J. (2009): State responsibility for cyber-attacks on international peace and security. *Polish Yearbook of International Law* 29: 139–151.
- Lakomy, M. (2010): Znaczenie cyberprzestrzeni dla bezpieczeństwa państw na początku XXI wieku. *Stosunki Międzynarodowe – International Relations* 3(4): 59.

- Lasota, A. (2014): Cyberatak jako wstęp do cyberwojny. *Studia Mazowieckie*, 4: 65–78.
- Lin, H. (2012): Escalation dynamics and conflict termination in cyberspace. *Strategic studies quarterly* 6(3): 48.
- Lisiak-Felicka, D. (2017): Information Security Incidents: A comparison between the Czech Republic and Poland, 20th International Scientific Conference. *Economic and Social Development*, Prague.
- Mačák, K. (2016): Decoding Article 8 of the International Law Commission's Articles on State Responsibility: Attribution of cyber operations by non-state actors. *Journal of Conflict and Security Law* 21(3): 408.
- Madej, M. (2009): Rewolucja informatyczna – istota, przejawy oraz wpływ na postrzeganie bezpieczeństwa państw i systemu międzynarodowego. In: Marek Madej and Marcin Terlikowski *Bezpieczeństwo teleinformatyczne państwa*, Warsaw: Polski Instytut Spraw Międzynarodowych, 17–40.
- Maness, R.C. – Valeriano, B. (2016): Cyber Spillover Conflicts: Transitions from Cyber Conflict to Conventional Foreign Policy Disputes?, Conflict, Security and Technology. In: Karsten Friis and Jens Ringsmose: *Conflict in Cyber Space. Theoretical, Strategic and Legal Perspectives*. London: Routledge, 45–64.
- MEDEA (2017): The 5th International Interdisciplinary Symposium On Art, Science, Technology Medea 2017. Available at: <https://uap.edu.pl/wp-content/uploads/2017/09/Medea-2017-eng.pdf> (21 June 2020).
- Minarik, T. (2016): National Cyber Security Organization: Czech Republic: available at: <https://ccdcoe.org/multimedia/national-cyber-security-organisation-czech-republic.html> (29 January 2020).
- NIST (2020): NIST Cybersecurity Framework: available at: <https://www.nist.gov/cyberframework> (10 April 2022).
- Nye, J. (2011): Nuclear lessons for cyber security? *Strategic Studies Quarterly* 5(4): 21.
- Nye, J. (2017): Deterrence and Dissuasion in Cyberspace. *International Security* 41(3): 51.
- Nye, J. and J. S. Nye (2011): Nuclear lessons for cyber security? *Strategic studies quarterly* 5(4): 22.
- Paganini, P. (2016): The website of the Hungarian Government temporarily shut by cyber-attack: available at: from <https://securityaffairs.co/wordpress/45898/hacking/hungarian-government-website.html> (18 June 2020).
- Poland 2019–2024 (2019): Poland's Cyber Security Strategy 2019–2024: available at: <https://ccdcoe.org/library/strategy-and-governance> (12 April 2022).
- Procner, W. (2015): Wywiad i kontrwywiad w procesie strategicznej dezinformacji. *Secretum* 1(2): 40–57.
- Rid, T. – Buchanan, B. (2015): Attributing Cyber Attacks. *Journal of Strategic Studies* 38(2): 7.
- Sanger, D. (2017): Cyber, Drones, and Secrecy. In: *Understanding Cyber Conflict. 14 Analogies*, edited by George Perkovich and Ariel E. Levite. Georgetown: Georgetown University Press, 61–78.
- Schmitt, M. N. – Watts, S. (2016): Beyond State-centrism: International Law and Non-state Actors in Cyberspace. *Journal of Conflict and Security Law* 21(3): 595–611.

- Slovakia 2021–2025 (2021): The National Cybersecurity Strategy 2021–2025: available at: <https://ccdcOE.org/library/strategy-and-governance> (12 April 2022).
- Sparks, C. (2003): Are the Western Media Really That Interested in China? *Javnost – The Public* 10(4): 93–108.
- Trim, P. – Upton, D. (2016): *Cyber Security Culture. Counteracting Cyber Threats through Organizational Learning and Training*, New York: Routledge.
- Valeriano, B. – Maness, R.C. (2014): The Dynamics of Cyber Conflict between Rival Antagonists, 2001–2011. *Journal of Peace Research* 51(3): 347–360.
- Warner, J. – Chapin, E. Matfess. H. (2019): Suicide Squads: The Logic of Linked Suicide Bombings. *Security Studies* 28 (1): 8–9.

Marek Górka graduated in Political Science at the Nicolaus Copernicus University in Toruń/ Poland. He is Associate 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. E-mail: marek_gorka@wp.pl.